VĚSTNÍK
ÚŘADU PRO OCHRANU OSOBNÍCH ÚDAJŮ
2011

Částka 58 **23. května 2011** **Cena 90,- Kč**

OBSAH

ÚVOD

Částka 58 Věstníku Úřadu pro ochranu osobních údajů je první částkou roku 2011. Obsahuje přehled zrušených registrací za období od 20. 11. 2010 do 3. 5. 2011.

V rubrice Sdělení Úřadu je začleněn oddíl Z rozhodovací činnosti Úřadu. Přináší přehled rozhodnutí, k nimž Úřad dospěl na základě řešení případů porušení zákona o ochraně osobních údajů nebo podezření z porušení tohoto zákona.

Součástí Sdělení je také „Stanovisko Úřadu pro ochranu osobních údajů k Návrhu směrnice Evropského parlamentu a Rady o používání údajů jmenné evidence cestujících pro prevenci, odhalování, vyšetřování a stíhání teroristických činů a závažné trestné činnosti“. Navrhovaná směrnice má zakotvit povinnost předávat údaje o všech cestujících na letech, které směřují ze států mimo Evropskou unii do členských států a naopak, a to do databáze, kterou má spravovat k tomuto účelu v každém členském státě, nebo centrálně zřízený, útvar pro informace o cestujících. Vzhledem k závažnosti dopadu chystaného opatření do práva na ochranu soukromí Úřad v tomto stanovisku předkládá vlastní pozici, která se snaží objasnit, jak navrhované opatření zasáhne do základních práv a svobod velkého počtu občanů Evropské unie.

Dalším materiálem této rubriky je dokument „Doporučení CM/Rec (2010) 13 Výboru ministrů členským státům o ochraně osob s ohledem na automatizované zpracování osobních údajů v souvislosti s profilováním“. Dokument objasňuje vážná rizika pro práva a svobody jednotlivce, která mohou vznikat v důsledku nedostatku transparentnosti, či dokonce „neviditelnosti“ profilování vyplývající z automatického užívání přednastavených vyhodnocovacích pravidel. Dokument také mimo jiné stanovuje podmínky shromažďování a zpracovávání osobních údajů v souvislosti s profilováním a apeluje na členské státy, aby podporovaly navrhování a zavádění postupů a systémů v souladu s ochranou soukromí a dat již ve fázi plánování, zejména cestou technologií zvyšujících ochranu soukromí.

Rubrika dále přináší Stanovisko č. 7/2010 Pracovní skupiny pro ochranu údajů podle článku 29 směrnice 95/46/ES (WP29) o sdělení Evropské komise o globálním přístupu k přenosům údajů jmenné evidence cestujících (PNR) do třetích zemí. Komise se rozhodla vytvořit soubor obecných kritérií, která by se měla vztahovat na všechny budoucí dohody týkající se PNR s třetími zeměmi. Sdělení mimoto obsahuje analýzu současného používání PNR a poskytuje informace o plánech Komise, jaké dohody s třetími zeměmi mají být v nadcházejících letech uzavřeny.

Jako poslední je v rubrice umístěna informace o technické chybě v 57. částce Věstníku.

Rubriku Materiály z Úředního věstníku Evropské unie naplňuje dokument Rozhodnutí Komise 2011/61/EU ze dne 31. 1. 2011 o odpovídající ochraně osobních údajů Státem Izrael v souvislosti s automatizovaným zpracováním osobních údajů podle směrnice Evropského parlamentu a Rady 95/46/ES. Úřad přetiskuje materiály z Úředního věstníku Evropské unie v jejich původní podobě a nepřebírá odpovědnost za případné nepřesnosti překladu.

Přehled zrušených registrací

Číslo registrace	Subjekt	Datum zrušení
00003323/001	KÖGEL AKCIOVÁ SPOLEČNOST	27.11.2010
00003323/002	KÖGEL AKCIOVÁ SPOLEČNOST	27.11.2010
00003323/003	KÖGEL AKCIOVÁ SPOLEČNOST	27.11.2010
00003323/004	KÖGEL AKCIOVÁ SPOLEČNOST	27.11.2010
00005938/009	MĚSTO NOVÝ JIČÍN	9.12.2010
00005938/010	MĚSTO NOVÝ JIČÍN	9.12.2010
00005938/011	MĚSTO NOVÝ JIČÍN	9.12.2010
00005938/012	MĚSTO NOVÝ JIČÍN	9.12.2010
00005938/013	MĚSTO NOVÝ JIČÍN	9.12.2010
00005938/014	MĚSTO NOVÝ JIČÍN	9.12.2010
00005938/015	MĚSTO NOVÝ JIČÍN	9.12.2010
00005938/016	MĚSTO NOVÝ JIČÍN	9.12.2010
00005938/017	MĚSTO NOVÝ JIČÍN	9.12.2010
00005938/018	MĚSTO NOVÝ JIČÍN	9.12.2010
00005938/020	MĚSTO NOVÝ JIČÍN	9.12.2010
00014709/004	VŠEOBECNÁ ZDRAVOTNÍ POJIŠŤOVNA ČESKÉ REPUBLIKY	4.2.2011
00023077/005	ČESKÉ DRÁHY, A.S.	14.1.2011
00023077/006	ČESKÉ DRÁHY, A.S.	14.1.2011
00023077/007	ČESKÉ DRÁHY, A.S.	14.1.2011
00023077/009	ČESKÉ DRÁHY, A.S.	14.1.2011
00023077/010	ČESKÉ DRÁHY, A.S.	14.1.2011
00023077/011	ČESKÉ DRÁHY, A.S.	14.1.2011
00023077/012	ČESKÉ DRÁHY, A.S.	14.1.2011
00023077/013	ČESKÉ DRÁHY, A.S.	14.1.2011
00023077/015	ČESKÉ DRÁHY, A.S.	14.1.2011
00023077/016	ČESKÉ DRÁHY, A.S.	14.1.2011
00023077/017	ČESKÉ DRÁHY, A.S.	14.1.2011
00023077/018	ČESKÉ DRÁHY, A.S.	14.1.2011
00023077/019	ČESKÉ DRÁHY, A.S.	14.1.2011
00023077/020	ČESKÉ DRÁHY, A.S.	14.1.2011
00023077/021	ČESKÉ DRÁHY, A.S.	14.1.2011
00023077/022	ČESKÉ DRÁHY, A.S.	14.1.2011
00023077/023	ČESKÉ DRÁHY, A.S.	14.1.2011
00023077/024	ČESKÉ DRÁHY, A.S.	14.1.2011
00025654/001	SIEMENS VDO AUTOMOTIVE	22.3.2011
00032456/001	OHL ŽS, A.S.	24.2.2011
00032714/001	INTERHOTEL VORONĚŽ A.S.	27.4.2011
00032714/002	INTERHOTEL VORONĚŽ A.S.	27.4.2011
00032714/003	INTERHOTEL VORONĚŽ A.S.	27.4.2011
00033930/001	MĚSTSKÝ ÚSTAV SOCIÁLNÍCH SLUŽEB KLÁŠTEREC NAD OHŘÍ, PŘÍSPĚVKOVÁ ORGANIZACE	14.4.2011
00034130/001	SCHIDLOF JAN GEORG VLADIMÍR	31.12.2010
00035730/001	DUŠAN PRACHAŘ	11.1.2011
00036493/001	PRVNÍ ZPRAVODAJSKÁ A.S.	11.3.2011
00036493/002	PRVNÍ ZPRAVODAJSKÁ A.S.	11.3.2011
00036493/003	PRVNÍ ZPRAVODAJSKÁ A.S.	11.3.2011
00037903/001	GE MONEY, S.R.O.	25.11.2010
00037903/002	GE MONEY, S.R.O.	25.11.2010
00037903/003	GE MONEY, S.R.O.	25.11.2010
00037903/004	GE MONEY, S.R.O.	25.11.2010
00037903/005	GE MONEY, S.R.O.	25.11.2010
00037903/006	GE MONEY, S.R.O.	25.11.2010
00037903/007	GE MONEY, S.R.O.	25.11.2010

II. SDĚLENÍ ÚŘADU

Z rozhodovací činnosti Úřadu

Sdělení úvodem:
Úřad pro ochranu osobních údajů se prostřednictvím následující stručné charakteristiky vyjadřuje k některým problematickým okruhům případů porušování povinností při zpracování osobních údajů, které projednává v rámci své rozhodovací činnosti.

1. Povinnosti zaměstnanců při zpracování osobních údajů

Správní orgán po posouzení postoupené spisové dokumentace dospěl k závěru, že jednání podezřelé J. M. spočívající v neoprávněném nahlížení do informačních systémů zaměstnavatele (Policie České republiky) je z hlediska plnění povinností dle zákona č. 101/2000 Sb. porušením povinnosti dle § 14. Dle tohoto ustanovení může zaměstnanec správce nebo zpracovatele osobních údajů zpracovávat osobní údaje pouze za podmínek nebo v rozsahu správcem nebo zpracovatelem stanoveném. Porušení povinnosti dle § 14 zákona č. 101/2000 Sb. přitom nenaplňuje skutkovou podstatu žádného z přestupků dle tohoto zákona. Ze spisového materiálu přitom nelze dovodit natolik silné podezření, že podezřelá osobní údaje sdělila třetí osobě, které by odůvodňovalo posouzení takového jednání jako porušení povinnosti mlčenlivosti dle § 15 zákona č. 101/2000 Sb., a tedy podezření ze spáchání přestupku dle § 44 odst. 1 písm. a) zákona č. 101/2000 Sb. (čj. *SPR-0274/10*)

2. Legální titul zpracování osobních údajů

Podle § 5 odst. 2 zákona č. 101/2000 Sb. má správce povinnosti zpracovávat osobní údaje pouze se souhlasem subjektu údajů, bez tohoto souhlasu je může zpracovávat při naplnění některé z výjimek uvedených v § 5 odst. 2 písm. a) až g). V tomto případě se jedná o jeden ze základních principů zákonnosti každého zpracování osobních údajů, tzn., že každé zpracování musí mít svůj legální titul. Základním právním titulem zpracování je nepochybně souhlas subjektu údajů. Není-li správce schopen zpracovávat osobní údaje na základě souhlasu subjektu údajů, musí jím prováděné zpracování být v souladu s některým z právních titulů vyjádřených v § 5 odst. 2 písm. a) až g) zákona č. 101/2000 Sb. Samotná objektivní nemožnost získat souhlas subjektu údajů ještě neznamená, že by bylo možné vyloučit aplikaci zbývajících částí tohoto ustanovení, neboť v tomto případě by zpracování jeho právní titul scházel. Proto pokud správce nesplní ani jednu z těchto nabízených možností pro zpracování osobních údajů bez souhlasu subjektu údajů, je nepochybné a zjevné, že takové zpracování je v rozporu s povinností uloženou mu celým zněním § 5 odst. 2 zákona č. 101/2000 Sb. (čj. *SPR-6070/09*)

3. Porušení zákazu zveřejnění osobních údajů v souvislosti s trestním řízením

Ve vztahu ke skutkové podstatě přestupku dle § 44a odst. 1 zákona č. 101/2000 Sb. se totiž správní orgán dále zabýval otázkou materiální stránky přestupku ve smyslu § 2 odst. 1 zákona č. 200/1990 Sb., tedy tím, zda by případné prokázání jednání JUDr. R. naplňující formální znaky přestupku bylo možné považovat za porušující nebo ohrožující zájem společnosti.

Dle čl. 17 Listiny základních práv a svobod je svoboda projevu a právo na informace zaručeno. Každý má právo vyjadřovat své názory slovem, písmem, tiskem, obrazem nebo jiným způsobem. Svobodu projevu a právo vyhledávat a šířit informace lze omezit zákonem, jde-li o opatření v demokratické společnosti nezbytná pro ochranu práv a svobod druhých, bezpečnost státu, veřejnou bezpečnost, ochranu veřejného zdraví a mravnosti. Podle čl. 10 Listiny základních práv a svobod má každý právo, aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno. Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě. Podle čl. 4 odst. 4 Listiny základních práv a svobod při používání ustanovení o mezích základních práv a svobod musí být šetřeno jejich podstaty a smyslu. Povinnost mlčenlivosti, jejíž zvláštní formou je i § 8b odst. 1 zákona č. 141/1961 Sb., je zákonným omezením práva na svobodu projevu. Podle Evropského soudu pro lidská práva je třeba při zasahování do svobody projevu posoudit, zda bylo „stanoveno zákonem, zda sledovalo jeden nebo více legitimních cílů a zda bylo nezbytné v demokratické společnosti“ k dosažení těchto cílů.

Do 31. března 2009 znělo ustanovení § 8a zákona č. 141/1961 Sb. (což bylo jediné relevantní ustanovení týkající se poskytování informací o trestním řízení) tak, že dle něj orgány činné v trestním řízení informují o své činnosti veřejnost poskytováním informací sdělovacím prostředkům. Přitom dbají toho, aby neohrožovaly objasnění skutečností důležitých pro posouzení věci, nezveřejňovaly o osobách, které mají účast v trestním řízení, údaje, které přímo nesouvisejí s trestnou činností, a aby neporušily zásadu, že dokud pravomocným odsuzujícím rozsudkem není vina vyslovena, nelze na toho, proti němuž se vede trestní řízení, hledět, jako by byl vinen.

Uvedené ustanovení bylo změněno zákonem č. 52/2009

Sb., přičemž původní vládní návrh zákona se týkal pouze zvýšení právní ochrany soukromí poškozených v trestním řízení a v případě obviněných (resp. osob, proti kterým se vede trestní řízení) pouze osob mladších 18 let (viz sněmovní tisk č. 443/0; www.psp.cz; pouze k této části také existuje důvodová zpráva). Teprve v rámci dalšího legislativního procesu byla doplněna ustanovení o zákazu poskytování informací umožňujících zjištění totožnosti osoby, proti které se vede trestní řízení, a to pouze ve fázi přípravného řízení, a s tím související zákaz pro osoby vykonávající práva nebo povinnosti v trestním řízení.

Správní orgán se na základě shora nastíněných ústavních principů a limitů a vývoje relevantní právní úpravy zabýval účelem zákazu obsaženého v § 8b zákona č. 141/1961 Sb. V prvé řadě je třeba konstatovat, že z právní úpravy vyplývá, že zákaz v § 8b odst. 1 zákona č. 141/1961 Sb., tedy pro osoby, které se informace dozvědí od orgánů činných v trestním řízení, (pro zjednodušení a v souvislosti s projednávanou věci dále jen „zmocněnec“) je přísnější než zákaz uvedený v § 8a odst. 1 zákona č. 141/1961 Sb., neboť ten se vztahuje jenom na přípravné řízení, zatímco zákaz pro zmocněnce není časově omezen. Dále platí pro oba případy, že poskytnutí informací je možné pro dosažení účelu trestního řízení, který je vyjádřen v § 1 odst. 1 zákona č. 141/1961 Sb., mimo jiné jako působení k upevňování zákonnosti, k předcházení a zamezování trestné činnosti, k výchově občanů v duchu důsledného zachovávání zákonů a pravidel občanského soužití.

