VĚSTNÍK
ÚŘADU PRO OCHRANU OSOBNÍCH ÚDAJŮ
2007

Částka 47 | **10. prosince 2007** | **Cena 108,– Kč**

OBSAH

ÚVOD

Ve čtyřicáté sedmé částce Věstníku Úřadu pro ochranu osobních údajů najdete přehled zrušených registrací za období od 25. 9. do 25. 11. 2007.

Rubrika Sdělení Úřadu obsahuje příspěvek Novelizace zákona o ochraně osobních údajů. Materiál informuje o nezbytných úpravách některých českých právních předpisů v souvislosti se zajištěním plného zapojení ČR do schengenské spolupráce, zejména v oblasti využívání tzv. Schengenského informačního systému (SIS).

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

Ve Sdělení je publikován příspěvek k případům z praxe; jde o vyjádření Úřadu ke konkrétním problémům, které jsou Úřadu předloženy ke konzultaci. Tentokrát se Úřad vyjadřuje k možnosti použití osobních údajů z veřejných telefonních seznamů za účelem nabízení obchodu nebo služeb.

Součástí rubriky je také informace o 29. mezinárodní konferenci komisařů pro ochranu dat a soukromí, která se konala ve dnech 25. – 28. září 2007 v kanadském Montrealu. V příspěvku jsou publikovány tři rezoluce prezentující závěry a výsledky spolupráce delegátů této konference.

Posledním materiálem rubriky Sdělení je dokument Pracovní skupiny pro ochranu dat podle článku 29 (tj. čl. 29 směrnice 95/46/ES), která se zabývá problematikou ochrany osobních údajů a soukromí. Je jím Stanovisko č. 5/2007 k další dohodě mezi Evropskou unií a Spojenými státy americkými o zpracování údajů jmenné evidence cestujících (PNR – Passenger Name Records) a jejich předávání leteckými dopravci Ministerstvu vnitřní bezpečnosti Spojených států uzavřené v červenci 2007. Úřad přetiskuje oficiální překlady právně nezávazných dokumentů WP29 v jejich původní podobě a nepřebírá odpovědnost za případné nepřesnosti překladu.

Z materiálů Úředního věstníku Evropské unie je v této částce publikováno Nařízení evropského parlamentu a Rady (ES) týkající se zřízení, provozu a využívání Schengenského informačního systému druhé generace (SIS II). Jedná se o přetisk z Úředního Věstníku EU.

Přehled zrušených registrací

Číslo registrace	Subjekt	Datum zrušení
00002843/003	MĚSTO HABRY	4.10.2007
00002843/004	MĚSTO HABRY	4.10.2007
00003225/002	SEVEROČESKÁ ENERGETIKA,A.S.	4.11.2007
00003736/001	CCS ČESKÁ SPOLEČNOST PRO PLATEBNÍ KARTY A.S.	4.10.2007
00004089/001	SEVEROMORAVSKÁ ENERGETIKA, A.S.	4.11.2007
00004325/002	VÝCHODOČESKÁ ENERGETIKA,A.S.	27.10.2007
00004840/003	PIVOVARY STAROPRAMEN A.S.	19.10.2007
00005428/001	ZÁPADOČESKÁ ENERGETIKA,A.S.	27.10.2007
00005428/002	ZÁPADOČESKÁ ENERGETIKA,A.S.	27.10.2007
00005428/003	ZÁPADOČESKÁ ENERGETIKA,A.S.	27.10.2007
00005428/004	ZÁPADOČESKÁ ENERGETIKA,A.S.	27.10.2007
00005428/005	ZÁPADOČESKÁ ENERGETIKA,A.S.	27.10.2007
00005428/006	ZÁPADOČESKÁ ENERGETIKA,A.S.	27.10.2007
00005428/007	ZÁPADOČESKÁ ENERGETIKA,A.S.	27.10.2007
00005428/008	ZÁPADOČESKÁ ENERGETIKA,A.S.	27.10.2007
00005428/009	ZÁPADOČESKÁ ENERGETIKA,A.S.	27.10.2007
00005428/010	ZÁPADOČESKÁ ENERGETIKA,A.S.	27.10.2007
00005428/011	ZÁPADOČESKÁ ENERGETIKA,A.S.	27.10.2007
00005512/001	STŘEDOČESKÁ ENERGETICKÁ A.S.	4.11.2007
00005512/002	STŘEDOČESKÁ ENERGETICKÁ A.S.	4.11.2007
00005512/003	STŘEDOČESKÁ ENERGETICKÁ A.S.	4.11.2007
00005512/004	STŘEDOČESKÁ ENERGETICKÁ A.S.	4.11.2007
00005512/005	STŘEDOČESKÁ ENERGETICKÁ A.S.	4.11.2007
00005512/006	STŘEDOČESKÁ ENERGETICKÁ A.S.	4.11.2007
00006436/001	NEMOCNICE CHRUDIM	14.11.2007
00006436/002	NEMOCNICE CHRUDIM	14.11.2007
00007423/001	STATUTÁRNÍ MĚSTO KARVINÁ	7.10.2007
00007423/002	STATUTÁRNÍ MĚSTO KARVINÁ	7.10.2007
00007423/003	STATUTÁRNÍ MĚSTO KARVINÁ	7.10.2007
00007423/004	STATUTÁRNÍ MĚSTO KARVINÁ	7.10.2007
00007423/005	STATUTÁRNÍ MĚSTO KARVINÁ	7.10.2007
00007423/006	STATUTÁRNÍ MĚSTO KARVINÁ	7.10.2007
00007423/007	STATUTÁRNÍ MĚSTO KARVINÁ	7.10.2007
00007423/008	STATUTÁRNÍ MĚSTO KARVINÁ	7.10.2007
00007423/009	STATUTÁRNÍ MĚSTO KARVINÁ	7.10.2007
00007423/010	STATUTÁRNÍ MĚSTO KARVINÁ	7.10.2007
00007423/A11	STATUTÁRNÍ MĚSTO KARVINÁ	7.10.2007
00007423/A12	STATUTÁRNÍ MĚSTO KARVINÁ	7.10.2007
00019939/001	ŠKOLEASE S.R.O.	3.11.2007
00027401/001	BP ČR, S.R.O.	2.11.2007
00030235/001	CCS ČESKÁ SPOLEČNOST PRO PLATEBNÍ KARTY A.S.	17.10.2007
00031028/001	ENERGETICKÉ STROJÍRNY BRNO, A.S.	16.11.2007

