úřad
pro ochranu
osobních
údajů

informační bulletin

1 / 2003

Změna sídla Úřadu

V souvislosti se vznikem Ministerstva informatiky, jehož organizační složky obsadily celou budovu bývalého Úřadu pro veřejné informační systémy, v níž doposud sídlil i Úřad pro ochranu osobních údajů, bylo v prosinci rozhodnuto o změně sídla Úřadu. Na základě výběrového řízení byl vybrán objekt v Praze 7 – Holešovicích, ulice Pplk. Sochora 27. S majitelem objektu byla podepsána smlouva o nájemním vztahu. Přesídlením do této budovy, která dostatečnou rozlohou využitelné kancelářské plochy i z dalších hledisek poskytuje dobré podmínky pro práci Úřadu, by se měl vyřešit od vzniku Úřadu přetrvávající problém jeho definitivního umístění v odpovídajících a důstojných prostorách. Na tento problém upozornila v létě loňského roku ve své zprávě i Hodnotící mise k ochraně osobních údajů v České republice tvořená zahraničními experty vyslanými Evropskou komisí (Peer Rewiew) a také Pravidelná zpráva Evropská komise za rok 2002.

Přechod kompetence k udělování akreditací poskytovatelům certifikačních služeb

S účinností od 1. ledna 2003 byl zákonem č. 517/2002 Sb. změněn zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, v § 2 a § 29. Udělování a odnímání akreditací k působení jako akreditovaný poskytovatel certifikačních služeb a dozor nad dodržováním povinností stanovených zákonem o elektronickém podpisu byly touto novelou dány do kompetence nově vzniklému Ministerstvu informatiky. V souvislosti s tím byl do tohoto ministerstva organizačně začleněn dosavadní Odbor elektronického podpisu Úřadu pro ochranu osobních údajů.

Sledování kamerovými systémy

Ve čtvrtém čtvrtletí roku 2002 se Úřad zabýval několika stížnostmi a podněty na sledování určitých prostor kamerovými systémy. Jednalo se zejména o veřejné prostory provozoven restaurací a také o pracoviště sledované z rozhodnutí zaměstnavatele. Pokud jsou kamerové systémy pro monitorování určitých prostor používány, je třeba, aby přitom byla dodržována určitá pravidla. Osoby, které se v takových prostorách nacházejí, by měly být viditelným nápisem či zvláštním sdělením upozorněny na skutečnost, že objekt je průmyslovými kamerami monitorován, s uvedením účelu (např. prevence proti krádežím). Sledovat nelze prostory určené k ryze soukromým účelům, např. toalety. Záznamy je třeba chránit před zneužitím a bez odkladu je likvidovat, jakmile pomine důvod, pro který byly pořízeny.

úřad pro ochranu osobních údajů

Národní zdravotní registry

Úřad pro ochranu osobních údajů zaujal kritický postoj k podmínkám, za nichž mají být zpracovávány osobní údaje pacientů v národních zdravotních registrech. Shromažďování citlivých údajů pro tyto registry má být realizováno na základě vyhlášky Ministerstva zdravotnictví. Je pochopitelné, že tyto údaje jsou pro určité zdravotnické účely potřebné. Nezbytně nutný rozsah údajů pro jednotlivé registry by však měl být podrobně posouzen jak odbornou zdravotnickou veřejností, tak ochránci osobních údajů a poté upraven zákonem, nikoli pouze ministerskou vyhláškou. Pro některé (např. statistické) účely by měly být osobní údaje anonymizovány. Obdobně kritický postoj jako Úřad zaujal k tomuto problému i vládní zmocněnec pro lidská práva Jan Jařab.

Věstník Úřadu pro ochranu osobních údajů

V částkách 20 a 21, které byly vydány v průběhu čtvrtého čtvrtletí roku 2002, byly zveřejněny překlady dalších dvou doporučení Rady Evropy k ochraně osobních údajů. V říjnové částce 20 Doporučení č. R 87 (15), upravující používání osobních údajů v policejním sektoru, a v prosincové částce 21 Doporučení o ochraně osobních údajů v oblasti telekomunikačních služeb, se zvláštním zřetelem k telefonním službám. Čtenáři Věstníku si mohli prostudovat také nový překlad Směrnice Evropského parlamentu a Rady 95/46/ES o ochraně jednotlivců v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, který zohledňuje terminologii používanou v zákoně č. 101/2000 Sb., ve znění pozdějších předpisů. Dále se mohli seznámit se Závěrečnou zprávou Peer Review – Hodnotící mise k ochraně osobních údajů v České republice, která se uskutečnila v létě loňského roku, a s Prohlášením o spolupráci mezi Úřadem pro ochranu osobních údajů a Agenturou na ochranu dat Španělska. Obsahem obou částek byly samozřejmě i informace o aktuálních změnách v registru povolených zpracování osobních údajů.