Správní orgán dále vycházel z následujících úvah: Ochrana soukromí je v trestním řízení nepochybně vyšší v případě poškozených, a poté svědků a dalších dotčených osob, než u osob, proti kterým se trestní řízení vede. Toto souvisí právě s preventivním účelem trestního řízení ve vztahu ke společnosti. Pomáhat k dosažení účelu trestního řízení nejsou oprávněny pouze orgány činné v trestním řízení, ale toto právo přísluší každému občanovi, tedy i poškozenému (srov. § 1 odst. 2 zákona č. 141/1961 Sb.). Je také fakticky nemožné zabránit tomu, aby se veřejnost v mediálně zajímavých trestních případech nedozvěděla o tom, proti komu je trestní řízení vedeno; lze přitom vycházet z toho, že mediální zájem ve většině případů pokrývá také veřejný zájem na informovanosti o trestné činnosti specifických osob (např. veřejně činných osob) nebo v souvislosti se specifickými okolnostmi (způsob spáchání, oběť, jiné okolnosti atd.). (čj. *SPR-1255/10*)

4. Zveřejnění osobních údajů vypovídajících o zdravotním stavu

Obviněný je zaměstnancem správce osobních údajů, J. spol. s. r. o., z čehož mu vyplývá povinnost stanovená v § 15 zákona č. 101/2000 Sb., tedy povinnost zachovávat mlčenlivost o osobních údajích. Tato povinnost mu plyne také ze zákona č. 20/1966 Sb., o péči o zdraví lidu, který v § 55 odst. 2 písm. d) stanoví povinnost zdravotnickému pracovníkovi zachovávat mlčenlivost o skutečnostech, o kterých se dověděl při výkonu svého povolání, s výjimkou případů, kdy skutečnost sděluje se souhlasem ošetřované osoby; povinnost oznamovat určité skutečnosti uložené zdravotnickému pracovníkovi zvláštním právním předpisem tím není dotčena. Povinností mlčenlivosti není zdravotnický pracovník vázán v rozsahu nezbytném pro obhajobu v trestním řízení a pro řízení před soudem nebo jiným orgánem, je-li předmětem řízení spor mezi ním, popřípadě jeho zaměstnavatelem a pacientem, nebo jinou osobou uplatňující práva na náhradu škody nebo na ochranu osobnosti v souvislosti s poskytováním zdravotní péče. V tomto případě se nejednalo o užití osobních údajů stěžovatele v souvislosti s obhajobou obviněného v některém z výše popsaných případů. Obviněný tyto osobní údaje uvedl ještě před tím, než bylo toto správní řízení zahájeno a ze skutečností uvedených v článku a v průběhu ústního jednání je zřejmé, že je užil hlavně za účelem vysvětlení resp. popření tvrzení pana A., který měl ve svém článku uvést závažné údaje poškozující dobré jméno nemocnice. Avšak tato skutečnost ještě nezakládá oprávnění lékaře zveřejnit osobní údaje pacienta, a zpřístupnit je tak široké veřejnosti. (čj. *SPR-2165/10*)

5. Obsah povinnosti mlčenlivosti

Obviněná je zaměstnankyní zpracovatele osobních údajů, z čehož jí vyplývá povinnost stanovená v § 15 zákona č. 101/2000 Sb., tedy povinnost zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by ohrozilo zabezpečení osobních údajů. V rámci své pracovní činnosti může sdělovat osobní údaje pouze samotným subjektům údajů, zejména tedy klientům advokátky JUDr. K. Sdělení či zpřístupnění informací jiným osobám, a to jakýmkoliv způsobem, je již třeba považovat za sdělení osobních údajů neoprávněnému subjektu, a tedy za porušení povinnosti mlčenlivosti. Podle § 4 odst. 1 písm. b) zákona č. 200/1990 Sb. je přestupek spáchán z nedbalosti, jestliže pachatel nevěděl, že svým jednáním může porušit nebo ohrozit zájem chráněný zákonem, ač to vzhledem k okolnostem a svým osobním poměrům vědět měl a mohl. V daném případě obviněná z přestupku měla a mohla vědět, že mezi časopisy, starými papíry a starou odbornou literaturou, kterou vyhazovala do kontejneru, mohou být i dokumenty obsahující osobní údaje. Složky s dokumentací prý přehlédla, rozhodně to nebyl její úmysl. Obviněná však měla a mohla vědět, že pokud do kontejneru, byť neúmyslně, vyhodí listiny obsahující osobní údaje, může dojít k jejich nalezení neoprávněnou osobou a k jejímu seznámení se s osobními údaji. Podle § 4 odst. 3 zákona č. 200/1990 Sb. se jednáním rozumí i opomenutí takového konání, k němuž byl pachatel podle okolností a svých osobních poměrů povinen. V tomto případě se jedná o povinnost obviněné při vyhazování starých papírů z archivu advokátní kanceláře do kontejneru pečlivě zkontrolovat, jestli některý z nich

neobsahuje osobní údaje. Obviněná z přestupku sice svůj čin podle svých slov nespáchala úmyslně, stalo se tak pouhou nedbalostí, v tomto případě je však nutno přihlížet zejména k následku, tedy k tomu, že zaviněním obviněné se s osobními údaji uvedenými v listinách seznámily neoprávněné osoby. K formě zavinění proto správní orgán přihlédl pouze při stanovení výše sankce. (čj. *SPR-3920/10*)

6. Náležitosti souhlasu se zpracováním osobních údajů

Souhlasem je jednostranný projev vůle subjektu údajů, který splňuje náležitosti dle § 4 písm. n) a § 5 odst. 4 zákona č. 101/2000 Sb. Tento úkon je dále správce osobních údajů povinen po celou dobu zpracování prokázat. Správní orgán po prostudování spisového materiálu dospěl k závěru, že k takovému úkonu ze strany nájemníků nedošlo. Z dokumentů a listin, které byly poskytnuty, nebo jinak zpřístupněny nájemníkům ze strany účastníka řízení nijak nevyplývá, že by v nich byli nájemníci jakýmkoliv způsobem požádáni o souhlas se zpracováním osobních údajů. Na základě těchto skutečností lze přinejmenším konstatovat, že i pokud by nekonání ze strany subjektů údajů (nájemníků) mělo být považováno za konkludentní souhlas, tomuto úkonu by scházel prvek vědomosti ve smyslu § 4 písm. n) zákona č. 101/2000 Sb., tedy to, že nájemníci věděli, že svojí nečinností souhlasí se zpracováním svých osobních údajů. Další prvek, který by takovému úkonu (konkludentnímu souhlasu) scházel, by byl prvek dobrovolnosti, resp. svobody vůle, neboť uvedené dokumenty nijak neinformovaly nájemníky, že se mohou, případně na koho, obrátit, aby nebyly jejich osobní údaje zpracovány, ani garance ze strany účastníka řízení, že takové žádosti okamžitě vyhoví. Že by v daném případě scházel prvek svobodnosti ostatně vyplývá i z toho, jakým způsobem účastník řízení přistoupil ke stížnosti pana K. Jinými slovy, pokud v informaci nájemníkům není uvedeno, že se oni sami mohou vyjádřit, zda se zpracováním svých osobních údajů souhlasí, a že jejich nesouhlas bude akceptován, nelze v daném případě hovořit ani o konkludentním souhlasu se zpracováním osobních údajů. (čj. *SPR-5685/09*)

7. Podmínky zpracování citlivých údajů

Podle § 5 odst. 1 písm. a) zákona č. 101/2000 Sb. je každý správce povinen stanovit účel zpracování osobních údajů. Jak je zřejmé z výše uvedeného, účastník řízení tak učinil, přičemž stanovil řadu jednotlivých účelů zpracování. V daném případě je ovšem třeba zdůraznit, že účel zpracování nemůže být stanoven naprosto libovolně; podle čl. 6 odst. 1 písm. b) směrnice Evropského parlamentu a Rady č. 95/46/ES ze dne 24. října 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, mohou být osobní údaje shromažďovány pro stanovené účely, výslovně vyjádřené a legitimní. V zákoně č. 101/2000 Sb. je toto pravidlo vyjádřeno v § 5 odst. 1 písm. a) ve spojení s § 45 odst. 1 písm. a), který upravuje skutkovou podstatu správního deliktu pro případy, kdy stanovený účel bude v rozporu s povinností vyplývající ze zvláštního zákona, nebo překročí oprávnění vyplývající ze zvláštního zákona. Účastník řízení byl nepochybně při stanovení účelu zpracování limitován tím, že je orgánem veřejné moci (správním úřadem), na který se vztahuje ústavní princip vyjádřený v čl. 2 odst. 3 Ústavy České republiky, resp. v čl. 2 odst. 2 Listiny základních práv a svobod, dle kterého lze státní moc uplatňovat jen v případech a mezích stanovených zákonem, a to způsobem, který zákon stanoví. Sběr osobních údajů o občanech státem (resp. jeho orgánem) bez jejich souhlasu je nepochybně v dané souvislosti výkonem a uplatněním státní moci vůči těmto občanům.

Ve smyslu shora uvedeného je tedy zřejmé, že účastník řízení byl oprávněn stanovit účel zpracování osobních údajů v centrálním úložišti jenom v tom rozsahu, který mu vyplýval z výslovného zákonného zmocnění. V daném případě z § 13 odst. 3 písm. n) zákona č. 378/2007 Sb. jednoznačně vyplývá oprávnění účastníka řízení v oblasti humánních léčiv zřídit a provozovat centrální úložiště. Současně ovšem uvedené ustanovení jednoznačně vymezuje účel tohoto centrálního úložiště, a tedy i účel zpracování osobních údajů, a to jako sběr a zpracování elektronicky předepisovaných léčivých přípravků. Ještě podrobněji jsou poté jednotlivé povinnosti účastníka řízení v souvislosti s centrálním úložištěm vyjádřeny v § 81 zákona č. 378/2007 Sb., přičemž všechny zde uvedené úkoly opět souvisejí jenom a pouze s elektronickými recepty.

Pokud tedy účastník řízení vymezil účely zpracování osobních údajů tak, jak je shora uvedeno, správní orgán konstatuje, že pro tento postup neměl žádnou oporu v zákoně, neboť stanovené účely nijak nesouvisely se sběrem a zpracováním elektronicky předepisovaných léčivých prostředků, a nelze je proto podřadit pod ustanovení § 81 zákona č. 378/2007 Sb. Správní orgán proto dospěl k závěru, že účastník řízení těmito stanovenými účely překročil oprávnění vyplývající ze zákona, konkrétně ze zákona č. 378/2007 Sb., a naplnil tak skutkovou podstatu správního deliktu dle § 45 odst. 1 písm. a) zákona č. 101/2000 Sb.

V této souvislosti správní orgán konstatuje, že s odkazem na čl. 10 odst. 3 Listiny základních práv a svobod a na povinnosti stanovené zákonem č. 101/2000 Sb. je zcela nepřípustné, aby jakýkoli státní orgán svévolně rozšiřoval své kompetence vymezené právními předpisy, a bez řádné opory v zákoně zřídil a provozoval informační systém sdružující rozsáhlé množství osobních a dokonce i citlivých údajů.

Podle § 5 odst. 2 zákona č. 101/2000 Sb. je správce osobních údajů povinen zpracovávat osobní údaje pouze se souhlasem subjektu údajů nebo v případech uvedených v § 5 odst. 2 písm. a) až g) zákona č. 101/2000 Sb. Podle § 9 zákona č. 101/2000 Sb. je poté správce povinen zpracovávat osobní údaje pouze s výslovným souhlasem subjektu

údajů [§ 9 písm. a) zákona č. 101/2000 Sb.], nebo bez tohoto souhlasu v případech uvedených v § 9 písm. b) až i) zákona č. 101/2000 Sb.

Ze spisového materiálu je zřejmé, že souhlasem subjektů údajů účastník řízení nedisponoval. Účastník řízení proto mohl shromažďovat a dále zpracovávat osobní a citlivé údaje osob, kterým byl vydán léčivý přípravek na listinný recept v lékárně připojené k centrálnímu úložišti, a osobám, kterým byl vydán léčivý přípravek bez lékařského předpisu s omezením, pouze za naplnění některé z výjimek ze souhlasu. Správní orgán přitom neshledal, že by byla naplněna některá z možných výjimek, zejména dle § 5 odst. 2 písm. a), resp. § 9 písm. c) zákona č. 101/2000 Sb. Dle správního orgánu nevyplývá právní povinnost účastníkovi řízení zpracovávat osobní údaje ve shora uvedeném rozsahu a uvedeným způsobem ani z § 13 odst. 3, § 82 odst. 3 písm. d) zákona č. 378/2007 Sb., ani ze směrnice Evropského parlamentu a Rady ze dne 6. listopadu 2001 č. 2001/83/ES, o kodexu Společenství týkajícím se humánních léčivých přípravků, ani z § 67b odst. 10 písm. b) zákona č. 20/1966 Sb., o péči o zdraví lidu. (čj. *SPR-6781/09*)

8. Zveřejnění osobních údajů poškozeného v trestním řízení

Podle § 8b odst. 2 zákona č. 141/1961 Sb. nesmí nikdo v souvislosti s trestným činem spáchaným na poškozeném jakýmkoliv způsobem zveřejnit informace umožňující zjištění totožnosti poškozeného, který je osobou mladší 18 let nebo vůči němuž byl spáchán trestný čin kuplířství nebo šíření pornografie nebo některý z trestných činů proti životu a zdraví, svobodě a lidské důstojnosti nebo proti rodině a mládeži. Hlava II nového zákona č. 40/2009 Sb., trestní zákoník, je označena jako trestné činy proti svobodě a právům na ochranu osobnosti, soukromí a listovního tajemství. Do této hlavy je poté v Díle 1. Trestné činy proti svobodě, zařazen také § 173 upravující trestný čin loupeže. Správní orgán vychází tedy z toho, že ačkoliv došlo k částečné změně v označení jednotlivých skupin trestných činů v jednotlivých hlavách trestního zákoníku, v případě trestného činu loupeže není pochyb o tom, že spadá mezi některé z trestných činů proti svobodě a lidské důstojnosti jak uvádí § 8b zákona č. 141/1961 Sb.

Podle § 43 odst. 1 zákona č. 141/1961 Sb. je poškozeným ten, komu bylo trestným činem ublíženo na zdraví, způsobena majetková, morální nebo jiná škoda. Jinou škodou se rozumí zejména škoda způsobená na právech, vzniká tak např. při jednání proti životu nebo zdraví, které je pouze přípravou nebo pokusem. Takovým jednáním jsou ohroženy společenské vztahy týkající se života, popř. zdraví občana, proti němuž útok směroval, je tedy způsobena např. jiná škoda na bezpečnosti života občana [srov. Trestní řád: Komentář; 1.díl (§ 1 až § 179h) / Pavel Šámal a kolektiv. 5. vyd. Praha: C.H.Beck, 2005. str. 298]. Škodou se tak ve smyslu § 43 odst. 1 zákona č. 141/1961 Sb. nerozumí jen škoda majetková nebo na zdraví, nýbrž i morální nebo jiná, tedy škoda v širším smyslu, tj. škodlivý zásah do práv a zájmů dotyčného subjektu, které jsou chráněny zákonem, i když takový zásah nemá za následek vznik nároku na náhradu škody [srov. R III/1967 in Trestní řád: Komentář; 1. díl (§ 1 až § 179h) / Pavel Šámal a kolektiv. 5. vyd. Praha: C.H.Beck, 2005. str. 309]. Správní orgán na základě shora uvedeného je toho názoru, že pokud byla paní M. přítomna při loupežném přepadení, tak bez ohledu na skutečnost, že odcizené finanční prostředky nebyly její, ale jejího zaměstnavatele, přesto je také poškozenou ve smyslu § 43 odst. 1 zákona č. 141/1961 Sb., neboť útok pachatele směřoval také přímo proti ní. Shodně k této otázce přistupoval dle svého sdělení i okresní soud. (čj. *SPR-7270/09*)

9. Zpracování osobních údajů pacientů v souvislosti s vedením účetnictví

Účastník řízení je správcem osobních údajů svých pacientů ve smyslu § 4 písm. j) zákona č. 101/2000 Sb., a proto je povinen dle § 5 odst. 1 písm. f) zákona č. 101/2000 Sb. zpracovávat osobní údaje pacientů pouze v souladu s účelem, k němuž byly shromážděny. Kód diagnózy pacienta je zpracováván za účelem informace o onemocnění pacienta a provedení vyšetřovacích výkonů, nikoli pro to, aby byl uváděn na zaslané faktuře, kde byl pro účely vyúčtování provedených vyšetřovacích výkonů také zcela nadbytečný.