II. SDĚLENÍ ÚŘADU

Novelizace zákona o ochraně osobních údajů

V souvislosti s přípravou České republiky na vstup do schengenského prostoru, tj. společného prostoru, v němž nejsou prováděny kontroly na vnitřních hranicích mezi členskými státy, bylo nezbytné upravit některé české právní předpisy tak, aby bylo zajištěno plné zapojení ČR do schengenské spolupráce, zejména v oblasti využívání tzv. Schengenského informačního systému (SIS).

Potřebné změny byly provedeny zákonem č. 170/2007 Sb., kterým se mění některé zákony v souvislosti se vstupem České republiky do schengenského prostoru, a který byl vyhlášen ve Sbírce zákonů (tj. nabyl platnosti) dne 12. června 2007. Tímto zákonem byly novelizovány veškeré právní předpisy, jejichž změna byla zapotřebí, a proto se tomuto zákonu také někdy říká „schengenský balíček".

Novelizovány byly konkrétně tyto předpisy:

- zákon č. 283/1991 Sb., o Policii České republiky,
- zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád),
- zákon č. 326/1999 Sb., o pobytu cizinců na území České republiky,
- zákon č. 325/1999 Sb., o azylu,
- zákon č. 185/2004 Sb., o Celní správě České republiky,
- zákon č. 13/1993 Sb., celní zákon,
- zákon č. 361/2000 Sb., o provozu na pozemních komunikacích (zákon o silničním provozu),
- zákon č. 56/2001 Sb., o podmínkách provozu vozidel na pozemních komunikacích,
- zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů,
- zákon č. 119/2002 Sb., o střelných zbraních a střelivu a o změně zákona č. 156/2000 Sb., o ověřování střelných zbraní, střeliva a pyrotechnických předmětů a o změně zákona č. 288/1995 Sb., o střelných zbraních a střelivu (zákon o střelných zbraních).

Vzhledem k tomu, že zmíněné legislativní změny bylo z důvodu nezbytných příprav zapotřebí uvést v účinnost s jistým předstihem, byla i účinnost zmíněné novely stanovena již k 1. září tohoto roku (k tomuto datu bylo českým orgánům umožněno využívat informace ze SIS a také některá data vkládat).

Na tomto místě lze zmínit, že Česká republika podstatnou část schengenského „acquis"[1)] implementovala již před svým vstupem do Evropské unie, neboť na základě tzv. Schengenského protokolu Amsterodamské smlouvy ze dne 1. května 1999 bylo schengenské acquis začleněno do institucionálního rámce EU. Z původně mezivládní úrovně tak byla schengenská spolupráce přesunuta na úroveň EU, buďto jako součást I. nebo III. pilíře, a předpisy přijímané po tomto datu představují unijní právní předpisy platné (s určitými výjimkami) pro všechny členské státy. Dle uvedeného protokolu se stalo schengenské acquis závazné v plném rozsahu také pro všechny budoucí členské státy EU včetně České republiky.