Internetové stránky zemí V4 a Pobaltí

Novým informačním kanálem se pro Úřad stala spoluúčast na webových stránkách států V4 a Pobaltí. Stránky vznikly jako podpůrný nástroj pro spolupráci mezi úřady pro ochranu osobních údajů uvedených států. Stejně jako ke vzniku spolupráce přispěly i k realizaci těchto stránek především český a polský úřad. Podoba stránek byla dojednána na pražské schůzce komisařů v dubnu roku 2002. Mají částečně informativní charakter sloužící veřejnosti a částečně podporují spolupráci ochránců osobních údajů z Bulharska, České republiky, Estonska, Maďarska, Litvy, Lotyšska, Polska a Slovenska, slouží jako prostředek konzultací a svým způsobem i permanentní konference. Na adrese www.ceecprivacy.org – Central and Eastern Europe Data Protection Authorities Web Site najdete představení všech úřadů sedmi uvedených států (Bulharsko své informace připravuje), podílejících se na této spolupráci, a přehled kompetencí, které jsou jim v ochraně osobních údajů svěřeny. V anglickém jazyce si zde můžete prostudovat právní předpisy těchto států i stanoviska publikovaná ke specifickým problémům ochrany osobních údajů, včetně odkazů na příslušné stránky vytvářené v jednotlivých úřadech. Součástí stránek je také přehled aktuálních událostí.

Krádež identity a jak jí předcházet

Podporuje-li překotný technologický rozvoj v telekomunikacích a informatice styk mezi podnikatelskou sférou a spotřebiteli, pak stejně tak umožňuje šířit ve velkém měřítku osobní údaje, což usnadňuje činnost kriminálních živlů. Objevil se nový a velmi nebezpečný fenomén – kradení identity osob. ***Zabývá se jím také tato naše informace čerpající ze zkušeností kanadských ochránců dat.***
Krádež identity je nedovolené shromažďování a používání osobních údajů, obvykle za účelem kriminální činnosti. Jméno, datum narození, adresa bydliště, číslo kreditní karty, číslo sociálního nebo zdra-

votního pojištění a především rodné číslo mohou posloužit pro otevření bankovního účtu, zřízení kreditní karty, výběr poštovní zásilky, předplacení služby mobilního telefonování, najmutí vozu nebo bytu, a také při nástupu do zaměstnání.

Pokud někdo ukradl vaši identitu, hrozí, že ponesete odpovědnost za účty, výdaje, nekryté šeky, daňové pohledávky a nejrůznější škody způsobené sice cizí osobou, ale vaším jménem. Například ve Spojených státech amerických je krádež identity jednou z nejrychleji rostoucích trestných činností. Podle odhadů se tam každoročně stane její obětí na půl miliónu osob. Primitivní způsoby, jako je hledání bankovních výpisů cizích osob v odpadkových koších, vystřídaly velmi sofistikované metody. Jsou známy případy, kdy hackeři dokázali proniknout do databází velkých firem a stáhnout spolu s dalšími údaji i čísla kreditních karet zaměstnanců.

Nabízí se otázka, jak může každý z nás předcházet krádeži identity. V odborném tisku se uvádí celá řada zásad. Následující přehled uvádí jen ty opravdu elementární a snadno použitelné:

- Požaduje-li někdo vaše osobní údaje, informujte se o účelu, pro který jsou shromažďovány, o způsobu jejich využití a zeptejte se, jaká opatření budou učiněna pro jejich ochranu před zneužitím.
- Neposkytujte více informací, než musíte. Noste při sobě co možná nejméně osobních údajů.
- Zacházejte s největší opatrností s rodným číslem. Umožňuje přístup k celé řadě dalších informací o vás.
- Číslo kreditní karty nesdělujte nikdy po telefonu ani elektronickou poštou, pokud neznáte druhého účastníka takové komunikace nebo máte pochybnosti o její bezpečnosti.
- Při práci na internetu používejte technologie ochraňující vaši bezpečnost a soukromí.
- Kontrolujte pečlivě výpisy z bankovních účtů a faktury za elektřinu, plyn a další služby. Nedostanete-li očekávaný výpis nebo účet, ověřte si, byl-li skutečně odeslán a zda nedošlo k jeho odcizení. Doporučuje se také, nenechávat si zasílat bankovní výpisy domů a raději je vybírat osobně v bance.
- V případě ztráty nebo odcizení identifikačních dokumentů nebo kreditní karty informujte ihned příslušné orgány (policie, banka, atd.).
- Před použitím bankomatu se ujistěte, že nikdo nemůže odečíst při zadávání váš PIN.
- Vybírejte si přístupová hesla, která se dají jen velmi obtížně uhodnout nebo odvodit. Zapamatujte si je a často měňte. V žádném případě je neuchovávejte napsaná v peněžence nebo na lehce přístupných místech.
- Zničte před odhozením do koše bankovní výpisy a jiné dokumenty obsahující informace o vašich finančních transakcích, popř. další osobní údaje.

Ze zahraničí

„Evropský přístup" k bezpečnosti sítí a elektronické komunikace

Evropský parlament se vyslovil pro jednotný přístup evropských států k bezpečnosti počítačových sítí a elektronické komunikace. Mezi opatřeními, která by měla být přijata na evropské úrovni, je i výzva Evropské komisi, aby navrhla akční plán na podporu elektronických podpisů na bázi evropských standardů tak, aby mohly být urychleně aplikovány v institucích Evropské unie. Evropský parlament podpořil myšlenku vytvoření výzkumné skupiny, jejímž úkolem by bylo zjistit, které národní orgány jsou odpovědné za řízení sítí v případě krizí, zajistit koordinaci těchto činností, zřídit centrum pro výměnu informací a preventivní opatření a organizovat evropská diskusní fóra.

Ochrana práv a soukromí zaměstnanců na pracovištích

Potřeba ochrany osobních údajů zaměstnanců na pracovišti, zejména s ohledem na respektování jejich práva na soukromí, je v poslední době velice aktuální téma, kterým se intenzivně zabývá i Ev-

ropská unie. Evropská komise v tomto směru uspořádala již dvě oficiální konzultace sociálním partnerům, tj. zástupcům různých zaměstnavatelských svazů, odborů apod. První konzultace proběhla v srpnu 2001 a zaměřila se především na oblast zacházení s citlivými údaji v pracovním procesu, jako je přístup ke zdravotním údajům a nakládání s těmito údaji, výsledky drogových a genetických testů a dohled nad používáním elektronické pošty a internetu zaměstnanci.

Druhá konzultace byla zahájena 31. října 2002, jednak na základě analýzy odezvy sociálních partnerů na první konzultaci, jednak vzhledem k potřebě reagovat na rostoucí riziko porušování základních práv zaměstnanců v souvislosti s technickým pokrokem, globalizací a pocitem nejistoty po 11. září 2001. Během druhé konzultace Komise navrhla sociálním partnerům rámcové evropské zásady a pravidla upravující ochranu osobních údajů zaměstnanců na pracovišti. Jak zaznělo během jednání, jedním z hlavních úkolů bude nalézt rovnováhu mezi základními právy zaměstnanců, zejména právem na soukromí, a legitimními zájmy zaměstnavatelů.

Komise navrhla řídit se následujícími hlavními tezemi:

- Nepovažovat samotný souhlas zaměstnance se zpracováním jeho údajů zaměstnavatelem za dostatečnou ochranu, zejména při zacházení s citlivými údaji (týkajícími se rasového a etnického původu, politických názorů, náboženského a filozofického přesvědčení, členství v odborech nebo sexuální orientace);
- Vytvořit na evropské úrovni obecný rámec pro zacházení se zdravotními údaji;
- Omezit testování užívání drog a shromažďování údajů z tohoto testování, stejně jako využívání genetických testů a dat vyplývajících z těchto testů zaměstnavateli (v Rakousku, Portugalsku a Nizozemí již zakázali využívání dat vyplývajících z genetických testů);
- Vytvořit soubor transparentních a explicitních zásad pro kontrolu chování zaměstnanců a dohled nad jejich komunikací, jako je například elektronická pošta a používání internetu.