Účastník řízení je povinen přihlédnout k charakteru osobních údajů a zvolit odpovídající relevantní opatření pro zajištění bezpečnosti při jejich předávání, čemuž výše popsaný způsob uvedení kódu diagnózy pacienta ve faktuře neodpovídá, když jeho uvedení nebylo nutné pro určení pacienta, ani pro určení rozsahu a předmětu plnění a faktura, která není zdravotnickou dokumentací (ta, nikoliv faktura, obsahuje všechny informace potřebné pro zajištění návaznosti poskytování zdravotní péče) a která se zakládá do účetnictví, splňuje i bez kódu diagnózy pacienta náležitosti daňového dokladu.

Správní orgán tedy na základě výše uvedeného považuje za prokázané, že účastník řízení zvoleným způsobem zpracování osobního údaje kódu diagnózy pacienta, ohrozil bezpečnost zpracovaných osobních údajů, protože faktura se stává součástí účetnictví s přístupem třetích osob, a to tím, že informaci o kódu diagnózy pacienta použil k jinému účelu, než ke kterému byla shromážděna. (čj. *SPR-0496/10*)

10. Anonymizace osobních údajů

Podle ustanovení § 4 písm. a) zákona č. 101/2000 Sb. se osobním údajem rozumí jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě

čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu. Účastník řízení opakovaně namítal, že shromažďoval osobní údaje pouze v rozsahu, kdy na jejich základě nelze dovodit konkrétní osobu či ji identifikovat nezaměnitelným způsobem. Podle správního orgánu základním kritériem pro posouzení, zda se jedná o osobní údaj či nikoliv, je potenciální možnost zjištění identity subjektu údajů (určenost nebo určitelnost). Je tedy nutno vycházet ze skutečnosti, zda správce může vytvořit přímou vazbu mezi informací a konkrétní fyzickou osobou. Tento vztah se vytváří převážně pomocí přesného identifikátoru a/nebo pomocí několika jiných údajů, které jednoznačnou identifikaci fyzické osoby tvoří (přímá identifikace). Při posuzování možnosti fyzickou osobu identifikovat je však nutno vycházet ze všech možností správce odlišit od sebe jednotlivé fyzické osoby. Tedy nikoliv pouze omezeným pohledem např. na obsah zpracovávaných dat v konkrétním zpracování (např. obsah jedné databáze), ale také zjištěním dalších možností správce subjekt údajů identifikovat. Jedná-li se např. o správce, který má zjevně v držení soubor identifikující subjekty údajů, nemůže být žádný jiný soubor, umožňující propojení na soubor s identifikátory subjektů údajů, považován za anonymní, a to ani v případech, když by zpracovávaný soubor přímou identifikaci subjektu údajů neobsahoval. Obdobně toto platí i o možnosti správce získat identifikátor ze souborů, které nejsou v jeho držení – např. z veřejných registrů, od zpracovatele, s nímž má uzavřenu smlouvu apod. V těchto případech se, v souladu s definicí osobního údaje, jedná o nepřímou možnost zjistit identifikaci subjektu údajů (nepřímá identifikace). Z výše uvedeného vyplývá, že subjekt údajů nemusí být identifikován pouze jménem, příjmením a adresou (přímá identifikace). Jakákoliv jiná kombinace informací, která umožní odlišit od sebe jednotlivé fyzické osoby (subjekty údajů), musí být považována také za identifikaci subjektu údajů.

Podle zjištění Úřadu pro ochranu osobních údajů učiněných v průběhu kontroly byla anonymizace osobních údajů dětí, žáků a studentů prováděna tak, že jednostranným algoritmem bylo zakódováno rodné číslo tak, aby v samotném datovém souboru nebylo možno na první pohled rozpoznat, o kterého žáka se jedná. Kódování používané účastníkem řízení je ovšem stále stejné, tak aby bylo možno každý rok přidávat další informace ke konkrétnímu žákovi (subjektu údajů). Subjekt údajů je pouze místo pod rodným číslem veden pod jiným číslem, do kterého je rodné číslo zakódováno, tedy pod jiným jedinečným „agendovým“ identifikátorem, což může nepochybně potenciálně vést k určení, o jaké dítě se konkrétně jedná. Nelze tedy hovořit o tom, že zpracovávané osobní údaje byly anonymizovány, naopak databáze vedená Ústavem tedy splňuje náležitosti databáze osobních údajů ve smyslu shora citovaného ustanovení § 4 písm. a) zákona č. 101/2000 Sb. Argumentaci účastníka řízení nelze přijmout také proto, že i podle dřívějších vyjádření samotného účastníka řízení byla předmětná databáze zřízena mj. pro mapování průchodnosti českého vzdělávacího systému, kdy je nutné mít k dispozici individuální údaje o žácích a studentech minimálně po dobu průchodu jedince počátečním vzděláváním v regionálním školství a po dobu možného dalšího vzdělání realizovaného v institucích regionálního školství (rekvalifikace, doplňování vzdělávání, vstup na vysokou školu a konání jednotlivé maturitní zkoušky); z povahy věci se tedy nemohlo jednat o údaje anonymní.

Na tomto místě je třeba podotknout, že zpracování osobních údajů bez souhlasu subjektu údajů je třeba vnímat jako zásah do práva na ochranu soukromého život ve smyslu čl. 10 Listiny základních práv a svobod a především čl. 8. Úmluvy o ochraně lidských práv a základních svobod (sdělení federálního ministerstva zahraničních věcí č. 209/1992 Sb., dále jen „EÚLP“). Ustanovení § 5 odst. 2 písm. a) zákona č. 101/2000 Sb. je promítnutím čl. 7 písm. c) směrnice Evropského parlamentu a Rady č. 95/46/ES ze dne 24. října 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů; k výkladu tohoto článku se vyjádřil Evropský soudní dvůr v rozsudku č. C-456/00 ze dne 20. května 2003 (Österreichischer Rundfunk a další; §§ 66-78). Při výkladu právní povinnosti přitom uvedl, že je třeba poměřovat, zda tato právní povinnost stanoví zásah do soukromí a zda je tento odůvodněný ve vztahu k čl. 8 EÚLP. Tento zásah je ospravedlnitelný, pokud je stanoven zákonem, sleduje jeden nebo několik legitimních cílů stanovených v odstavci 2 čl. 8 EÚLP a je nezbytný v demokratické společnosti pro dosažení tohoto nebo těchto cílů. Jedním z požadavků ve vztahu k zásahu do soukromí tedy je, aby zákon, resp. právní norma a její výklad, zněl dostatečně přesně, aby umožnil adresátům zákona řídit jejich chování a odpovídal tak požadavku předvídatelnosti stanoveném judikaturou Evropského soudu pro lidská práva (viz zejména rozsudek Evropského soudu pro lidská práva ve věci Rekvényi v. Maďarsko ze dne 20. května 1999, § 34). Proto je třeba i z uvedeného hlediska vykládat ustanovení § 28 odst. 5 zákona č. 561/2004 Sb., které dle správního orgánu obsahuje zmocnění ke zpracování osobních údajů pro statistické účely v tom smyslu, co tento pojem znamená, tedy k vytvoření statistických informací. K otázce, zda pojem statistické zpracování zahrnuje i tvorbu časových řad, tedy i zpracování osobních údajů po dobu delší než jeden rok, správní orgán s odkazem na shora uvedené konstatuje, že z hlediska požadavků čl. 8 odst. 2 EÚLP („nezbytné v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, předcházení nepokojům a zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných“) rozhodně nepovažuje tvorbu časových řad umožňujících sledovat průběh studijního života na úrovni účastníka řízení za v demokratické společnosti nezbytné opatření; je ostatně otázkou, k jakému předvídanému účelu by měl takový zásah do soukromého života sloužit.

Správní orgán je tedy toho názoru, že při absenci výslovného zákonného zmocnění účastníka řízení (jehož případnou ústavnost, resp. soulad s EÚLP by byly oprávněny přezkoumávat pouze k tomu příslušné soudy) k tvorbě časových řad vypovídajících o studijním životu subjektu údajů, je třeba vykládat zmocnění ke statistickým účelům a především odkaz na jiné právní povinnosti co nejúžeji, tedy pouze jako oprávnění k (bezodkladnému) vytvoření statistických informací (tj. agregovaných dat). V této souvislosti shledává správní orgán jako mnohem významnější veřejný zájem právo každého na ochranu soukromého života (tedy pokud možno co nejmenší shromažďování osobních údajů ze strany veřejné moci, volba alternativních metod k dosažení stanovených cílů, používání anonymních údajů, a to i v případech, kdy použití osobních údajů by bylo cestou snazší) před účastníkem řízení tvrzeným veřejným zájmem obhajujícím jeho dosavadní postup. Ve vztahu k jiným právním povinnostem ve smyslu § 28 odst. 5 zákona č. 561/2004 Sb., které účastník řízení dovozuje ze svých kompetencí a povinností podle zákona č. 561/2004 Sb., resp. dokonce podle zákona č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky, lze ve smyslu shora uvedených principů konstatovat, že takovýto odkaz by zakládal oprávnění zpracovávat osobní údaje bez souhlasu subjektu údajů pouze v případě, kdy by stanovoval jednoznačný účel zpracování a rozsah zpracovávaných údajů; ad absurdum by bylo možné argumentovat, že za účelem ochrany osobních údajů, které je v kompetenci správního orgánu (Úřadu pro ochranu osobních údajů) by tento měl zpracovávat veškeré osobní údaje, jejichž zpracování probíhá na území České republiky, (tj. osobní údaje ze všech smluv, ze všech úředních evidencí apod.), proto, aby mohl řádně plnit svoje povinnosti; ministerstvo zdravotnictví by zase mělo zpracovávat osobní údaje všech nemocných atd. Správní orgán je tedy toho názoru, že všechny účastníkem řízení uváděné povinnosti, kterými odůvodňuje potřebnost zpracovávat osobní údaje způsobem vedoucím ke tvorbě časových řad vypovídajících o průběhu studijního života, je možné splnit na základě statistických informací, tj. souhrnných, agregovaných dat. Závěrem k této otázce lze konstatovat, že dle správního orgánu v případě, kdy má právní norma představovat zásah do základních práv a svobod konkrétní fyzické osoby, je nezbytné, aby byla formulována co nejpřesněji, a rozhodně je třeba odmítnout rozšiřování jejího dopadu pomocí teleologického výkladu odkazujícího na důvodovou zprávu k zákonu (zejména, pokud je jejím autorem sám účastník řízení). (čj. *SPR-2298/10*)

Poznámky:

[1)] Za jednotlivými texty, které jsou rozděleny do tematických okruhů, jsou vždy kurzívou uvedena interní čj., pod kterými jsou jednotlivé případy v Úřadu evidovány.

[2)] Materiál je také k dispozici na internetové adrese Úřadu www.uoou.cz v sekci Dozorová činnost v rubrice Správní delikty/Z rozhodovací činnosti.

Stanovisko Úřadu pro ochranu osobních údajů k Návrhu směrnice Evropského parlamentu a Rady o používání údajů jmenné evidence cestujících pro prevenci, odhalování, vyšetřování a stíhání teroristických činů a závažné trestné činnosti

Sdělení úvodem:
Níže uvedený materiál byl dne 9. března 2011 odeslán Senátu Parlamentu ČR a Poslanecké sněmovně Parlamentu ČR. Oproti odeslanému materiálu jsou vysvětleny v textu se vyskytující zkratky.

Vzhledem k závažnosti dopadů chystaného opatření do práva na ochranu soukromí a s ohledem na skutečnost, že Odbor bezpečnostní politiky MV nezohlednil ve své Rámcové pozici pro Parlament všechny připomínky Úřadu pro ochranu osobních údajů (dále jen Úřad) – především zásadní kritiku nedostatečného prokázání účelnosti a nezbytnosti předávání PNR dat –, vypracoval Úřad vlastní pozici, která se snaží objasnit, jak navrhované opatření zasáhne do základních práv a svobod velkého počtu občanů EU.

Návrh směrnice vychází z předchozího návrhu rámcového rozhodnutí o využívání údajů jmenné evidence cestujících (dále jen „PNR data" nebo „údaje PNR") pro účely vymáhání práva, který dne 6. listopadu 2007 Komise přijala. Po 1. prosinci 2009, kdy vstoupila v platnost Smlouva o fungování Evropské unie (Lisabonská smlouva), však dokument zastaral. Komise tak přišla s novým návrhem, tentokrát ve formě směrnice. Tento dokument má zakotvit povinnost předávat údaje o **všech** cestujících na letech přes hranice EU, tedy těch, které směřují ze států mimo Evropskou unii do členských států a naopak, do databáze, kterou má spravovat k tomu účelu v každém členském státě nebo centrálně zřízený útvar pro informace o cestujících (Passenger Information Unit, dále jen PIU). V některých státech EU, zejména ve Velké Británii, sílí tlak na rozšíření působnosti směrnice rovněž na lety mezi jednotlivými zeměmi EU (vnitrounijní lety).

A/ OBECNÁ VÝCHODISKA

1. **Úřad je přesvědčen, že dosud nebyla uspokojivě prokázána především účelnost a nezbytnost navrhovaného řešení, jak to vyžaduje čl. 8 Evropské úmluvy o lidských právech a čl. 52 Listiny základních práv EU**, který v odst. 1 stanoví: „Každé omezení výkonu práv a svobod uznaných touto listinou musí být stanoveno zákonem a respektovat podstatu těchto práv a svobod. Při dodržení zásady proporcionality mohou být omezení zavedena pouze tehdy, pokud jsou nezbytná a pokud skutečně odpovídají cílům obecného zájmu, které uznává Unie, nebo potřebě ochrany práv a svobod druhého". Před zavedením takového systému je nutné provést test proporcionality tj. zvážit alternativní možnosti s ohledem na rušivou povahu rozhodnutí (signalizujících podezření na jednání určitých osob), přijímaných automaticky podle nastavených kritérií, a vzhledem k potížím fyzických osob vznést námitky vůči těmto rozhodnutím.

   Bez prokázání nezbytnosti nového opatření agresivně zasahujícího do oblasti soukromí a ochrany osobních údajů tedy nestačí pouze tvrzení (i tak ne zcela prokázané) o využitelnosti či užitečnosti pro deklarované účely boje proti terorismu a závažné trestné činnosti. Dosud nebylo vyhodnoceno, kolika lidí se PNR systém dotýká, kolik z těchto lidí PNR systém vyhodnotil jako potenciální podezřelé ze spáchání zločinu (a jakých zločinů), kolik z těchto podezřelých skutečně předpokládaný zločin spáchalo a kolik těchto spáchaných zločinů by bez použití PNR systému zůstalo neodhaleno. Až takové vyhodnocení umožní kvalifikovanou odpověď na otázku, zda v rámci zpracování PNR dat bude zachována rovnováha mezi právy nevinných cestujících a stanoveným účelem prevence a stíhání terorismu a závažné trestné činnosti. Užitečnost takového zpracování se navíc zdůvodňuje bez dostatečného posouzení možného využití již existujících databází (Schengenský informační systém (SIS), Vízový informační systém (VIS), Předběžné informace o cestujících (API), databáze Europolu a další) pro naplnění stanoveného účelu.

   Považujeme dále za nutné připomenout, že myšlenka shromažďovat PNR data původně vznikla a byla uskutečněna v USA po událostech 11. září 2001. Nyní se kontext přesouvá k obecnému zpracování pro různé a mnohem širší bezpečnostní účely.