V souladu se Smlouvou o přistoupení k Evropské unii byly nově přistoupivší státy od počátku povinny aplikovat část schengenského acquis (někdy také nazývané schengenské acquis I. kategorie). Ohledně zbývající části schengenského acquis (schengenské acquis II. kategorie) bylo stanoveno, že bude prováděna až na základě jednomyslného rozhodnutí Rady EU, kterému bude předcházet ověření připravenosti kandidátské země na plné zapojení do schengenské spolupráce.

Zákon č. 170/2007 Sb., tak pouze završil proces implementace schengenského acquis tím, že především vytvořil právní podmínky pro fungování SIS v České republice. Současně byly provedenými změnami zohledněny výsledky schengenských evaluací České republiky[2)].

Co se týče jednotlivých novelizovaných právních předpisů, lze ve stručnosti uvést, že změny zákona o Policii České republiky směřovaly především k určení Policie ČR (resp. Policejního prezidia) jako subjektu odpovědného za zřízení a provoz národní součásti SIS. Zároveň došlo změnou citovaného zákona k rozšíření práv subjektů údajů požadovat informace o osobních údajích, které o nich policie vede (konkrétně došlo ke zrušení lhůty jednoho roku pro opakování žádosti o tyto informace). Do trestního řádu byla doplněna ustanovení zakotvující právní podmínky pro výměnu informací mezi justičními orgány a Policejním prezidiem za účelem využívání SIS pro potřeby trestního řízení. V zákoně o pobytu cizinců byly provedeny změny upřesňující přeshraniční rozměr rozhodnutí o správním vyhoštění, upravující výčet údajů vkládaných do SIS a stanovující působnost ředitelství služby cizinecké a pohraniční policie k vkládání záznamů o cizincích, kterým má být odepřen vstup a pobyt na území schengenských států, do SIS. Dále byl do tohoto zákona a také do zákona o azylu vložen výčet orgánů s právem přístupu k SIS, jejichž konkretizaci komunitární právo vyžaduje.

Schengenský balíček dále obsahoval přesun úpravy problematiky zpracování osobních údajů v celní oblasti z celního

[1)] Soubor všech právních předpisů

[2)] Evaluační proces proběhl ve všech oblastech schengenské spolupráce, kterými jsou ochrana vnějších hranic, policejní a justiční spolupráce, vízová a konzulární spolupráce, ochrana osobních údajů a provoz Schengenského informačního systému, přičemž výsledkem každé hodnotící mise byly zprávy obsahující doporučení na zlepšení právního prostředí nebo praxe v dané oblasti. Pokrok v nápravě zjištěných nedostatků byl následně sledován a hodnocen.

zákona do zákona o Celní správě České republiky a současně zakotvil právo celních orgánů na přístup do SIS. Zákony upravující silniční provoz, resp. podmínky provozu na pozemních komunikacích, byly doplněny o ustanovení vztahující se k registru řidičů a registru silničních vozidel, v nichž budou vedeny některé nové kategorie údajů korespondující s SIS.

Změny provedené v zákoně o ochraně osobních údajů se týkaly především úpravy kompetencí Úřadu pro ochranu osobních údajů v tom smyslu, aby byla zajištěna jeho pravomoc dohlížet na řádné zpracování osobních údajů v SIS, upřesnění terminologie, doplnění výjimek pro zpracování citlivých údajů a dále zpřesnění povinností správců osobních údajů v oblasti zabezpečení zpracovávaných dat. Tyto změny byly provedeny na základě hodnotící zprávy evaluační mise v oblasti ochrany osobních údajů, která proběhla na jaře roku 2006.

Konkrétní změny provedené novelou č. 170/2007 Sb. v zákoně o ochraně osobních údajů vyplývají z následující tabulky:

Změny zákona o ochraně osobních údajů provedené zákonem č. 170/2007 Sb.	
znění před novelizací	**znění po novelizaci**
§ 2 odst. 2 Úřadu jsou svěřeny kompetence ústředního správního úřadu pro oblast ochrany osobních údajů v rozsahu stanoveném tímto zákonem a další kompetence stanovené zvláštním právním předpisem.	**§ 2 odst. 2** Úřadu jsou svěřeny kompetence ústředního správního úřadu pro oblast ochrany osobních údajů v rozsahu stanoveném tímto zákonem a další kompetence stanovené zvláštním právním předpisem, mezinárodními smlouvami, které jsou součástí právního řádu, a přímo použitelnými předpisy Evropských společenství.
§ 2 odst. 3 **neexistoval**	**§ 2 odst. 3** Úřad vykonává působnost dozorového úřadu pro oblast ochrany osobních údajů vyplývající z mezinárodních smluv, které jsou součástí právního řádu.
§ 4 písm. b) Citlivým údajem je osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a jakýkoliv biometrický nebo genetický údaj subjektu údajů.	**§ 4 písm. b)** Citlivým údajem je osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů.
§ 9 písm. i) **neexistoval**	**§ 9 písm. i)** *(Citlivé údaje je možné zpracovávat, jen jestliže)* se jedná o zpracování podle zvláštních zákonů při předcházení, vyhledávání, odhalování trestné činnosti, stíhání trestných činů a pátrání po osobách.
§ 13 odst. 3 neexistoval	**§ 13 odst. 3** V rámci opatření podle odstavce 1 správce nebo zpracovatel posuzuje rizika týkající se a) plnění pokynů pro zpracování osobních údajů osobami, které mají bezprostřední přístup k osobním údajům, b) zabránění neoprávněným osobám přistupovat k osobním údajům a k prostředkům pro jejich zpracování, c) zabránění neoprávněnému čtení, vytváření, kopírování, přenosu, úpravě či vymazání záznamů obsahujících osobní údaje a d) opatření, která umožní určit a ověřit, komu byly osobní údaje předány.

§ 13 odst. 4 neexistoval	**§ 13 odst. 4** V oblasti automatizovaného zpracování osobních údajů je správce nebo zpracovatel v rámci opatření podle odstavce 1 povinen také a) zajistit, aby systémy pro automatizovaná zpracování osobních údajů používaly pouze oprávněné osoby, b) zajistit, aby fyzické osoby oprávněné k používání systémů pro automatizovaná zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby, c) pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány, a d) zabránit neoprávněnému přístupu k datovým nosičům.
§ 29 odst. 1 písm. a) *(Úřad)* provádí dozor nad dodržováním povinností stanovených tímto zákonem.	**§ 29 odst. 1 písm. a)** *(Úřad)* provádí dozor nad dodržováním povinností stanovených zákonem při zpracování osobních údajů.
§ 29 odst. 1 písm. c) *(Úřad)* přijímá podněty a stížnosti na porušení tohoto zákona a informuje o jejich vyřízení.	**§ 29 odst. 1 písm. c)** *(Úřad)* přijímá podněty a stížnosti na porušení povinností stanovených zákonem při zpracování osobních údajů a informuje o jejich vyřízení.
§ 29 odst. 1 písm. g) *(Úřad)* zajišťuje plnění požadavků vyplývajících z mezinárodních smluv, jimiž je Česká republika vázána.	**§ 29 odst. 1 písm. g)** (Úřad) zajišťuje plnění požadavků vyplývajících z mezinárodních smluv, jimiž je Česká republika vázána, a z přímo použitelných předpisů Evropských společenství.

K § 2 odst. 2

Doplnění tohoto ustanovení mělo za cíl jednoznačně v zákoně o ochraně osobních údajů zakotvit, že je Úřadu svěřena působnost ústředního správního orgánu pro oblast ochrany osobních údajů bez ohledu na to, zda ke zpracování dat dochází na základě zákona o ochraně osobních údajů, jiných zákonů nebo mezinárodních smluv, které jsou součástí právního řádu ČR (tj. včetně schengenských úmluv), a že Úřad je v České republice oním příslušným subjektem, kompetentním plnit roli nezávislého dozorového orgánu.

K § 2 odst. 3

Tímto ustanovením byla jednoznačněji doplněna již dříve vyjádřená pozice Úřadu jako dozorového úřadu ve smyslu mezinárodních smluv, které jsou součástí právního řádu ČR, a v nichž je výslovně zakotven závazek smluvních stran určit nezávislý dozorový orgán pro oblast ochrany osobních údajů. Navrhovaná (relativně obecná) dikce současně zajišťuje, že nedojde k omezení působnosti Úřadu pouze na oblast zpracování osobních údajů v SIS, neboť jeho kompetence vyplývají i z jiných mezinárodních smluv, např. o Europolu.

K § 4 písm. b)

Provedená úprava znění tohoto ustanovení směřovala k upřesnění toho, které biometrické údaje jsou z hlediska zákona o ochraně osobních údajů považovány za citlivé. Původní znění umožňovalo totiž výklad, že na veškeré biometrické údaje je třeba pohlížet jako na citlivé, čímž mohly být na příslušné správce kladeny nepřiměřené požadavky (odlišné od praxe v Evropské unii). Nicméně ne každý biometrický údaj sám o sobě umožňuje přímo, bez spojení s jinými údaji, identifikovat konkrétní fyzickou osobu a tyto biometrické údaje tak nemohou být citlivými údaji (jako příklad lze uvést údaj o váze či velikosti nohy). Definice citlivého údaje byla proto zpřesněna a tím byly omezeny povinnosti správců a zpracovatelů na užší, skutečně „citlivou“, množinu biometrických údajů. Důvodem této změny v souvislosti s schengenskou problematikou byla skutečnost, že v oblasti bezpečnosti a policejní praxe jsou biometrické údaje stále častěji využívány a již v současné době je připravován Schengenský informační systém druhé generace, který bude biometriku (konkrétně biometrické údaje získané z otisků prstů a fotografií obličeje) obsahovat.