Komise konstatovala, že v oblasti zacházení s osobními údaji zaměstnanců přijaly ze všech členských států příslušnou specifickou legislativu pouze Finsko a Dánsko. Velká Británie a Nizozemí jsou připraveny řešit tuto otázku prostřednictvím etických kodexů. Současně také připomněla, že vytvoření specifických pravidel ochrany osobních údajů používaných pro zaměstnanecké účely požadují rovněž Mezinárodní organizace práce (ILO) a Rada Evropy.

Sociální partneři byli vyzváni, aby do šesti týdnů Komisi seznámili se svými stanovisky k jejím návrhům. V průběhu konzultačního období by měli vyjádřit svoji vůli dospět v dané záležitosti ke vzájemní dohodě a tu pak uzavřít do devíti měsíců.

Belgie:
Internet na pracovišti – pouze pro pracovní potřebu?

Průzkumy a studie ukazují, že odesílání soukromých e-mailů a surfování po internetu na pracovišti způsobuje podnikům značné finanční ztráty, především v důsledku ztraceného pracovního času. Proto firmy stále častěji sledují své zaměstnance, jak a k čemu používají prostředky elektronické komunikace, kterými jsou vybavena jejich pracovní místa. Nabízí se tak otázka, jak sladit přirozený zájem zaměstnavatelů s nárokem zaměstnanců na ochranu soukromí.

Snaha o nalezení vyváženého a systémového řešení tohoto problému je patrná již několik let. Například v belgickém parlamentu byl minulý rok předložen návrh, jak legislativní cestou dosáhnout vyváženého řešení. Jednalo se o návrh zákona, který má „upravovat používání internetu a e-mailu na pracovišti". Tento dokument má zaměstnavatelům umožnit provádění kontroly, jak zaměstnanci nakládají s prostředky elektronické komunikace na pracovišti, ovšem při zachování určitých pravidel, která především vyplývají z článku 8 Evropské úmluvy o lidských právech.

Návrh je založen na třech základních principech: proporcionalita, transparentnost a stanovení účelu.

Princip proporcionality vyjadřuje zásadu, aby kontrola pracovníků byla časově omezená nebo pouze namátková. Průběžná kontrola automatizovanými prostředky by měla být přípustná, jen pokud existuje konkrétní podezření, že daný pracovník zneužívá svěřených prostředků pro soukromé účely.

Princip transparentnosti spočívá v požadavku, aby zaměstnanci byli předem informováni o možnosti jejich sledování při užití prostředků elektronické komunikace. Také by měli vědět, jakými prostředky a za jakým účelem ke sledování dochází.

Princip stanovení účelu říká, že zaměstnavatel by měl kontrolu provádět jenom za přesně vymezeným účelem. Výše uvedený návrh zákona stanovuje následující účely, které považuje za přípustné:

- ochrana práv a svobod jiných osob
- ochrana majetku a firemního tajemství před zničením nebo odcizením
- potřeba zachování pracovního tajemství
- kontrola plnění pracovních úkolů
- záruka zachovávání dobrých mravů na pracovišti
- zajišťování prevence, zkoumání a odhalování podezřelých činností v rámci odpovědnosti zaměstnavatele
- obrana proti vyzrazení důvěrných nebo škodlivých informací o podniku, jeho smluvních partnerech, třetích osobách nebo jiných pracovnících
- zajištění bezpečnosti a funkčnosti sítě
- prevence a odhalování jakéhokoli užívání prostředků elektronické komunikace na pracovišti, které je protizákonné nebo neslučitelné s pravidly stanovenými zaměstnavatelem.

I v případě dodržování výše uvedených principů se doporučuje, aby zaměstnavatel uzavřel se svými pracovníky (například prostřednictvím zaměstnanecké rady) dohodu, která by specifikovala zásady užívání prostředků elektronické komunikace na pracovišti, a také podmínky a způsob kontroly.

Ve sdělovacích prostředcích, odborných publikacích a samozřejmě na webu existuje nepřeberné množství materiálů k této problematice. Na tomto místě odkazujeme především na internetové stránky evropských komisařů ochrany dat. Jsou dostupné například přes webovou stránku Úřadu pro ochranu osobních údajů (www.uoou.cz).

Švýcarsko:
Může pacient požadovat skartování své zdravotnické dokumentace, přestože zákon vyžaduje její zachování?

Může.