2. **Názor uvedený v bodě 1. vůbec není ojedinělý. Rozhodně by měly být vzaty v úvahu např. postoje:**

   Evropského parlamentu vyjádřené v usnesení z listopadu 2008 poukazujícím na nedostatečně prokázanou potřebu navrhovaných opatření,

   Pracovní skupiny pro ochranu dat podle článku 29 směrnice 95/46/ES (tzv. WP29, tedy poradního orgánu Komise složeného z předsedů dozorových orgánů typu Úřadu pro ochranu osobních údajů), která v dokumentech WP 145 a WP 178 kritizuje mj. nedostatečně prokázanou účelnost využití údajů PNR donucovacími orgány a nepřiměřenost navrhovaných opatření,

Evropského inspektora ochrany údajů kritizujícího ve stanovisku z 19. října 2010 neprokázanost nezbytnosti a přiměřenosti návrhu a skutečnost, že opatření přispívá ke „společnosti pod dohledem“,

Senátu Parlamentu ČR, který v usnesení 370 z 23. dubna 2008 v reakci na příslušný návrh rámcového rozhodnutí Rady poukázal na to, že státy, které tato data sbírají, doposud neprokázaly efektivnost PNR v boji proti terorismu a organizovanému zločinu a dále také vyjádřil názor, že doba uchovávání a rozsah sbíraných dat jsou nepřiměřené. Vládě doporučil zaujmout k návrhu negativní stanovisko a požádal ji, aby jej informovala o způsobu, jakým stanovisko Senátu zohlednila.

3. **Analýza údajů o všech cestujících, jak předpokládá návrh směrnice, se jeví být v rozporu s Ústavou ČR.** Právo na ochranu soukromého a rodinného života, jakož i právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě jsou chráněna článkem 10 Listiny základních práv a svobod. Státní moc lze v souladu s čl. 2 odst. 3 zákona č. 1/1993 Sb. (Ústava ČR) a čl. 2 odst. 2 Listiny základních práv a svobod uplatňovat jen v případech, v mezích a způsoby, které stanoví zákon.

   Zavedení systému sběru dat PNR v EU a z něj plynoucí zásah do soukromí lze akceptovat jen, pokud existuje zájem vyšší ochrany jiného základního lidského práva nebo svobody. Aby mohla být dána přednost ochraně jiného ústavního práva před ochranou soukromí, je třeba postupovat dle „receptu“ uvedeného v rozhodnutí Ústavního soudu České republiky Pl. ÚS 4/94, tedy posoudit, zda v dané situaci je ochrana jiného základního práva nebo svobody natolik závažná (důvodná) a toto právo natolik ohroženo, že je rozumné akceptovat zásah do soukromí, a částečně tak omezit základní lidské právo na soukromý a rodinný život. Hodnotící proces podle receptu Ústavního soudu musí obsahovat následující kritéria (a systém PNR by tedy měl být):

   – prokazatelně vhodný k vyřešení daného problému,
   – prokazatelně nezbytný k řešení daného problému,
   – proporcionální vůči jeho přínosu pro bezpečnost,
   – do soukromí osob zasahující prokazatelně méně, než alternativní opatření,
   – pravidelně podrobován přezkumu, aby se zaručilo, že jsou daná opatření stále přiměřená.

4. **Nebyly dostatečně zváženy důsledky reciprocity.** Evropský režim PNR by mohl být důvodem k tomu, aby obdobné požadavky vznesly na základě vzájemnosti také nedemokratické a zkorumpované státy (neposkytující dostatečné záruky ochrany základních práv a svobod, včetně osobních údajů). PNR data v moci těchto států by mohla představovat vážný problém.

5. **Dosud nebylo prokázáno, že při boji proti terorismu a závažné trestné činnosti je nutné využívat i jiné údaje než údaje API.** Na rozdíl od údajů API nejsou údaje PNR ověřené a musejí být považovány za nespolehlivé. V rámci zajištění Evropského prostoru svobody, bezpečnosti a spravedlnosti ve vztahu ke Stockholmskému programu je možné zvažovat i jiná opatření, která by zajistila dosažení stejných cílů za využití stávajících nástrojů, např. využití povinnosti leteckých dopravců předávat API data nejen za účelem boje s imigrací, ale také za účely vnitřní bezpečnosti a vynucování práva. Tato možnost však nebyla vůbec vzata v potaz.

B/ KOMENTÁŘ K NĚKTERÝM DÍLČÍM ASPEKTŮM NÁVRHU SMĚRNICE A RÁMCOVÉ POZICE ČR

1. **Jak již bylo řečeno úvodem, návrh směrnice počítá se zahrnutím „pouze“ letů přes hranice EU, nicméně připouští diskusi o rozšíření působnosti i na lety vnitrounijní.** Úřad je jednoznačně proti tomuto širšímu řešení, při kterém by došlo k mnohonásobnému nárůstu sledovaných údajů o cestujících, do jejichž soukromí by bylo zasahováno, se všemi důsledky na další disproporcionalitu, nevyváženost a neprůkaznou účinnost tohoto opatření, o jeho nákladnosti nemluvě. Konstatování v návrhu rámcové pozice, že ČR nebude rozšíření iniciovat, že však nebude proti, pokud s návrhem přijde některý jiný členský stát, se nám jeví jako vrcholně alibistické a demagogické. Předkladatelé návrhu rámcové pozice dobře vědí, že řada (byť menšina) států již v minulosti s takovým návrhem přišla a v současné době jej již konkrétně předložila Velká Británie. Navrhujeme proto v pozici ČR jednoznačně odmítnout možnost rozšíření na vnitrounijní lety.

2. **K otázce zřízení útvarů PIU**, kde by se údaje podle určitých kritérií vyhodnocovaly a které by v jednotlivých odůvodněných případech poskytovaly údaje pro směrnicí stanovené účely, zastáváme jednoznačné stanovisko, že by mělo jít o entity zřízené a fungující na základě speciálních zákonných pravidel. V žádném případě by nemělo jít o orgány v rámci stávajících struktur např. policie, MV apod., které by se vedle obecných zásad daných směrnicí řídily pouze interními předpisy národních orgánů vynucujících zákon. Z tohoto hlediska by tedy nemělo být ponecháno na volbě na národní úrovni, zda zahrnout nebo nezahrnout PIU do stávajících struktur, protože vzhledem k předpokládané výměně dat mezi státy a PIU centry je problém rizikovosti v oblasti soukromí a ochrany dat záležitostí sdílenou.

3. **Je sporné, zda očekávaná účinnost bude proporcionální nejen z hlediska významného zásahu do soukromí, ale také ve vztahu k finančním nákladům**

a administrativní zátěži, které vzniknou jednak na straně leteckých dopravců a jednak na straně veřejné správy, která bude muset PIU vybavit softwarem, hardwarem a kvalifikovanými pracovníky. Otázkou zůstává, kdo by hradil vstupní náklady dopravců na zavedení EU PNR push systému (systému, v němž by PNR data předávaly samy letecké společnosti) a roční náklady dopravců.

K odhadům nákladů uvádí Komise v dokumentu Hodnocení dopadů zpracování PNR následující čísla:

Náklady na straně dopravce na zasílání PNR dat v push režimu se odhadují ve výši 0,04 eur na jednoho cestujícího. Vstupní náklad veřejné správy velkého členského státu (hardware a software, odhad na základě odhadu Velké Británie) – 75 000 000 eur,

Roční náklad veřejné správy velkého členského státu (zaměstnanci, odhad na základě odhadu Velké Británie) – 11 500 000 eur.

4. **Rozsah sbíraných dat se s ohledem na zásadu přiměřenosti jeví jako nadměrný**. Rozsah osobních údajů musí být zpracováván s přihlédnutím ke konkrétnímu účelu. Např. boj proti terorismu nebude nutně vyžadovat stejné údaje a nebude mít za následek stejnou rovnováhu práv a zájmů jako např. boj proti pašování drog.

5. **Doba uchovávání 5 let, byť v pseudoanonymizované (maskované) podobě, je nepřiměřená**, jak ve vztahu k ochraně cestujících, tak ve vztahu k vyšetřování závažné trestné činnosti.

6. **Úřad považuje za nutné vyjádřit se rovněž k Hodnocení dopadu zpracování PNR (Impact Assessment), který tvoří doprovodný materiál Komise k návrhu směrnice.** Je nutné konstatovat, že ani tento materiál vypracovaný Komisí neprokázal nezbytnost zavedení EU PNR. Kapitola 3.2 materiálu nazvaná „Dodržení základních práv" nikterak neprokázala nezbytnost EU-PNR systému. V prvním odstavci tato kapitola pouze konstatovala, že při hodnocení byl použit „Check List" vytvořený Komisí pro efektivní implementaci Listiny základních práv [COM (2010)573 z 19. října 2010], aniž byly uvedeny jakékoliv podrobnosti hodnocení. V závěru třetího odstavce pak tato kapitola přináší následující důkaz nezbytnosti EU-PNR systému, jde však evidentně o chybný důkaz kruhem: Podle materiálu je právní podmínkou umožňující zásah do práva na ochranu údajů (definovanou v čl. 52 Listiny základních práv EU) to, že takový zásah bude nezbytný pro předcházení trestné činnosti. Účelem EU-PNR systému je předcházení terorismu a závažné trestné činnosti, a proto je jasně v souladu s touto právní podmínkou. Takto formulovaná věta však žádným způsobem neprokazuje **nezbytnost a přiměřenost** systému.

Stále zůstává nedořešena otázka, zda stávající formy policejní a justiční spolupráce, zaměřené na předcházení a stíhání trestných činů, kam patří i boj proti terorismu a závažné trestné činnosti, ve stávající podobě (Europol a další formy spolupráce), s využitím systémů typu SIS, dostatečné nástroje k dosažení účelu, kterého má být zavedením systému EU PNR dosaženo. Hodnocení dopadu naopak výslovně připouští, že povinné zavedení zpracování PNR dat všemi členskými státy v důsledku nanejvýš pouze změní způsob dopravy používaný teroristy.

Námořní a pozemní hranice EU nebudou chráněny prostřednictvím zpracování PNR dat, takže zůstane vysoká pravděpodobnost, že teroristé a zločinci využijí těchto cest, ba dokonce existuje riziko, že po zavedení EU PNR se tato pravděpodobnost zvýší, takže efektivita užívání PNR dat se sníží. Tento fakt výslovně připouští i Komise v uvedeném dokumentu. Komise však tuto námitku přechází bez dalšího argumentu tvrzením, že přes toto riziko užívání PNR dat zajistí zvýšení bezpečnosti v EU a bude dostatečným nástrojem identifikace potenciálních dosud neznámých podezřelých osob usilujících o vstup do EU a umožní analýzu a vytváření předem daných kritérií podezřelosti, na jejichž základě budou tipováni tito dosud neznámí podezřelí.

Závěr

Ani Důvodová zpráva, ani obšírné Hodnocení dopadu zpracování PNR dat tedy **neprokázaly**, že zpracování PNR dat:

1. Může zásadním způsobem přispět k boji proti terorismu a závažnému zločinu;
2. Je nezbytné;
3. Jeho přínosy převáží nad zásahem do soukromí cestujících.

Poznámka:
Materiál je také k dispozici na internetové adrese Úřadu www.uoou.cz v sekci Názory Úřadu/Na aktuální téma.

Doporučení CM/Rec (2010) 13 Výboru ministrů členským státům o ochraně osob s ohledem na automatizované zpracování osobních údajů v souvislosti s profilováním[1]

(Schváleno Výborem ministrů 23. listopadu 2010 na 1099. zasedání ministerských zástupců)

Výbor ministrů,

maje na zřeteli, že cílem Rady Evropy je dosažení větší jednoty mezi jejími členy;

bera na vědomí, že informační a komunikační technologie (IT) umožňují shromažďování a zpracování velkého množství dat, včetně osobních údajů v soukromém i veřejném sektoru; bera na vědomí, že IT mají široké spektrum využití, včetně služeb obecně přijímaných a ceněných společností, spotřebiteli i v hospodářské oblasti; a současně vědom si toho, že neustálý rozvoj v technologii spojů přináší nové problémy při shromažďování a dalším zpracování dat;

bera na vědomí, že ke shromažďování a zpracování může docházet v různých situacích a pro různé účely a může se týkat různých druhů dat, jako například údajů cestovních, informací o internetovém vyhledávání uživatele, o nákupních zvycích spotřebitele, o aktivitách, životním stylu a o chování uživatelů telekomunikačních zařízení, včetně geolokalizačních dat, stejně jako mohou být shromažďovány údaje pocházející ze sociálních sítí, kamerových systémů, systémů využívajících biometriku a radiofrekvenční identifikaci (RFID), které předznamenávají příchod „internetu věcí“;

bera na vědomí, že je žádoucí hodnotit rozdílné situace a účely odlišným způsobem;

bera na vědomí, že takto shromážděné údaje se zpracovávají počítačově, porovnávají a statisticky vyhodnocují s cílem vytvořit profily, které díky porovnání údajů několika jednotlivců mohou mnoha způsoby sloužit nejrůznějším účelům a pro různé využití; bera na vědomí, že rozvoj IT umožňuje provedení těchto úkonů při poměrně nízkých nákladech;

maje na zřeteli, že tímto propojováním velkého počtu individuálních, i když anonymních, poznatků může mít technika profilování dopad na příslušné osoby tím, že je zařazuje, často bez jejich vědomí, do předem definovaných kategorií;

maje na zřeteli, že profily přiřazené subjektu údajů umožňují generovat nové osobní údaje, jež ale nejsou těmi, které subjekt údajů správci sdělil, nebo o nichž mohl odůvodněně předpokládat, že budou správci známy;

maje na zřeteli, že nedostatek transparentnosti, či dokonce „neviditelnost“ profilování, a nedostatek přesnosti, který může vyplývat z automatického užívání přednastavených vyhodnocovacích pravidel, mohou představovat vážná rizika pro práva a svobody jednotlivce;

maje zejména na zřeteli, že ochrana základních práv, především práva na soukromí a ochranu osobních údajů, zahrnuje různé a samostatné oblasti života, v nichž každý jednotlivec (subjekt údajů) může kontrolovat, jakým způsobem je nakládáno s jeho identitou;

maje na zřeteli, že profilování může být v legitimním zájmu jak osoby, která ho využívá, tak i osoby, které se týká, například tím, že vede k lepší segmentaci trhu, umožňuje analýzu rizik a podvodů, nebo přizpůsobuje nabídku poptávce poskytováním lepších služeb; maje také na zřeteli, že profilování tak může přinášet prospěch uživatelům, ekonomice i celé společnosti;

maje však také na zřeteli, že profilování může v důsledku znamenat neoprávněné zamezení přístupu jednotlivce (subjektu údajů) k určitému zboží nebo službám, a tím k porušení zásady nediskriminace;

maje dále na zřeteli, že techniky profilování, které zdůrazňují vzájemný vztah mezi citlivými údaji ve smyslu článku 6 Úmluvy Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních dat (ETS č. 108, dále jen „Úmluva č. 108“) a jinými osobními údaji, mohou umožnit vygenerování nových citlivých údajů týkajících se identifikované nebo identifikovatelné osoby; maje dále na zřeteli, že takové profilování může vystavit jednotlivce velmi vysokému riziku diskriminace a útoků na jeho osobní práva a důstojnost;

maje na zřeteli, že profilování dětí může pro ně mít závažné důsledky během jejich dalšího života, a vzhledem k tomu, že samy nejsou schopny poskytnout svobodný, vědomý a informovaný souhlas ve věci shromažďování svých osobních údajů pro účely profilování, jsou pro ochranu dětí nutná specifická a odpovídající opatření učiněná v jejich nejlepším zájmu a se zřetelem na rozvoj dětské osobnosti v souladu s Úmluvou o právech dítěte Organizace spojených národů;