K § 9 písm. i)

Doplněním tohoto ustanovení byla do výčtu situací, kdy lze zpracovávat citlivé údaje (např. informace o náboženském vyznání nebo etnické příslušnosti), výslovně vložena oblast předcházení, vyhledávání, odhalování trestné činnosti, stíhání trestných činů a pátrání po osobách. Tato změna neznamená, že by snad dříve nebylo možné citlivé údaje pro tyto činnosti zpracovávat, když je zjevné, že práce policie nebo státních zastupitelství je mnohdy na citlivých údajích přímo založena, tyto postupy však byly předmětem dílčích úprav ve zvláštních zákonech (zejména zákon o Policii ČR nebo trestní řád). Doplnění tohoto obecného zmocnění tak směřuje ke zvýšení transparentnosti právní úpravy v oblasti zpracování osobních údajů a současně vychází vstříc požadavku podřadit zpracování osobních údajů v Schengenském informačním systému, v němž budou zpracovávány i citlivé údaje, pod režim obecné úpravy ochrany osobních údajů a nikoliv pod režim výjimek.

K § 13 odst. 3 a 4

Motivací k doplnění těchto ustanovení byla dlouhodobá zkušenost Úřadu s praxí v oblasti zajištění bezpečnosti zpracovávaných dat, resp. s dodržováním povinnosti stanovené v § 13 odst. 1 zákona o ochraně osobních údajů. Citované ustanovení ukládá správcům a zpracovatelům povinnost přijmout taková opatření, aby nedošlo k ohrožení anebo nedovolenému nakládání s osobními údaji, přičemž rozhodnutí o tom, jaká konkrétní opatření jsou v daném případě nezbytná ponechával zákon o ochraně osobních údajů na jednotlivých správcích, popř. zpracovatelích. Tato velmi obecně vyjádřená povinnost byla však ze strany povinných subjektů častým terčem kritiky. Cílem doplněných ustanovení tak byla specifikace konkrétních povinností správců a zpracovatelů při zajištění plnění této povinnosti, a to zejména s ohledem na stále častější zpracování dat v rámci rozsáhlých automatizovaných databází (mezi něž patří i SIS). V této souvislosti je dále třeba zdůraznit, že nová ustanovení nepřináší nové povinnosti, ani další byrokratickou zátěž, neboť zhodnocení vyjmenovaných rizik a přijetí odpovídajících opatření bylo již dříve povinností vyplývající z § 13 odst. 1 zákona o ochraně osobních údajů, ke kterému se ostatně nově vložené odstavce váží.

K § 29 odst. 1 písm. a)

Touto úpravou došlo ke zpřesnění vyjádření dozorové působnosti Úřadu, který je oprávněn provádět dozor nejen nad dodržováním povinností stanovených přímo zákonem o ochraně osobních údajů, ale i podle zvláštních zákonů, v nichž jsou upraveny postupy při zpracování osobních údajů. Nejedná se o změnu dosavadního přístupu Úřadu, neboť ten byl vždy při výkonu své dozorové činnosti nucen se vypořádat se systematikou právního řádu, kdy povinnosti v oblasti ochrany dat nejsou upraveny pouze na obecné úrovni (v zákoně o ochraně osobních údajů), ale často také formou výjimek (zvláštních pravidel pro odůvodněné případy) v jiných právních předpisech. Uvedená změna primárně řeší nejasnosti ve výkladu kompetencí Úřadu, které byly kritizovány v průběhu schengenského hodnocení a které by dle názoru evropských expertů mohly vést ke zpochybnění dozorové kompetence Úřadu.

K § 29 odst. 1 písm. c)

Tato změna přináší především výslovné zakotvení kompetence Úřadu přijímat podněty a stížnosti na porušení povinností pro zpracování osobních údajů stanovené jak v zákoně o ochraně osobních údajů, tak ve zvláštních zákonech upravujících agendu zpracování dat, mj. právě v oblasti Schengenského informačního systému. Uvedenou úpravou došlo také ke sladění tohoto ustanovení s již zmíněnými § 2 odst. 2 a § 29 odst. 1 písm. a), neboť dozorová činnost Úřadu je mj. založena na podnětech a stížnostech týkajících se podezření z nesprávného zpracování osobních údajů.