Kantonální právní předpisy zpravidla vyžadují, aby zdravotnická dokumentace pacienta byla uchovávána po dobu deseti let – tato lhůta se ovšem může kanton od kantonu lišit. Pacient však má právo zbavit lékaře povinnosti tuto dokumentaci archivovat a může požadovat její likvidaci. V takovém případě se však musí, před vypršením skartační lhůty, vzdát všech svých nároků na léčbu, vyplývajících ze smlouvy mezi ním a lékařem. Je v zájmu pacienta předložit svou příslušnou žádost lékaři, klinice či laboratoři, jichž se tato záležitost týká. Pacient může rovněž vyžadovat písemné potvrzení o realizaci skartace.

Připomeňme, že pozůstalý člen manželského páru může toto právo uplatnit za zesnulého člena tohoto svazku. Manžel tak kupříkladu může vyžadovat likvidaci zdravotnické dokumentace své zesnulé manželky, a to pokud to nebude v rozporu s převažujícím zájmem některého z dalších pozůstalých manželky, nebo pokud to nebude v konfliktu s opodstatněným zájmem třetí strany.

Pokud si navíc pozůstalý manžel bude přát nahlédnout do zdravotnické dokumentace zesnulé manželky, může se odvolat na článek 1, § 7 vyhlášky k zákonu o ochraně osobních údajů. Ten žadatele opravňuje k nahlížení do zdravotnické dokumentace zesnulé osoby, pokud k ní má úzký příbuzenský vztah (rodiče, manžel apod.).

Žadatel však v tomto svém právu může být omezen rozhodnutím Federálního soudu, pokud zesnulý za svého života vyslovil přání, aby jeho zdravotnická dokumentace byla po jeho smrti pokládána za důvěrnou. Toto právo zesnulého musí být respektováno, manželský partner zesnulé osoby však může své právo na nahlížení do zdravotnické dokumentace zesnulého partnera uplatnit nepřímo: má totiž možnost pověřit lékaře (kterého si může sám zvolit), aby se v jeho zastoupení seznámil s obsahem zdravotnické dokumentace zesnulého a aby mu následně sdělil všechny podstatné informace.

Švýcarský spolkový úřad pro ochranu osobních údajů (PFPD) požaduje, aby zákon o ochraně osobních údajů byl při reklamních akcích realizovaných prostřednictvím pošty respektován.

Podnikatel Martin Fűrst již po delší dobu pravidelně zasílá společnostem a soukromým osobám nevyžádanou poštu, jejímž předmětem je inzerce na různé produkty a služby. Pro tuto činnost používá jakožto odesílatel jmen různých společností (do dnešního dne jsou známy např. Fűrst E–Marketing, Horizon Business Corporation for Work and Living).

Shromažďování, používání a předávání poštovních adres tak, jak je tomu i v tomto případě, představuje podle spolkového zákona o ochraně osobních údajů **zpracování osobních údajů**, a to ve smyslu čl. 2, odst. 1, písm. a). Z tohoto důvodu je správce databáze těchto údajů (v tomto případě je to pan Martin Fűrst) na požádání dotčených osob povinen sdělit těmto osobám veškeré osobní údaje, které se jich týkají a které zpracovává a – pokud si to tyto osoby přejí – tyto údaje ve své databázi zlikvidovat. Podle sdělení dotčených osob však Martin Fűrst na takové žádosti nereflektoval.

Ve smyslu doporučení PFPD byl p. Fűrst vyzván, aby dotčené osoby informoval, respektive zlikvidoval jejich údaje v příslušné databázi, jak to stanoví spolkový zákon o ochraně osobních údajů.

V případě, že pan Fűrst do 30 dnů od obdržení tohoto doporučení nevyhoví zmíněnému požadavku, bude věc postoupena Spolkovému výboru pro ochranu údajů.

Celé výše uvedené doporučení je (v němčině) zveřejněno na internetových stránkách PFPD *www.edsb.ch/d/.*

Bez rodného čísla nepohnojí ...

Rodné číslo je problém. Ne proto, že se objevuje v televizi v nejsledovanějších časech. Ani ne proto, že na něj narazíte na téměř neuvěřitelných místech. Takový místem je pro mne evidence o použití hnojiv na lesním pozemku. Ale jak říkám, proto rodné číslo problém není; dokonce ani proto ne, že ho po mně chtějí na nějakých vrátnicích. Rodné číslo je čistý, nefalšovaný a ne uměle (např. médii) vyvolaný problém. Takový problém se pozná výhradně podle toho, že se úplně jinak jeví tomu, kdo něčí rodné číslo chce – prosím za prominutí – vlastně potřebuje a úplně jinak tomu, jehož rodné číslo je vyžadováno nebo i bez vyžadování obyčejně použito. Pravda je, že pro některé lidi rodné číslo problémem jistojistě není – do chvíle, než se jím stane – obvykle použitím jejich vlastního rodného čísla nebo čísla osoby jim blízké, společně s dalšími osobními údaji.