maje na zřeteli, že používání profilů, i zákonným způsobem, by bez preventivních a specifických ochranných opatření mohlo vážně poškodit lidskou důstojnost, stejně jako další základní práva a svobody, včetně práv ekonomických a sociálních;

přesvědčeni, že je proto nezbytné regulovat profilování s ohledem na ochranu osobních údajů, aby byla chráněna

základní práva a svobody jednotlivců, zejména právo na soukromí, a zabránilo se diskriminaci na základě pohlaví, rasového a etnického původu, náboženství nebo jiného přesvědčení, zdravotního postižení, věku nebo sexuální orientace;

připomínaje v tomto ohledu všeobecné zásady o ochraně údajů v Úmluvě č. 108;

připomínaje, že každá osoba má mít právo na přístup k údajům, které se jí týkají, a maje na zřeteli, že každá osoba by měla znát metodu užitou při profilování; přičemž by toto právo nemělo mít dopad na práva a svobody ostatních, a zejména by nemělo nepříznivě ovlivnit obchodní tajemství, duševní vlastnictví nebo autorské právo chránící příslušný software;

připomínaje nezbytnost shody s již existujícími zásadami stanovenými v dalších souvisejících doporučeních Rady Evropy, především v Doporučení Rec(2002)9 o ochraně osobních údajů shromažďovaných a zpracovávaných pro účely pojištění a Doporučením Rec(97)18 o ochraně osobních údajů shromažďovaných a zpracovávaných pro statistické účely;

s ohledem na Úmluvu Rady Evropy o počítačové kriminalitě (ETS No. 185 – Budapešťská úmluva), která obsahuje nařízení o uchovávání, shromažďování a výměně dat, jež obsahuje podmínky a záruky přijaté v zájmu odpovídající ochrany lidských práv a svobod; s ohledem na článek 8 Evropské úmluvy o lidských právech (ETS No. 5), jak byl vyložen Evropským soudem pro lidská práva, a na nová rizika vytvořená užíváním informačních a komunikačních technologií;

maje na zřeteli, že ochrana lidské důstojnosti a dalších základních práv a svobod v kontextu profilování může být účinná pouze a jen tehdy, pokud všechny zainteresované strany společně přispějí ke korektnímu a zákonnému profilování jednotlivců;

s ohledem na to, že mobilita jednotlivců, globalizace trhů a využívání nových technologií vyvolávají potřebu přeshraniční výměny informací, a to i v oblasti profilování, a vyžadují srovnatelnou ochranu údajů ve všech členských státech Rady Evropy,

doporučuje, aby vlády členských států:

1. Použily dodatek tohoto doporučení při shromažďování a zpracovávání osobních údajů použitých v kontextu profilování a zejména přijaly taková opatření, která zajistí, aby se zásady stanovené v dodatku k tomuto doporučení promítly do jejich zákonů a praxe;
2. Zajistily šíření zásad stanovených v dodatku k tomuto doporučení mezi osobami, správními orgány a veřejnými nebo soukromými institucemi, především těmi, které se podílejí na profilování a používají je, například tvůrci a dodavatelé softwaru, tvůrci profilů, poskytovatelé elektronických komunikačních služeb a poskytovatelé služeb informační společnosti, jakož i mezi orgány odpovědnými za ochranu dat a mezi normalizačními institucemi,
3. Vybízely tyto osoby, správní orgány a veřejné nebo soukromé instituce k zavádění a podpoře samoregulačních mechanismů jako jsou kodexy chování zajišťující respekt k ochraně soukromí a dat, a k zavádění technologií popsaných v dodatku k tomuto doporučení.

Dodatek k Doporučení č. CM/Rec(2010)13

1. Definice

Pro účely tohoto doporučení:

a) „Osobním údajem“ se rozumí jakákoli informace vztahující se k určenému nebo určitelnému jednotlivci („subjektu údajů“). Jednotlivec není považován za „identifikovatelného“, pokud zjištění jeho totožnosti vyžaduje nepřiměřené množství času nebo úsilí.

b) „Citlivým údajem“ se rozumí osobní údaj vypovídající o rasovém původu, politických názorech, náboženském nebo jiném přesvědčení, jakož i osobní údaje týkající se zdraví, sexuálního života nebo odsouzení za trestný čin, stejně jako další údaje definované vnitrostátním právem jako citlivé.

c) „Zpracováním“ se rozumí jakákoli operace nebo soustava operací vykonávaných částečně nebo zcela pomocí automatizovaných procesů a prováděných s osobními údaji, jako například ukládání, uchovávání, úprava nebo změna, vyjímání, nahlížení, používání, sdělování, porovnávání nebo propojování, stejně jako vymazávání nebo likvidace.

d) „Profilem“ se odkazuje na soubor údajů charakterizující určitou kategorii osob s úmyslem tuto kategorii vztahovat na jednotlivce.

e) „Profilováním“ se rozumí technika automatizovaného zpracování údajů, která spočívá v použití „profilu“ na jednotlivce, zejména za účelem činit o dané osobě rozhodnutí nebo analyzovat či předvídat její osobní preference, chování nebo postoje.

f) „Službou informační společnosti“ se rozumí jakákoliv služba poskytovaná na dálku elektronickými prostředky, a to zpravidla za úplatu.

g) „Správcem“ se rozumí fyzická nebo právnická osoba, správní orgán, agentura nebo jakýkoli jiný subjekt, který sám nebo ve spolupráci s jinými určuje účely a prostředky používané při shromažďování a zpracovávání osobních údajů.

h) „Zpracovatelem“ se rozumí fyzická nebo právnická osoba, správní orgán, agentura nebo jakýkoli jiný subjekt, který zpracovává osobní údaje jménem správce.

2. Obecné zásady

2.1. Při shromažďování a zpracovávání osobních údajů podle tohoto doporučení musí být zaručeno dodržování základních práv a svobod, zejména práva na soukromí a zásady nediskriminace.

2.2. Členské státy by měly podporovat navrhování a zavádění postupů a systémů v souladu s ochranou soukromí a dat již ve fázi plánování, zejména cestou technologií zvyšujících ochranu soukromí. Také by měly přijmout odpovídající opatření proti vývoji a využití technologií určených plně nebo částečně k nezákonnému obcházení technických opatření pro ochranu soukromí.

3. Podmínky shromažďování a zpracovávání osobních údajů v souvislosti s profilováním

A. Zákonnost

3.1. Shromažďování a zpracovávání osobních údajů v kontextu profilování by mělo být korektní, zákonné a přiměřené, za konkrétním a legitimním účelem.

3.2. Osobní údaje použité v kontextu profilování by měly být přiměřené, měly by se týkat účelů stanovených pro jejich shromažďování a zpracování a tyto účely by neměly překračovat.

3.3. Osobní údaje použité v kontextu profilování by měly být uchovávány ve formě, která neumožňuje identifikaci subjektů údajů po dobu delší, než je nutné pro účely, pro které jsou údaje shromažďovány a zpracovávány.

3.4. Shromažďování a zpracovávání osobních údajů v kontextu profilování může být prováděno pouze:

a) pokud je upraveno zákonem; nebo

b) pokud je povoleno zákonem a

- subjekt údajů nebo jeho zákonný zástupce poskytl svobodný, konkrétní a informovaný souhlas;
- je nutné pro plnění smlouvy, u které je subjekt údajů smluvní stranou, nebo pro zavedení předsmluvních opatření učiněných na žádost subjektu údajů;
- je nutné pro plnění úkolů konaných ve veřejném zájmu nebo při výkonu úředních pravomocí udělených správci nebo třetí straně, které jsou osobní údaje zpřístupňovány;
- je nutné pro účely legitimních zájmů správce nebo třetí strany nebo stran, kterým jsou profily nebo údaje poskytovány, kromě případů, kdy jsou těmto zájmům nadřazena základní práva a svobody subjektů údajů;
- je v životním zájmu subjektu údajů.

3.5. Shromažďování a zpracovávání osobních údajů v souvislosti s profilováním osob, které nemohou samy vyjádřit svůj svobodný, konkrétní a informovaný souhlas, by mělo být zakázáno, kromě případů, kdy je to v oprávněném zájmu subjektu údajů, nebo pokud je zde nadřazený veřejný zájem, pod podmínkou, že zákon stanoví příslušná ochranná opatření.

3.6. Je-li požadován souhlas, je povinností správce prokázat, že subjekt údajů souhlasil s profilováním a to v souladu se zásadami informovaného souhlasu definovaného v části 4.

3.7. V nejvyšší možné míře a nevyžaduje-li požadovaná služba znalost totožnosti subjektu údajů, by měl mít každý přístup k informacím o zboží nebo službách nebo přímo k tomuto zboží a službám, aniž by musel sdělovat osobní údaje poskytovateli tohoto zboží nebo těchto služeb. Aby byl zajištěn svobodný, konkrétní a informovaný souhlas s profilováním, měli by poskytovatelé služeb informační společnosti zajistit standardní neprofilovaný přístup k informacím o svých službách.

3.8. V kontextu s profilováním by šíření a využití softwaru zaměřeného na pozorování nebo monitorování toho, jaké je využití příslušného terminálu nebo elektronické komunikační sítě, mělo být povoleno bez vědomí subjektu údajů pouze v případě, kdy to výslovně upravuje vnitrostátní právo a za příslušných ochranných opatření.

B. Kvalita údajů

3.9. Správce by měl učinit vhodná opatření, aby napravil faktory způsobující nepřesnost údajů a omezil riziko chyb způsobených profilováním.

3.10. Správce by měl pravidelně a v přiměřeném časovém úseku hodnotit jak kvalitu dat, tak důsledky z těchto dat vyvozované.

C. Citlivé údaje

3.11. Shromažďování a zpracovávání citlivých údajů v souvislosti s profilováním je zakázáno kromě případů, kdy jsou tyto údaje nutné pro zákonné a konkrétní účely zpracování, a pokud vnitrostátní právo poskytuje odpovídající ochranná opatření. Je-li vyžadován souhlas, mělo by být explicitně uvedeno, zda se zpracování týká i citlivých údajů.

4. Informace

4.1. V případě, že jsou v kontextu profilování shromažďovány osobní údaje, správce by měl subjektům údajů poskytnout následující informace:

a) o skutečnosti, že jejich údaje budou použity v souvislosti s profilováním;

b) o účelu, pro který je profilování prováděno;

c) o kategoriích použitých osobních údajů;

d) o totožnosti správce a, v případě nutnosti, jeho zástupce;

e) o existenci odpovídajících ochranných opatření;

f) o potřebném zajištění korektního profilování, jako například:

- o kategoriích osob nebo orgánů, kterým mohou být osobní údaje sděleny a za jakým účelem;

- o možnosti subjektů údajů odmítnout v určitých případech poskytnutí souhlasu, nebo o možnosti jeho odvolání, i o důsledcích odvolání;
- o podmínkách pro uplatňování práva na přístup, námitku nebo opravu, jakož i o právu podat stížnost odpovědným orgánům;
- o osobách nebo orgánech, od nichž budou osobní údaje získávány;
- o tom, zda je odpověď na otázku týkající se osobních údajů povinná nebo dobrovolná a jaký je důsledek toho, když nebude poskytnuta;
- o době uchovávání údajů;
- o předpokládaném důsledku přiřazení profilu subjektu údajů.

4.2. V případě, že bude probíhat sběr osobních údajů od subjektu osobních údajů, správce mu poskytne informace v souladu s výčtem uvedeným pod 4.1, nejpozději však v době, kdy probíhá sběr osobních údajů.

4.3. V případě, že sběr osobních údajů neprobíhá od subjektů osobních údajů, správce poskytne subjektům údajů informaci ve výčtu pod 4.1 ve chvíli, kdy jsou údaje zaznamenány nebo pokud má dojít ke sdělení osobních údajů třetí straně, nejpozději v okamžiku, kdy jsou osobní údaje třetí straně poprvé sděleny.

4.4. V případě, kdy jsou osobní údaje shromažďovány bez úmyslu použít profilovací metody, ale později jsou zpracovávány v kontextu profilování, správce by tehdy měl také poskytnout informace uvedené pod 4.1.

4.5. Ustanovení informovat subjekty údajů podle zásad 4.2, 4.3 a 4.4 neplatí, pokud:
a) byl subjekt údajů již informován;
b) se ukáže jako nemožné dané informace poskytnout nebo by to vyžadovalo nepřiměřené úsilí;
c) zpracování nebo sdělení osobních údajů pro profilování výslovně upravuje vnitrostátní právo.

V případech spadajících pod body b) a c) by měla být zavedena odpovídající ochranná opatření.

4.6. Informace poskytnuté subjektu údajů by měly být přiměřené a přizpůsobené okolnostem.

5. Práva subjektů údajů

5.1. Subjekt údajů, který je nebo byl předmětem profilování, by měl mít nárok obdržet na svoji žádost od správce v přiměřené době a ve srozumitelné formě informace týkající se:
a) jeho osobních údajů;
b) metody, která tvoří základ zpracování jeho osobních údajů a byla použita k přiřazení profilu, a to minimálně v tom případě, kdy došlo k automatizovanému rozhodnutí;
c) účelů, za jakými bylo profilování provedeno a o kategorii osob nebo orgánů, kterým mohou být údaje sděleny.

5.2. Subjekty údajů by měly mít nárok na opravu, výmaz nebo blokování svých osobních údajů v případě, kdy profilování bylo v průběhu zpracování osobních údajů provedeno v rozporu s vnitrostátním právem, které provádí zásady tohoto doporučení.

5.3. Pokud právo neupravuje profilování v kontextu zpracování osobních údajů, subjekt údajů by měl mít právo námitky proti použití svých osobních údajů k profilování ze závažného legitimního důvodu souvisejícího s jeho situací. V případě důvodné námitky by k profilování nemělo být použito osobních údajů daného subjektu údajů. Je-li účelem zpracování přímý marketing, nemusí subjekt údajů uvádět žádné zdůvodnění.

5.4. Pokud existují důvody pro omezení práv, které odpovídají ustanovením uvedeným v článku 6, mělo by takové rozhodnutí být oznámeno subjektu údajů jakýmikoli záznam umožňujícími prostředky s odkazem na právní a věcné důvody takového omezení.
Uvedený odkaz je možno opomenout v případě, kdy existuje skutečnost, která ohrožuje důvod pro dané omezení. V takových případech by měl subjekt údajů dostat informaci, jak může dané rozhodnutí napadnout u příslušného národního orgánu dozoru, právního orgánu nebo u soudu.

5.5. V případě, kdy je osoba předmětem rozhodnutí, které má pro ni právní důsledky nebo se jí citelně dotýká, a to výhradně na základě profilování, měla by mít možnost podat proti takovému rozhodnutí námitku, pokud neplatí, že:
a) věc upravuje zákon, který stanovuje opatření na ochranu legitimních zájmů subjektů údajů, a to zejména tím, že jim umožňuje vyjádřit vlastní názor;
b) rozhodnutí bylo učiněno během plnění smlouvy, kde subjekt údajů je smluvní stranou nebo z důvodu plnění předsmluvních opatření přijatých na žádost subjektu údajů, kdy tato opatření chrání legitimní zájmy subjektu údajů.

6. Výjimky a omezení

V případech, kdy je to v demokratické společnosti nutné z důvodů státní bezpečnosti, veřejné bezpečnosti, měnových zájmů státu, předcházení a potlačování trestných činů nebo ochrany subjektu údajů či práv a svobod ostatních, nemusejí členské státy použít ustanovení obsažená v části 3, 4 a 5 tohoto doporučení, pokud to upravuje zákon.