K § 29 odst. 1 písm. g)

Zpřesněním formulace tohoto ustanovení došlo k zohlednění způsobu implementace mezinárodních smluv vyplývajících z přistoupení k Evropské unii a zavazujících Českou republiku v oblasti ochrany osobních údajů. Jednoznačně tak byla stanovena kompetence Úřadu k plnění těchto závazků a byly odstraněny některé nejasnosti a pochybnosti, které v tomto směru mohly (i dle názoru schengenské hodnotící mise) při plnění dozoru nad SIS vzniknout.

Zapojení České republiky do schengenského prostoru je jednou z priorit české zahraniční politiky. Za podmínky splnění všech schengenských standardů, včetně zprovoznění SIS, by měl být schengenský prostor rozšířen o 9 nových členských států EU (kromě ČR se jedná o Estonsko, Litvu, Lotyšsko, Maďarsko, Maltu, Polsko, Slovensko a Slovinsko[3)] dne 21. prosince 2007[4)].

Cílem zmíněné novely (tj. zákona č. 170/2007 Sb.) bylo po legislativní stránce umožnit bezproblémové začlenění ČR do schengenské spolupráce ve všech jejích oblastech a upravit činnost všech zainteresovaných orgánů tak, aby mohly co nejlépe plnit své nové úkoly. Z hlediska Úřadu tak došlo bezpochyby ke zvýšení úrovně základního právního předpisu v oblasti ochrany osobních údajů (tj. zákona o ochraně osobních údajů) a k vyjasnění kompetencí Úřadu ve vztahu k nadnárodním, sdíleným databázím, jejichž rozšiřování a stále častější využívání lze v budoucnu předpokládat[5)].

[3)] Kypr, který je desátým novým členem EU přijatým v roce 2004, deklaroval svůj zájem vstoupit do Schengenu až poté, co bude uveden do provozu Schengenský informační systém druhé generace (SIS II).

[4)] Původně avizované datum 31. prosince 2007 bylo změno na základě iniciativy portugalského předsednictví EU; jedná se více méně o politický krok. K rozšíření má dojít o půlnoci z 20. na 21. prosince 2007, tento pátek před vánočními svátky tak bude prvním „schengenským" dnem ČR.

[5)] Bližší informace ke vstupu ČR do Schengenu naleznete na webových stránkách Euroskop.cz anebo na stránkách Úřadu v rubrice Schengen.

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 projednávaných Úřadem pro ochranu osobních údajů v rámci své rozhodovací činnosti.

1. K vedení daňového řízení

Správce osobních údajů může při výkonu své běžné činnosti, kterou je v daném případě vedení daňového řízení, a v souladu se zásadou účelnosti zpřístupňovat osobní údaje svým jednotlivým zaměstnancům, třetím osobám, se kterými je ve smluvním vztahu, nebo dalším osobám, které v rámci plnění zákonem stanovených oprávnění přicházejí u správce do styku s osobními údaji. V případě řízení podle zákona č. 337/1992 Sb., o správě daní a poplatků, se podle § 1 odst. 2 tohoto zákona správou daně rozumí právo činit opatření potřebná ke správnému a úplnému zjištění, stanovení a splnění daňových povinností. V souladu s tímto principem se nelze vůči správci daně dovolávat porušení povinnosti mlčenlivosti, pokud za účelem správného a úplného vyměření daňové povinnosti poskytl potřebné informace ze spisu daňového subjektu znalci k vypracování znaleckého posudku, který je podle § 31 odst. 4 zákona č. 337/1992 Sb. jedním z důkazních prostředků v daňovém řízení. Okruh osob, které se účastní daňového řízení, je vymezen v § 7 odst. 1 a 2 zákona č. 337/1992 Sb., které stanovují jako osoby zúčastněné na daňovém řízení pověřené pracovníky správce daně, daňové subjekty a třetí osoby, přičemž za třetí osoby uvádí mj. i znalce. Povinnost mlčenlivosti znalce je poté zajištěna jednak § 24 odst. 1 zákona č. 337/1992 Sb., o které musí být v souladu s § 24 odst. 2 tohoto zákona předem poučen, a jednak obecnou úpravou povinnosti mlčenlivosti o osobních údajích v § 15 odst. 1 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, kdy znalec je osobou, která přichází do styku s osobními údaji v rámci plnění zákonem stanovených oprávnění a povinností. Závěrem proto lze konstatovat, že není, v souladu se shora uvedenými závěry, porušením povinnosti mlčenlivosti, poskytne-li finanční úřad znalci pro vypracování znaleckého posudku příslušné listiny z daňového spisu.