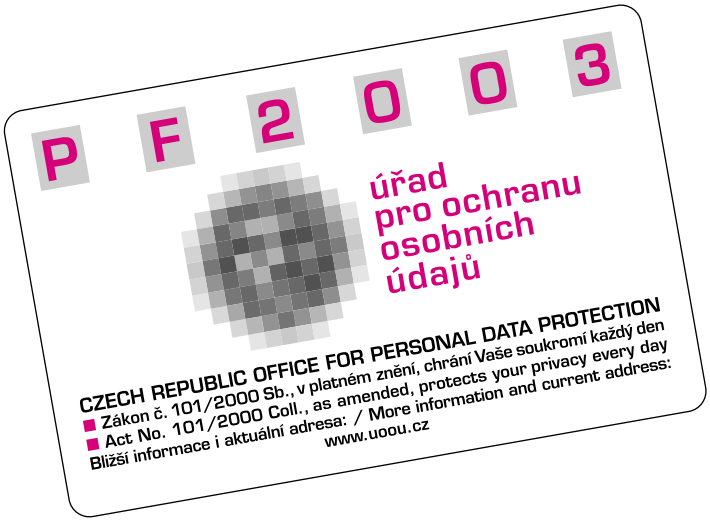
Říkám si, jak k tomu takový nevinný, čistě výpomocný identifikátor vlastně přišel? Proč se se změnou politických poměrů rozběhl do všech existujících zákoutí institucionalizovaných mezilidských vztahů? Jakkoli je obtížné pochopit, proč se bez něj občané republiky neožení nebo neprovdají a nemohou být pohřbeni (do umírání se nějak rodné číslo nedostalo), při troš-

ce snahy to jde. Řeknu si, že u mrtvých na nějakém osobním údaji už nezáleží. Ta rodná čísla na oddacím listu třeba plní kontrolní funkci a stvrzují, že sňatek uzavřely – jak zákony této země očekávají – osoby různého pohlaví, pro případ, že manželství uzavřeli Andrea Kubů a Andrea Krejčí. Zaženu i pochybnost vtírající se s námitkou, že manželství uzavřeli Andrea Kubů a osoba jiné státní příslušnosti, jejíž jméno pohlaví též neprozrazuje. I námitku o nerovnosti podmínek námořníků vybavených námořnickou knížkou podle českých zákonů a námořníků s námořnickými knížkami vystavenými za hranicemi naší vlasti a bez rodných čísel potlačím. Uniká mi, proč se nelze přihlásit jako uchazeč o složení makléřské zkoušky bez rodného čísla, když makléři mi připadají jako bezchybný symbol dokonané globalizace. Taktéž mi stále uniká, proč jsou pro informování veřejnosti o projektech a výzkumných záměrech podporovaných z veřejných prostředků tak důležitá rodná čísla všech řešitelů a spoluřešitelů, když pro kontrolu nakládání s veřejnými prostředky u cizinců stačí datum narození.

Už to mám! Prostě to vidím příliš z nadhledu: oslnily mne ty desítky zákonů a desítky vyhlášek i několik nařízení vlády, které do formulářů nebo i dokladů a veřejných listin rodná čísla zavádějí. Kontroly není nikdy dost! Mám-li něčí rodné číslo, mám tolik možností si o jím obsazeném jedinci něco zjistit. Stačí mi k tomu veřejně dostupné zdroje a prameny. A pokud v nich „mým RČ" obsazený jedinec není, je na zvážení, jestli to není jeho (myslím toho obsazeného) nedostatek.

Jenom pořád nevím, proč se bez rodného čísla nepohnojí lesní pozemek. Myslíte, že to někdo ví?

mt



VYDÁVÁ ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ

ODPOVĚDNÝ REDAKTOR: MGR. LADISLAV HEJLÍK

ADRESA REDAKCE: ÚOOÚ, PPLK. SOCHORA 27, PRAHA 7, 170 00

TELEFON: 234 665 248, 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 3. 2. 2003