7. Opravné prostředky

Vnitrostátní právo by mělo poskytovat odpovídající postihy a opravné prostředky pro případ porušení vnitrostátního práva provádějícího zásady tohoto doporučení.

8. Bezpečnost údajů

8.1. K zajištění ochrany osobních údajů zpracovávaných v souladu s vnitrostátním právem provádějícím zásady tohoto doporučení by měla být přijata vhodná technická a organizační opatření, aby osobní údaje byly chráněny před náhodným nebo nezákonným zničením a náhodnou ztrátou, stejně jako neoprávněným přístupem, pozměňováním, sdělováním nebo jakoukoli jinou formou nezákonného zpracování.
Tato opatření mají zajišťovat vlastní standardy bezpečnosti dat s ohledem na současný stav technického rozvoje, a také se zřetelem na citlivou povahu osobních údajů sbíraných a dále zpracovávaných v souvislosti s profilováním a měla by rovněž zabezpečit vyhodnocení možných rizik. Pravidelně a v přiměřených intervalech by měla být podrobena revizi.

8.2. Správci by měli v souladu s vnitrostátním právem stanovit odpovídající vnitřní předpisy s patřičným ohledem na příslušné zásady tohoto doporučení.

8.3. Správci by v případě potřeby měli jmenovat nezávislou osobu odpovědnou za bezpečnost informačních systémů a ochranu dat, kvalifikovanou k poskytování rad v těchto záležitostech.

8.4. Správci by měli vybrat zpracovatele, kteří nabízejí odpovídající ochranná opatření s ohledem na technický a organizační aspekt chystaného zpracování, a měli by zajistit, že tato ochranná opatření budou dodržována a zejména, že bude zpracování v souladu s jejich pokyny.

8.5. Měla by být zavedena vhodná opatření, která by chránila před jakoukoli možností, že by anonymní a agregované statistické údaje použité při profilování vedly ke zpětné identifikaci subjektů údajů.

9. Orgány dozoru

9.1. Členské státy by měly pověřit jeden nebo více nezávislých orgánů k zajištění souladu s vnitrostátním právem provádějícím zásady tohoto doporučení, které budou mít v tomto ohledu potřebné pravomoci vyšetřovat a zasahovat, zejména pravomoc projednávat stížnosti podané jednotlivými osobami.

9.2. Navíc mohou členské státy v případech zpracování, které využívá profilování a představuje zvláštní rizika z hlediska ochrany soukromí a osobních údajů usoudit, že buď:
a) správci musí uvědomit orgán dozoru před zahájením zpracování,
nebo že
b) toto zpracování je předmětem předběžné kontroly ze strany orgánu dozoru.

9.3. Výše uvedené orgány dozoru by měly informovat veřejnost o uplatňování legislativy zavádějící zásady vytyčené tímto doporučením.

Poznámka:

[1] Při schvalování tohoto doporučení si zástupce Spojeného království v souladu s článkem 10.2.c Jednacích pravidel pro zasedání ministerských zástupců vyhradil právo své vlády tomuto doporučení buď vyhovět, nebo nevyhovět.

[2] Materiál je také k dispozici na internetové adrese Úřadu www. uoou.cz v sekci Zahraničí/Rada Evropy.

PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29

622/10/CS
WP 178

Stanovisko č. 7/2010 o sdělení Evropské Komise o globálním přístupu k přenosům údajů jmenné evidence cestujících (PNR) do třetích zemí

Přijaté dne 12. listopadu 2010

Tato pracovní skupina byla zřízena podle článku 29 směrnice 95/46/ES. Jedná se o nezávislý evropský poradní orgán ve věci ochrany údajů a soukromí. Její úkoly jsou popsány v článku 30 směrnice 95/46/ES a článku 15 směrnice 2002/58/ES.

Její sekretariát je na Ředitelství C (Základní práva a občanství Unie) Evropské komise, Generální ředitelství pro spravedlnost, B-1049 Brusel, Belgie, kancelář č. MO-59 06/036.

Internetové stránky: http://ec.europa.eu/justice/policies/privacy/index_en.htm

PRACOVNÍ SKUPINA PRO OCHRANU FYZICKÝCH OSOB V SOUVISLOSTI SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ

zřízená směrnicí Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995,

s ohledem na článek 29 a čl. 30 odst. 1 písm. a) a odst. 3 uvedené směrnice a

čl. 15 odst. 3 směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002,

s ohledem na svůj jednací řád,

přijala toto stanovisko:

1. ÚVOD

Dne 21. září 2010 předložila Evropská komise své sdělení o globálním přístupu k přenosům údajů jmenné evidence cestujících (PNR) do třetích zemí. Komise se domnívá, že používání údajů PNR pro účely vynucování práva má rostoucí tendenci a je považováno za hlavní a nezbytný prvek činností souvisejících s vynucováním práva. Komise se proto rozhodla vytvořit soubor obecných kritérií, která by se měla vztahovat na všechny budoucí dohody týkající se PNR s třetími zeměmi. Sdělení mimoto obsahuje analýzu současného používání PNR a poskytuje informace o plánech Komise, jaké dohody s třetími zeměmi mají být v nadcházejících letech uzavřeny.

Jelikož PNR požaduje stále více zemí, zvýší se pravděpodobně rovněž počet dohod. Komise se proto rozhodla, že je vhodné stanovit rámec, který bude použitelný na všechny budoucí dohody týkající se PNR, s cílem zamezit u leteckých společností i členských států právní nejistotě a rovněž zbytečné administrativní zátěži vyplývající z nutnosti dodržovat různé soubory pravidel pro jednotlivé třetí země. Pracovní skupina zřízená podle článku 29 vítá globální přístup, který Komise přijala k nakládání se žádostmi na úrovni EU a zajištění silných norem ochrany údajů při úplném dodržování základních práv.

Pracovní skupina chce zdůraznit, že by výměna údajů PNR neměla být posuzována samostatně. Globální přístup by se proto měl rozšířit na žádosti třetích zemí týkající se všech údajů o cestujících, včetně předběžných informací o cestujících, porovnávání seznamů podezřelých a jiné činnosti v oblasti předběžné kontroly. To by mělo rovněž znamenat, že by Komise měla při přijetí žádosti týkající se údajů o cestujících rozhodnout, zda a jaký druh údajů, například předběžné informace o cestujících, bude postačovat, a uzavřít za tímto účelem dohodu.

Co se týká údajů PNR, pracovní skupina pečlivě sledovala jednání, která vedla k uzavření dohod týkajících se PNR s USA, Kanadou a Austrálií, a vydala řadu stanovisek, v nichž byly určeny problémy týkající soukromí, které souvisí s těmito systémy PNR. Až dosud nebylo mnoha námitkám, které pracovní skupina vznesla, vyhověno. Stávající sdělení však představuje krok správným směrem, ačkoliv řada obav přetrvává.

II. NEZBYTNOST POUŽÍVÁNÍ ÚDAJŮ PNR

Pracovní skupina vždy podporovala boj proti mezinárodnímu terorismu a závažné nadnárodní trestné činnosti. Pracovní skupina se domnívá, že tento boj je nezbytný a oprávněný. Uznává, že osobní údaje mohou být za určitých okolností cenné, zastává však názor, že k potlačení tohoto jevu nemusí postačovat shromažďování a zpracovávání všech údajů o cestujících a že k zvýšení bezpečnosti a zajištění bezpečné a efektivní letecké dopravy je nutno využívat rovněž všechny ostatní dostupné prostředky, pokud možno s méně rušivým dopadem na nevinné cestující. Je nutno zdůraznit, že letecké společnosti shromažďují a používají údaje o cestujících pro vlastní obchodní účely. Aby bylo možno použít tyto údaje k jinému účelu, tj. pro účely vynucování práva, je nutný vyvážený přístup mezi požadavky na ochranu veřejné bezpečnosti a jinými veřejnými zájmy, jako jsou základní práva jednotlivců.

Ve stávajícím sdělení Evropská komise pouze konstatuje, že PNR je stále více považována za nezbytný nástroj boje proti terorismu a závažné trestné činnosti, aniž by toto tvrzení odůvodnila. Nezdá se, že by Komise rozlišovala mezi rostoucím používáním údajů PNR a stále větším akceptováním používání těchto údajů. Může se stát, že si donucovací orgány skutečně zvyknou na to, že mají k dispozici údaje PNR, avšak samotná tato skutečnost neprokazuje politický nebo veřejný souhlas se shromažďováním a používáním údajů PNR, ani neodůvodňuje jejich nezbytnost.

Zdá se, že tři argumenty uvedené v bodě 2.2 sdělení spíše naznačují, že „je dobré, že donucovací orgány mají k dispozici údaje PNR“ než že „donucovací orgány potřebují údaje PNR k boji proti terorismu a závažné trestné činnosti“. Pracovní skupina rovněž lituje, že Komise nepovažovala za nutné zabývat se blíže účelností používání údajů PNR, což je zásadní prvek při posuzování nezbytnosti.

Ve svých předchozích stanoviscích pracovní skupina opakovaně zdůrazňovala význam snah o náležitou rovnováhu. Dosud tomu tak nebylo. Co je důležitější, neexistují žádné objektivní statistické údaje nebo důkazy, které by jednoznačně prokazovaly význam údajů PNR v mezinárodním boji proti terorismu a závažné nadnárodní trestné činnosti. To znemožňuje posoudit jednoznačně nezbytnost nebo přiměřenost používání PNR pro účely vynucování práva.

Podle pracovní skupiny by jakýkoli systém PNR měl být:

- prokazatelně nezbytný k vyřešení problému;
- prokazatelně vhodný k vyřešení problému;
- přiměřený přínosu v oblasti bezpečnosti;
- prokazatelně méně rušivý než alternativní opatření a
- pravidelně přezkoumáván s cílem zajistit, že opatření jsou dosud přiměřená[1].

Tyto požadavky lze podrobně rozvést následovně. Musí být zjištěno, že je nezbytné analyzovat modely cestování cestujících s přihlédnutím ke konkrétnímu a zvláštnímu předpokládanému účelu. Pro ilustraci: boj proti terorismu nebude nutně vyžadovat stejné údaje a nebude mít za následek stejnou rovnováhu práv a zájmů jako například boj proti pašování drog. Je nutno připomenout, že údaje PNR byly původně shromažďovány po událostech ze dne 11. září 2001 vzhledem k mimořádné hrozbě. Nyní se kontext přesouvá

[1] Stanovisko pracovní skupiny ze dne 5. prosince 2007 o evropském systému PNR.
Viz rovněž usnesení 29. mezinárodní konference komisařů pro ochranu údajů a soukromí, která se konala v Montrealu dne 28. září 2007.

k obecnému zpracovávání pro různé účely, někdy bez jakékoli souvislosti s původním odůvodněním.

Před zvažováním případných nových dohod týkajících se PNR nebo vývojem nových systémů PNR by měla být provedena podrobná analýza účinnosti stávajících databází a výměn informací, k nimž již dochází[2].

Pracovní skupina znovu opakuje, že k vyhovění žádosti třetí země týkající se údajů o cestujících by mohlo v mnoha případech postačovat splnění požadavku týkajícího se nezbytnosti předběžných informací o cestujících. Na základě přesných informací o totožnosti namísto údajů o účelech cesty by bylo snazší zjistit vhodnost a přiměřenost zpracovávaných údajů. Pracovní skupina mimoto požaduje jednoznačně stanovené účely pro používání systémů předběžných informací o cestujících a PNR ze strany donucovacích orgánů s cílem zajistit, aby byla účinnost těchto systémů skutečně měřitelná.

Pokud jde o žádosti o údaje o cestujících nebo o potřebu těchto údajů, je v současnosti zavedeno mnoho systémů a mechanismů, včetně dvoustranných dohod mezi členskými státy a USA. Před uzavřením nových dohod by Komise měla posoudit, zda lze žádostem třetích zemí o údaje o cestujících vyhovět prostřednictvím stávajících systémů a mechanismů.

Přiměřenost systému je nutno posoudit s přihlédnutím k dopadu použitých prostředků (například analýza modelů a posouzení rizik) na základní práva jednotlivců. Před zavedením takovéhoto systému je nutno pečlivě uvážit alternativní možnosti s ohledem na rušivou povahu rozhodnutí, která jsou (přinejmenším z velké části) přijímána automaticky podle standardních modelů, a vzhledem k potížím fyzických osob vznést námitky vůči těmto rozhodnutím. Pracovní skupina by proto uvítala náležité posouzení dopadů na základní práva, které by bylo provedeno u všech budoucích legislativních návrhů Evropské komise souvisejících s PNR.

S ohledem na vědecké údaje a nejnovější studie je nutno zcela zpochybnit užitečnost rozsáhlého profilování na základě údajů o cestujících. Pracovní skupina dosud nezaznamenala žádné informace, které by potvrzovaly užitečnost tohoto profilování. V nejnovějších studiích bylo naopak spíše zjištěno, že takovéto prověřování je kontraproduktivní, zejména co se týká boje proti terorismu[3].

---

[2] Například mnohostranné nebo dvoustranné dohody mezi členskými státy a třetími zeměmi. Viz rovněž v rámci právních předpisů EU týkajících se VIS a SIS a dohod s třetími zeměmi o externích výměnách údajů, zejména Dohody o vzájemné právní pomoci mezi Evropskou unií a Spojenými státy americkými, Dohody mezi USA a Evropským policejním úřadem ze dne 6 prosince 2001 a Dohody mezi Eurojustem a USA ze dne 6. listopadu 2006.

[3] Harvard Civil Rights – Civil Liberties Review, „Government Data Mining, the Need for a Legal Framework“, Fred H. Cate, strana 468: „Z narůstajících důkazů vyplývá, že vytěžování dat nebude pravděpodobně u mnoha účelů, pro něž se je vláda snaží využívat, účinné, zejména v oblasti národní bezpečnosti a prosazování práva. Nejenže se státním úředníkům nepodařilo určit úspěšné snahy o odhalení teroristické činnosti či dokonce o předcházení takovéto činnosti na základě analýz databází, nýbrž existují významné překážky, které brání tomu, aby byly tyto snahy úspěšné. K těmto překážkám patří zábrany, které představují otázky kvality údajů, problémy s porovnáváním údajů a omezení nástrojů pro vytěžování dat, zejména v případě, je-li vytěžování dat v oblasti národní bezpečnosti v rozporu s vytěžováním dat pro komerční cílený marketing“.
A strana 475: „Pokud by systém vytěžování dat, který má potenciálním teroristům zabránit ve vstupu na palubu letadla, přinesl falešně kladný výsledek ve výši pouze jednoho procenta (což je mnohem lepší výsledek, než jakého bylo dosaženo prostřednictvím veřejně zpřístupněného státního nebo komerčního vytěžování dat) znamenalo by to, že by 7,4 milionu cestujících (jedno procento z celkem 739 milionů cestujících, které Úřad pro bezpečnost dopravy v USA prověřil v roce 2005) bylo nesprávně identifikováno jako osoby podezřelé z terorismu.“
Viz rovněž Jeff Jonas a Jim Harper, „Effective Counterterrorism and the Limited Role of Predictive Data Mining“, Policy Analysis ze dne 11. prosince 2006, s. 8 a 9: „Na rozdíl od nákupních zvyků spotřebitelů a finančních podvodů nedochází k teroristickým činům dostatečně často, aby bylo možno vytvořit platné prognostické modely. (...) Bez

Co se týká technické sítě leteckých společností nebo počítačových rezervačních systémů, přizpůsobení infrastruktury tak, aby bylo možno snáze vyhovět žádostem týkajícím se vynucování práva, vyvolává vážné otázky týkající se soukromí: v předběžné fázi by nemělo dojít k novému vymezení systému pro účely, které nemají v zásadě žádnou spojitost s hlavními obchodními činnostmi. Naopak, tato infrastruktura by měla být navržena tak, aby vyhovovala potřebám daného odvětví, a nikoli účelům vynucování práva. V souladu s potřebami odvětví by návrh systému měl zahrnovat technologie zvyšující ochranu soukromí, zejména s cílem zamezit neoprávněnému přístupu a chránit integritu osobních údajů.