Současně je ale nutné uvést, že správce daně musí při vedení daňového řízení jako správce osobních údajů dodržet povinnost stanovenou v § 5 odst. 1 písm. f) zákona č. 101/2000 Sb., tedy povinnost zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny. Proto může správce daně v daňovém řízení poskytnout znalci pouze ty listiny, které znalec bezprostředně potřebuje pro vypracování svého znaleckého posudku. V této souvislosti je dále nutné konstatovat, že na zpracování osobních údajů v běžném daňovém řízení se výjimka uvedená v § 3 odst. 6 zákona č. 101/2000 Sb. nevztahuje, neboť takovéto řízení nelze považovat za významný finanční zájem České republiky nebo Evropské unie ve smyslu ustanovení § 3 odst. 6 písm. f) tohoto zákona. Povinnosti správce osobních údajů uvedené v § 5 odst. 1 zákona č. 101/2000 Sb. se proto na správce daně při takovémto daňovém řízení vztahují v plném rozsahu.

Ustanovení § 24 odst. 3 zákona č. 337/1992 Sb. poté z hlediska zákona č. 101/2000 Sb. poněkud nadbytečně upravuje oprávnění pracovníků správců daně ve vztahu k jiným pracovníkům správce daně a odvolacímu orgánu. Ostatní oprávnění pracovníků správce daně, které znamenají výjimku z povinnosti mlčenlivosti, se týkají poskytování informací třetím subjektům, vůči kterým by jinak platila absolutní povinnost mlčenlivosti. *(zn. cs02319/06)*

2. K vyžadování údajů z evidence obyvatel

Postup okresního soudu, tj. získání osobních údajů stěžovatele z informačního systému evidence obyvatel a jejich využití v rámci soudního řízení, tak směřoval k naplnění jeho povinností stanovených zákonem č. 99/1963 Sb., občanský soudní řád, podle kterého byl okresní soud povinen postupovat v soudním řízení tak, aby věc byla co nejrychleji projednána a rozhodnuta. V situaci, kdy se stěžovateli (žalovanému) nedařilo doručovat, byl tedy okresní soud oprávněn vyžádat si poskytnutí osobních údajů stěžovatele a jeho rodičů z informačního systému evidence obyvatel a využít je k dotazu na platnou adresu stěžovatele. Současně byl okresní soud oprávněn zahájit, a to i bez návrhu, opatrovnické řízení, neboť okresní soud je podle zákona č. 99/1963 Sb. povinen ustanovit opatrovníka osobám, které ho podle zákona mít musejí, přičemž důvodem pro ustanovení opatrovníka je jak neznámý pobyt účastníka řízení, tak neúspěšnost doručování na adresu v cizině. V rámci opatrovnického řízení byl okresní soud oprávněn si vyžádat stanovisko rodičů stěžovatele, zda by byli ochotni roli opatrovníka vykonávat, neboť právní řád neukládá povinnost roli opatrovníka přijmout a okresní soud tímto postupem předchází možnosti, že ustanovený opatrovník se bude domáhat zrušení usnesení, jímž mu byla tato role svěřena. Okresní soud tedy při oslovení rodičů stěžovatele využil standardní, v obdobných situacích běžně užívaný postup.

Zpřístupnění osobních údajů stěžovatele, v rozsahu nezbytném pro zdůvodnění dotazu na místo pobytu stěžovatele a možnost přijetí role opatrovníka, jeho rodičům, lze považovat za zpracování osobních údajů prováděné v souladu s § 5 odst. 2 písm. a) zákona č. 101/2000 Sb., podle kterého může správce osobních údajů (okresní soud) zpracovávat osobní údaje bez souhlasu subjektu údajů (stěžovatele), jestliže provádí zpracování nezbytné pro dodržení právní povinnosti správce. Právní povinnost správce je přitom v tomto případě založena zákonem č. 99/1963 Sb. *(zn. cs02441/06)*

3. Ke zveřejňování osobních údajů na internetu

Obviněný tím, že systematicky shromažďoval a zveřejňoval prostřednictvím internetových stránek, které spravuje, zápisy ze schůzí a usnesení rady města obsahující osobní údaje osob, jejichž záležitosti projednávala, tj. zpracovával osobní údaje ve smyslu § 4 písm. e) zákona č. 101/2000 Sb., a to za účelem informovat o činnosti rady města, byl správcem těchto osobních údajů podle § 4 písm. j) zákona č. 101/2000 Sb., neboť určil účel a prostředky zpracování osobních údajů, toto zpracování prováděl a tedy za něj odpovídal. Ze shora uvedeného dále vyplývá, že údaje obsažené ve zveřejněných dokumentech jsou osobními údaji podle § 4 odst. a) zákona č. 101/2000 Sb. a v některých případech i údaji citlivými ve smyslu § 4 odst. b) tohoto zákona. Vzhledem k velikosti města a počtu jeho obyvatel je zřejmé, že k identifikaci konkrétní osoby postačuje již i např. jméno, příjmení a vztah k radou města projednávané věci.