III. NORMY, OBSAH A KRITÉRIA

Pracovní skupina vítá obecné normy stanovené v bodě 3.3 sdělení. Tyto normy by se však měly pokládat za základní prvky, jež by měla splňovat každá budoucí dohoda týkající se PNR, a nikoli za seznam požadavků, které mají být projednány. Mnoho norem a kritérií odstraňuje problémy, na které v minulosti upozornila jak pracovní skupina, tak i Evropský parlament. Jejich uplatňování prostřednictvím závazných dohod by pro evropské občany v zásadě znamenalo mnohem lepší úroveň ochrany údajů a zajistilo by právní jistotu. Pracovní skupina však vidí prostor pro další zlepšení a ráda by zákonodárce EU vyzvala, aby do rámce obecných norem a kritérií pro budoucí dohody týkající se PNR a rovněž následných mandátů k vyjednávání zahrnul níže uvedené prvky.

Soulad s právním rámcem EU pro ochranu soukromí a údajů

Musí být zřejmé, že by jakákoli budoucí dohoda týkající se PNR měla zcela splňovat podmínky stanovené v právním rámci EU pro ochranu soukromí a údajů, a to v rámci bývalého prvního a bývalého třetího pilíře. To mimo jiné znamená, že by ve všech budoucích dohodách týkajících se PNR měla být zajištěna alespoň práva udělená subjektům údajů ve směrnici 95/46/ES, rozhodnutí 2008/977/SVV a ve vnitrostátních prováděcích předpisech. Mělo by být zřejmé, že by všechna práva přidělená subjektu údajů měla být rovněž vykonatelná v praxi. Měla by být zajištěna taktéž soudržnost s budoucím uceleným rámcem EU pro ochranu údajů a budoucí obecnou dohodou mezi EU a USA o výměně údajů v rámci policejní a soudní spolupráce v trestních věcech. Dohody by měly mimoto respektovat právo na ochranu osobních údajů fyzických osob, jak je stanoveno v Listině základních práv EU, která má od vstupu Lisabonské smlouvy v platnost právně závazný charakter.

Pracovní skupina zdůrazňuje, že v přijímající třetí zemi musí existovat odpovídající právní předpisy, které povolují shromažďování a zpracovávání údajů PNR pro účely vynucování práva ze strany příslušných orgánů. Každá budoucí dohoda týkající se PNR musí odkazovat na příslušné vnitrostátní právní předpisy. Jelikož by všechny podmínky v dohodě měly být dohodnuty dvoustranně a měly by být dodržovány všemi stranami, neměly by být podmínky ukládány, měněny či vykládány jednostranně.

Kvalita údajů

Ve své analýze mezinárodních trendů týkajících se PNR Komise poznamenává, že údaj PNR je neověřená informace, kterou poskytují většinou samotní cestující nebo provozovatelé souborných služeb pro cesty, pobyty a zájezdy či cestovní agentury a která je shromažďována

---

náležitě vytvořených algoritmů založených na rozsáhlých historických modelech nebude v případě terorismu prediktivní vytěžování dat úspěšné. Výsledkem by bylo zaplavení systému národní bezpečnosti falešně pozitivními výsledky – podezřelými, kteří jsou ve skutečnosti nevinní“.

pro obchodní účely, nikoli pro účely vynucování práva. Jelikož neexistuje (snadný) způsob, jak tyto údaje objektivně ověřit, nelze údaje PNR považovat za přesné informace. Jejich shromažďování pro účely vynucování práva a přistěhovalectví proto vyvolává otázky týkající se vhodnosti a přesnosti. Pokud se prokáže nezbytnost výměny údajů PNR, je nutno tuto výměnu posoudit podle okolností každého jednotlivého případu, včetně ověření naprosté nezbytnosti a přiměřenosti.

Doba uchovávání údajů donucovacími orgány v přijímající třetí zemi

Jak se ve sdělení správně uvádí, doba uchovávání údajů by neměla být delší, než co je nezbytné k realizaci vymezeného cíle. Jinými slovy, doba uchovávání údajů by měla být náležitá a přiměřená. Uchovávání údajů o fyzických osobách, které nejsou podezřelé, vyvolává otázku jejich nezbytnosti a v některých členských státech může být v rozporu s ústavními zásadami. Pracovní skupina dosud nezaznamenala žádné důkazy, že konkrétně stanovené doby uchovávání jsou náležité a přiměřené. Údaje by měly být vymazány neprodleně po analýze, vyjma ve zvláštních případech, kdy vedly k zahájení vyšetřování ve vztahu k určitému cestujícímu. V těchto případech mohou být uchovávány v příslušných spisech tak dlouho, jak je to nezbytné pro probíhající vyšetřování, v souladu se stávajícím právním procesním rámcem, který obsahuje přiměřené záruky s ohledem na bezpečnost a integritu osobních údajů, a z původní databáze by měly být vymazány. Vzhledem k požadovanému harmonizačnímu účinku obecných norem se pracovní skupina domnívá, že je vhodné do všech budoucích dohod týkajících se PNR zahrnout stejnou dobu uchovávání údajů, a současně znovu zdůrazňuje, že by doba uchovávání neměla být delší, než je nezbytně nutné.

Podmínky předání údajů

Pracovní skupina je spokojena s tím, že Komise navrhuje používat výhradně tzv. „push“ metodu předání, podle níž údaje vybírají a orgánům předávají přímo letecké společnosti, místo tzv. „pull“ systému. „Pull“ systémy budou proto patřit minulosti. Ačkoliv pracovní skupina souhlasí s tím, že „push“ systém zajišťuje lepší ochranu soukromí než „pull“ systém, navrhuje, že by u budoucích dohod bylo možno uvážit i jiné systémy předávání údajů, které byly vyvinuty s funkcemi zajišťujícími ochranu soukromí. Tím by mohl být například systém, v němž nedochází k ukládání nebo uchovávání údajů, nejsou-li použity za účelem výstrahy nebo vyšetřování, takže donucovacím orgánům jsou fakticky předávány pouze údaje, u nichž bylo zjištěno, že jsou nezbytné. Takovýto systém by měl být navržen s přihlédnutím k současnému stavu zabezpečení, včetně záznamů o přístupech.

Pracovní skupina se rovněž domnívá, že je vhodné, aby před předáním údajů PNR donucovacím orgánům letečtí dopravci (jako správci údajů) vyfiltrovali citlivé údaje. Není-li to z technických důvodů možné, měl by být zaveden mechanismus pro filtrování údajů, aby měly donucovací orgány přístup pouze k filtrovaným údajům. Závěrem pracovní skupina znovu opakuje své námitky vůči tzv. hromadnému předávání údajů PNR. Z hlediska přiměřenosti by předání údajů PNR bylo přijatelné pouze tehdy, je-li naprosto nezbytné a vyžadují-li je okolností jednotlivého případu. Dožadující příslušný orgán pak musí odůvodnit, že v daném konkrétním případě jsou údaje PNR nezbytné.

Přístup a ukládání

V souladu s kritériem přiměřenosti by měl být přístup k údajům umožněn podle okolností jednotlivého případu. Kritéria používaná ke kontrole seznamu cestujících by měla fungovat na základě „shody/neshody“ s přístupem k identifikovatelným informacím pouze v případě „shody“. Měly by být zavedeny kontroly přístupu, aby přístup k osobním údajům měli pouze oprávnění pracovníci příslušných orgánů, a to na základě opodstatněné potřeby. Jak bylo zmíněno dříve, osobní údaje by měly být ukládány pouze v případě, souvisí-li s vyšetřováním týkajícím se určitého cestujícího.

Následné předávání údajů

Sdělení se nevyjadřuje velmi jasně k otázce následného předávání údajů PNR, a to jiným veřejným orgánům v přijímající zemi nebo jiným třetím zemím. Pracovní skupina souhlasí s uvedenými kritérii, chce však ještě více omezit možnosti následného předávání údajů. Co je nejdůležitější, měla by se použít zásada omezení účelu, což znamená, že shromážděné údaje nemohou jiné veřejné orgány v přijímající zemi použít k jiným účelům než k boji proti závažné nadnárodní trestné činnosti a terorismu. Obecně je nutno poukázat na skutečnost, že orgán, jenž si údaje PNR vyžádal původně, je nutno považovat za správce údajů, který za údaje odpovídá i po jejich předání třetím stranám. V případě pochybností by měl mít dotyčný orgán povinnost nedat svolení k zpřístupnění údajů třetí straně. V případě, že tato třetí strana zneužije údaje PNR, musí mít subjekt údajů možnost pokládat za odpovědného původního příjemce údajů. Konkrétněji, co se týká předání údajů jiným veřejným orgánům, pracovní skupina požaduje, aby byl jako příloha ke každé budoucí dohodě připojen omezený seznam jednoznačně stanovených orgánů, které mohou obdržet údaje PNR. Při zvažování ustanovení o následném předávání údajů během vyjednávání musí Komise přihlédnout k stávajícím dvoustranným dohodám o výměně údajů PNR, které mohla dotyčná třetí země uzavřít. Pracovní skupina by upřednostňovala, aby měla dohoda EU vždy větší váhu než dvoustranné dohody.

Společný přezkum

Pracovní skupina souhlasí s Komisí, že je nezbytné pravidelně sledovat a přezkoumávat dohody týkající se PNR. Do těchto společných přezkumů by se měli zapojit rovněž zástupci evropských orgánů pro ochranu údajů. Do společného přezkumu by měly být zahrnuty záležitosti jako možnost posoudit fungování dohody, včetně výsledků uplatňování práva na přístup a jiných důležitých práv subjektů údajů a spolupráce mezi orgány dohledu. Pracovní skupina mimoto pokládá za důležité, aby všechny budoucí dohody stanovily sankce v případě, nebude-li naplánovaný společný přezkum proveden včas, či pokud nebude proveden vůbec. To by mělo nakonec vést k ukončení dohody.

Ustanovení o skončení platnosti
Je nutné pravidelně posuzovat a vyhodnocovat nezbytnost systému PNR. Toto ucelené důkladné posouzení nelze provést během výše popsaného přezkumu. Do každé budoucí dohody by proto mělo být vloženo ustanovení o skončení platnosti, které nařizuje důkladné a nezávislé posouzení a vyhodnocení ustanovení o systému PNR. Po uplynutí data uvedeného v ustanovení o skončení platnosti nelze vyměňovat žádné údaje, pokud se strany dohody výslovně nerozhodnou prodloužit její platnost.

IV. ZÁVĚR

Pracovní skupina je celkově spokojena se skutečností, že Evropská komise jednoznačně prokázala, že chápe nutnost věnovat v budoucích dohodách týkajících se PNR ochraně údajů větší pozornost, a že je připravena uzavírat závazné dohody s cílem zajistit právní jistotu a rovné zacházení. Sdělení, které bylo předloženo dne 21. září 2010, je krokem správným směrem. S ohledem na vědecké údaje a nejnovější studie je však nutno zcela zpochybnit užitečnost rozsáhlého profilování na základě údajů o cestujících.

Pracovní skupina znovu zdůrazňuje nutnost globálního přístupu u všech údajů o cestujících, nejen údajů PNR. Na základě současného vývoje, včetně přezkumu právního rámce EU pro ochranu údajů a navrhovaných jednání s USA o obecné dohodě o ochraně údajů, je nezbytná soudržnost.

Pracovní skupina zdůrazňuje, že obecné normy a kritéria obsažené ve sdělení je nutno považovat za minimální úroveň ochrany údajů, jíž má být v budoucích dohodách týkajících se PNR dosaženo. V řadě bodů by však normy mohly a měly být dále rozvinuty.

Pracovní skupina proto Komisi, Evropský parlament a Radu vyzývá, aby při diskusích o mandátech k vyjednávání a předlohách budoucích dohod týkajících se PNR vzaly toto stanovisko v úvahu a aby pracovní skupinu informovaly o následných opatřeních. Pracovní skupina je samozřejmě připravena spolupracovat s kterýmkoli z orgánů EU v případě, je-li nutné objasnění či podrobné rozvedení jejího postoje.

Závěrem chce pracovní skupina znovu požádat, aby byla konzultována nebo požádána o vydání doporučení s ohledem na prvky týkající se ochrany údajů v jakékoli budoucí dohodě, zejména vzhledem ke své úloze oficiálního poradního orgánu EU v oblasti ochrany údajů a skutečnosti, že členy pracovní skupiny jsou vnitrostátní orgány dohledu pro dopravce, kteří budou povinni případné budoucí dohody dodržovat. Pracovní skupina rovněž žádá, aby byla během jednání o těchto budoucích dohodách pravidelně informována o situaci.

V Bruselu dne 12. listopadu 2010

Za pracovní skupinu
předseda
Jacob KOHNSTAMM

Sdělení o technické chybě

Vážení čtenáři, sdělujeme Vám, že ve Věstníku v částce 57 došlo k technické chybě, a sice k opakování stejné stránky. Obsah strany 3241 byl omylem uveden ještě jednou na straně 3267. Opravenou stranu 3267 proto otiskujeme ve správné podobě. *Za vzniklé nedopatření se omlouváme a děkujeme za pochopení.*

Redakce Věstníku

společnost rovněž stále více uvědomují jejich význam. To zase posiluje nutnost uplatňovat přísná opatření k jejich ochraně.

8. Z výše uvedených skutečností vyplývá, že porušení ochrany osobních údajů může mít pro správce údajů ve veřejném a soukromém sektoru značné negativní dopady. Možné chyby v aplikacích elektronické veřejné správy a elektronického zdravotnictví budou mít z hospodářského hlediska, zejména s ohledem na dobrou pověst, ničivé následky. Pro správce údajů ve všech odvětvích je proto zásadní minimalizovat rizika, vytvořit si a udržovat dobrou pověst a zajistit důvěru občanů a spotřebitelů.

9. Výše uvedené skutečnosti prokazují, že je naprosto nutné, aby správci údajů uplatňovali skutečná a účinná opatření na ochranu údajů, jejichž cílem je řádná správa ochrany údajů a současně minimalizace rizik v právní a hospodářské oblasti a rizik ztráty dobré pověsti, která mohou vyplynout z nedostatečných postupů v oblasti ochrany údajů. Jak je rozvedeno níže, dosažení těchto cílů mají zajistit mechanismy založené na odpovědnosti.

II.2 Možná celková právní úprava mechanismů založených na odpovědnosti

10. V této souvislosti je důležitou otázkou, jíž je nutno se zabývat, způsob, jakým může právní rámec správce údajů podnítit, aby přijali opatření, která zajišťují skutečnou ochranu v praxi. Jinými slovy, jak by měla vypadat právní úprava systémů založených na odpovědnosti.

11. Před projednáním této úpravy je třeba hned na úvod zdůraznit, že tyto systémy nijak nemění ani neovlivňují hlavní zásady ochrany údajů, nýbrž mají zajistit jejich lepší fungování.

12. Jedním ze způsobů, jak přimět správce údajů, aby zavedli takováto opatření, je připojení zásady odpovědnosti do revidovaného znění směrnice. Očekávané dopady takovéhoto ustanovení by zahrnovaly zavedení vnitřních opatření a postupů prosazujících stávající zásady ochrany údajů a zajišťujících jejich účinnost a povinnost toto prokázat, pokud o to orgány pro ochranu údajů požádají. Jak je podrobněji popsáno níže, druhy postupů a mechanismů se budou lišit podle rizik vyplývajících ze zpracování a povahy údajů.

13. Kromě výše uvedených aspektů by bylo možno uvážit zvláštní požadavky, například povinnost provádět v určitých případech posouzení dopadů na soukromí nebo jmenovat osoby určené pro ochranu údajů. Tyto zvláštní požadavky by mohly doplňovat obecnou zásadu odpovědnosti.

14. Pracovní skupina zřízená podle článku 29 uznává, že správci údajů mohou chtít zavést politiky a postupy, jež nejsou v právních předpisech na ochranu údajů striktně stanoveny. Správce údajů se může například zavázat, že bude ve velmi krátké době reagovat na žádosti o přístup, ačkoliv právní předpisy umožňují určitou pružnost. Může se rovněž zavázat, že bude reagovat na žádosti o přístup současně on-line a off-line, aby bylo zajištěno okamžité a účinné přijetí těchto informací. Lze si rovněž představit případy, kdy chce správce údajů překročit minimální požadavky stanovené v obecném právním rámci. Správce údajů se

III. MATERIÁLY Z ÚŘEDNÍHO VĚSTNÍKU EVROPSKÉ UNIE

ROZHODNUTÍ KOMISE

ze dne 31. ledna 2011

podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně osobních údajů Státem Izrael v souvislosti s automatizovaným zpracováváním osobních údajů

(oznámeno pod číslem K(2011) 332)

(Text s významem pro EHP)

(2011/61/EU)

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na směrnici Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů [1], a zejména na čl. 25 odst. 6 uvedené směrnice,

po konzultaci s evropským inspektorem ochrany údajů,

vzhledem k těmto důvodům:

(1) V souladu se směrnicí 95/46/ES jsou členské státy povinny zajistit, aby k předávání osobních údajů do třetí země docházelo, pouze pokud dotyčná třetí země zajišťuje odpovídající úroveň ochrany a pokud jsou před předáním údajů dodržovány právní předpisy členských států provádějící ostatní ustanovení směrnice.

(2) Komise může dospět k závěru, že třetí země zajišťuje odpovídající úroveň ochrany. Takové zemi mohou členské státy předávat osobní údaje, aniž by byly nutné dodatečné záruky.

(3) V souladu se směrnicí 95/46/ES má být úroveň ochrany údajů hodnocena s ohledem na všechny okolnosti související s předáním nebo předáváním údajů, a to se zvláštním zřetelem na celou řadu podmínek týkajících se předávání a uvedených v článku 25 této směrnice.

(4) S ohledem na rozdíly v přístupu třetích zemí k ochraně údajů by mělo být dbáno na to, aby hodnocení odpovídající úrovně této ochrany a uplatňování všech rozhodnutí na základě čl. 25 odst. 6 směrnice 95/46/ES nebyla svévolně nebo neodůvodněně diskriminační vůči třetím zemím, kde jsou obdobné podmínky, nebo mezi nimi, a aby nevytvářela skrytou překážku obchodu s ohledem na stávající mezinárodní závazky Evropské unie.

(5) Právní řád Státu Izrael nemá psanou ústavu, avšak ústavní sílu dovodil Nejvyšší soud Státu Izrael u některých „základních zákonů“. Tyto „základní zákony“ doplňuje objemný soubor judikatury, jelikož se právní řád Izraele ve značném rozsahu řídí zásadami obyčejového práva. Právo na soukromí je zahrnuto v „základním zákonu o právu na lidskou důstojnost a svobodu“ v oddíle 7.

(6) Právní normy upravující ochranu osobních údajů ve Státě Izrael vycházejí ve velké míře z norem stanovených směrnicí 95/46/ES a jsou stanoveny v zákoně o ochraně soukromí 5741-1981, naposledy pozměněném v roce 2007 za účelem zavedení nových požadavků na zpracování osobních údajů a podrobné organizace orgánu dozoru.

(7) Tyto právní předpisy v oblasti ochrany údajů dále doplňují vládní rozhodnutí provádějící zákon o ochraně soukromí 5741-1981 a o organizaci a fungování orgánu dozoru, která povětšinou vycházejí z doporučení formulovaných ve zprávě Komise pro přezkum právních předpisů týkajících se databází (Schoffmanova zpráva) pro ministerstvo spravedlnosti.

(8) Ustanovení ohledně ochrany údajů jsou rovněž obsažena v celé řadě právních nástrojů upravujících různá odvětví, jako jsou předpisy ve finančním sektoru, ve zdravotnictví a předpisy týkající se veřejných rejstříků.

(9) Právní normy v oblasti ochrany údajů platné ve Státě Izrael pokrývají všechny základní zásady nutné pro odpovídající úroveň ochrany pro fyzické osoby ve vztahu k zpracování osobních údajů automatizovanými databázemi. Kapitola 2 zákona o ochraně soukromí 5741-1981, která stanoví zásady zpracování osobních údajů, se nevztahuje na zpracování osobních údajů v databázích, které nejsou automatizované (manuální databáze).

(10) Uplatňování právních norem ochrany osobních údajů zaručují správní a soudní prostředky nápravy a nezávislý dozor prováděný dozorčím orgánem, jímž je Izraelský úřad pro právo, informace a technologie (ILITA), který je nadán pravomocemi k provádění šetření a zásahů a je zcela nezávislý.

[1] Úř. věst. L 281, 23.11.1995, s. 31.

(11) Izraelské orgány pro ochranu osobních údajů poskytly vysvětlení a záruky ohledně způsobu výkladu izraelského práva a poskytly záruky ohledně provádění izraelských předpisů na ochranu údajů v souladu s takovým výkladem. Toto rozhodnutí přihlíží k uvedeným vysvětlením a zárukám, a je jimi proto podmíněno.

(12) Stát Izrael je proto třeba považovat za zemi zajišťující odpovídající úroveň ochrany osobních údajů podle směrnice 95/46/ES, pokud jde o automatizované mezinárodní předávání osobních údajů z Evropské unie do Státu Izrael nebo o případy, kdy toto předávání není automatizováno, avšak tyto údaje jsou předmětem dalšího automatizovaného zpracování ve Státě Izrael. Opačně, na mezinárodní předávání osobních údajů z EU do Státu Izrael, u kterého samo předávání a následné zpracování je prováděno výlučně neautomatizovanými prostředky, by se toto rozhodnutí nemělo vztahovat.

(13) V zájmu průhlednosti a aby příslušné orgány v členských státech zajistily ochranu fyzických osob v souvislosti se zpracováním jejich osobních údajů, je nezbytné uvést výjimečné okolnosti, za nichž může být odůvodněno pozastavení určitých toků údajů, bez ohledu na zjištění odpovídající úrovně ochrany.

(14) Závěry týkající se úrovně ochrany osobních údajů v tomto rozhodnutí odkazují na Stát Izrael vymezený podle mezinárodní práva. Další následné předávání příjemci mimo Stát Izrael vymezený podle mezinárodního práva by mělo být považováno za předávání osobních údajů do třetí země.

(15) Pracovní skupina pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů, zřízená podle článku 29 směrnice 95/46/ES, předložila kladné stanovisko k úrovni ochrany osobních údajů, pokud jde o automatizované mezinárodní předávání osobních údajů z Evropské unie, nebo o případy, kdy předávání není automatizované, avšak tyto údaje jsou předmětem dalšího automatizovaného zpracování ve Státě Izrael. Ve svém kladném stanovisku pracovní skupina vyzvala izraelské úřady, aby přijaly další ustanovení, která rozšíří uplatňování izraelských právních předpisů na manuální databáze, výslovně uznají, že bude uplatňování zásada proporcionality na zpracování osobních údajů v soukromé sféře, a která budou vykládat výjimky při mezinárodním předávání tak, aby byl jejich výklad v souladu s požadavky stanovenými v jejím „pracovním dokumentu o jednotném výkladu čl. 26 odst. 1 směrnice 95/46/ES“ [1]. Toto stanovisko bylo zohledněno při přípravě toho rozhodnutí [2].

(16) Výbor zřízený podle čl. 31 odst. 1 směrnice 95/46/ES nepředložil stanovisko ve lhůtě stanovené jeho předsedou,

PŘIJALA TOTO ROZHODNUTÍ:

Článek 1

1. Pro účely čl. 25 odst. 2 směrnice 95/46/ES se Izrael považuje za zemi poskytující odpovídající úroveň ochrany osobních údajů předávaných z Evropské unie, pokud jde o automatizované předávání osobních údajů z Evropské unie do Izraele nebo o případy, kdy toto předávání není automatizováno, avšak tyto údaje jsou předmětem dalšího automatizovaného zpracování ve Státě Izrael.

2. Orgánem dozoru Státu Izrael, který má pravomoc uplatňovat normy ochrany osobních údajů ve Státě Izrael, je Izraelský úřad pro právo, informace a technologie (ILITA) uvedený v příloze tohoto rozhodnutí.

Článek 2

1. Toto rozhodnutí se zabývá pouze úrovní ochrany zajišťované ve Státě Izrael vymezeném podle mezinárodního práva s cílem naplnit požadavky čl. 25 odst. 1 směrnice 95/46/ES a nedotýká se ostatních podmínek nebo omezení provádějících ostatní ustanovení zmíněné směrnice, které se vztahují na zpracování osobních údajů v členských státech.

2. Toto rozhodnutí se použije v souladu s mezinárodním právem. Rozhodnutím není dotčen status Golanských výšin, pásma Gazy a Západního břehu Jordánu, včetně východního Jeruzaléma podle mezinárodního práva.

Článek 3

1. Aniž jsou dotčeny pravomoci příslušných orgánů členských států přijímat opatření, která zajišťují, aby byly dodržovány vnitrostátní předpisy přijaté na základě jiných ustanovení než článku 25 směrnice 95/46/ES, mohou tyto orgány vykonávat své stávající pravomoci, aby pozastavily předávání údajů příjemci ve Státě Izrael s cílem chránit fyzické osoby v souvislosti se zpracováním jejich osobních údajů v těchto případech:

a) pokud příslušný izraelský orgán zjistí, že příjemce nedodržuje standardy uplatňované v oblasti ochrany, nebo

[1] Dokument WP114 ze dne 25. listopadu 2005. K dispozici na internetové stránce: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_en.pdf

[2] Stanovisko 6/2009 k úrovni ochrany osobních údajů v Izraeli. K dispozici na internetové stránce http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp165_en.pdf

b) pokud je velmi pravděpodobné, že nebyly dodržovány normy týkající se ochrany, pokud se lze důvodně domnívat, že příslušný orgán Státu Izrael včas nepřijal nebo nepřijme odpovídající opatření nezbytná pro vyřešení dané věci; pokud by pokračování v předávání údajů vyvolalo bezprostřední riziko vzniku vážné újmy subjektům údajů a pokud příslušné orgány členského státu za daných okolností přiměřeně usilují o informování strany odpovědné za zpracování údajů usazené ve Státě Izrael a poskytly jí příležitost zaujmout stanovisko.

2. Pozastavení předávání údajů skončí, jakmile je zajištěno dodržování norem ochrany a jakmile je o této skutečnosti informován příslušný orgán členského stát.

Článek 4

1. Členské státy neprodleně uvědomí Komisi o přijetí opatření podle článku 3.

2. Členské státy a Komise se rovněž vzájemně informují o případech, kdy opatření přijatá subjekty pověřenými zajištěním dodržování norem ochrany ve Státě Izrael nejsou dostatečná.

3. Pokud informace shromážděné podle článku 3 a podle odstavců 1 a 2 tohoto článku prokážou, že kterýkoli subjekt pověřený zajištěním dodržování norem ochrany ve Státě Izrael neplní účinně svou úlohu, uvědomí o tom Komise příslušný orgán Státu Izrael a, bude-li třeba, předloží návrh opatření postupem podle čl. 31 odst. 2 směrnice 95/46/ES s cílem zrušit toto rozhodnutí, pozastavit je nebo omezit jeho oblast působnosti.

Článek 5

Komise sleduje provádění tohoto rozhodnutí a jakékoli předmětné poznatky sdělí výboru zřízenému podle článku 31 směrnice 95/46/ES, včetně jakýchkoliv důkazů, které by mohly mít vliv na hodnocení prováděné podle článku 1 tohoto rozhodnutí, zda je úroveň ochrany ve Státě Izrael odpovídající ve smyslu článku 25 směrnice 95/46/ES, a jakýchkoliv důkazů, že se toto rozhodnutí provádí diskriminačním způsobem. Komise zejména sleduje zpracovávání osobních údajů v manuálních databázích.

Článek 6

Členské státy přijmou veškerá opatření, která jsou nezbytná pro dosažení souladu s tímto rozhodnutím, do tří měsíců od data jeho oznámení.

Článek 7

Toto rozhodnutí je určeno členským státům.

V Bruselu dne 31. ledna 2011.

Za Komisi

Viviane REDING

místopředsedkyně

PŘÍLOHA

Příslušný orgán dozoru uvedený v čl. 1 odst. 2 tohoto rozhodnutí:

The Israeli Law, Information and Technology Authority (Izraelský úřad pro právo, informace a technologie)
The Government Campus
9th floor
125 Begin Rd.
Tel Aviv
Izrael
Poštovní adresa:
P.O. Box 7360
Tel Aviv, 61072
Tel.: + 972 3 7634050
Fax: + 972 2 6467064
E-mail: ILITA@justice.gov.il
Internetová stránka: http://www.justice.gov.il/MOJEng/RashutTech/default.htm

Věstník Úřadu pro ochranu osobních údajů

Vydavatel: Úřad pro ochranu osobních údajů
Adresa redakce: Úřad pro ochranu osobních údajů, Pplk. Sochora 27, 170 00 Praha 7
Redakce: Miluše Nejedlá, tel.: 234 665 232, fax: 234 665 505
e-mail: posta@uoou.cz
internetová adresa: www.uoou.cz

Administrace: Písemné objednávky předplatného, změny adres a počtu odebíraných výtisků – SEVT, a. s., Pekařova 4, 181 06 Praha 8-Bohnice, telefon: 283 090 352, 283 090 354, fax: 233 553 422, www.sevt.cz, e-mail: sevt@sevt.cz. – **Předpokládané roční předplatné** se stanovuje za dodávku kompletního ročníku a je od předplatitelů vybíráno formou záloh ve výši oznámené ve Věstníku a pro tento rok činí 400 Kč – Vychází podle potřeby – **Tiskne**: Sprint servis, Lovosická 31, Praha 9.

Distribuce: Předplatné, jednotlivé částky na objednávku i za hotové – SEVT, a. s., Pekařova 4, 181 06 Praha 8-Bohnice, telefon: 283 090 352, 283 090 354, fax: 233 553 422; drobný prodej v prodejnách SEVT, a. s. – Praha 4, Jihlavská 405, tel.: 261 260 414 – Brno, Česká 14, tel.: 542 213 962 – Ostrava, roh ul. Nádražní a Denisovy, tel.: 596 120 690 – České Budějovice, Česká 3, tel.: 387 319 045 a ve vybraných knihkupectvích. Distribuční podmínky předplatného: Jednotlivé částky jsou expedovány předplatitelům neprodleně po dodání z tiskárny. Objednávky nového předplatného jsou vyřizovány do 15 dnů a pravidelné dodávky jsou zahajovány od nejbližší částky po ověření úhrady předplatného, nebo jeho zálohy. Částky vyšlé v době od zaevidování předplatného do jeho úhrady jsou doposílány jednorázově. Změny adres a počtu odebíraných výtisků jsou prováděny do 15 dnů. Lhůta pro uplatnění reklamací je stanovena na 15 dnů od data rozeslání, po této lhůtě jsou reklamace vyřizovány jako běžné objednávky za úhradu. V písemném styku vždy uvádějte IČ (právnická osoba) a kmenové číslo předplatitele. Podávání novinových zásilek povoleno ŘPP Praha.

ISSN 1213-3442