Každý správce osobních údajů je povinen osobní údaje zpracovávat v souladu se zákonem č. 101/2000 Sb., který za účelem provedení ochrany ústavně zaručeného práva na soukromí stanoví zákonné limity pro nakládání s osobními údaji. Základním předpokladem legálního zpracování osobních údajů je existence souhlasu subjektu údajů se zpracováním osobních údajů, a to souhlasu předcházejícího předmětnému zpracování a uděleného po poučení v rozsahu podle § 5 odst. 4 a § 11 zákona č. 101/2000 Sb. Obviněný však existenci souhlasu se zpracováním osobních údajů těch, jejichž osobní údaje byly obsaženy v zápisech ze schůzí a v usneseních rady města, zveřejněním na internetových stránkách, neprokázal. Bez takového souhlasu je možné osobní údaje zpracovávat pouze, jedná-li se o některou z výjimek taxativně vyjmenovaných v § 5 odst. 2 písm. a) až g) zákona č. 101/2000 Sb., z nichž ovšem žádnou nelze na předmětné zpracování osobních údajů, prováděné obviněným, aplikovat. Navíc v případě citlivých údajů je k jejich zpracování zapotřebí výslovný souhlas subjektu údajů podle § 9 písm. a) zákona č. 101/2000 Sb., který obviněný též neprokázal, přičemž na předmětné zpracování citlivých údajů také nelze aplikovat žádnou z výjimek taxativně vyjmenovaných v § 9 písm. b) až ch) tohoto zákona.

Zákon č. 128/2000 Sb., o obcích (obecní zřízení), stanoví zvláštní úpravu poskytování informací o činnosti zastupitelstev a rad územních samosprávných celků, kdy osoby vymezené v § 16 odst. 1 a 3 a § 17 zákona č. 128/2000 Sb. (dále jen „občané obce“) jsou na základě § 16 odst. 1 písm. e) tohoto zákona oprávněny mj. nahlížet do usnesení a zápisů ze schůzí zastupitelstva obce a do usnesení rady obce a pořizovat si z nich výpisy. Uvedeným osobám tedy musejí být zpřístupněna usnesení rady, usnesení zastupitelstva města a zápis z jednání zastupitelstva města, a to v neanonymizované podobě, tj. včetně případných osobních údajů těch, o jejichž záležitostech bylo jednáno. Zákon č. 128/2000 Sb. tak upravuje právo konkrétně vymezeného okruhu osob (občanů obce) na zpřístupnění i takových informací (osobních údajů), které jsou obecně zákonem č. 101/2000 Sb. a zákonem č. 106/1999 Sb., o svobodném přístupu k informacím, chráněny. Skutečnost, že občané obce mají právo seznamovat se i s osobními údaji obsaženými v uvedených písemnostech, však nezakládá jejich oprávnění s takto nabytými informacemi dále volně nakládat.

Obdobně u obviněného, který jako zastupitel a člen rady města měl podle zákona č. 128/2000 Sb. právo přístupu k zápisům ze schůzí a usnesením rady města a právo seznamovat se s osobními údaji obsaženými v uvedených dokumentech, však toto právo nezakládalo jeho oprávnění s takto nabytými informacemi dále volně nakládat. Na další nakládání s osobními údaji, které občané obce a obviněný jako zastupitel a člen rady města uvedeným způsobem získají, je nutno dále aplikovat režim stanovený zákonem č. 101/2000 Sb.

Obec jako správce osobních údajů je plně odpovědná za dodržování zákona č. 101/2000 Sb., odpovědnost nesou také fyzické osoby uvedené v § 15 tohoto zákona, které v rámci plnění stanovených oprávnění a povinností přicházejí do styku s osobními údaji u správce. Obviněný byl, jako zastupitel města, bezpochyby na základě zákona č. 128/2000 Sb. oprávněn se s předmětnými osobními údaji seznámit, již ale nikoli je dále zpřístupňovat prostřednictvím svých internetových stránek, tedy zcela neomezenému okruhu subjektů.

Dále byl obviněný povinen zachovávat mlčenlivost o osobních údajích, se kterými přicházel do styku v rámci plnění zákonem č. 128/2000 Sb. stanovených oprávnění a povinností. Jak navíc vyplývá z písemného materiálu, zaslalo město obviněnému opakovaně upozornění na nezákonnost jeho jednání a dále rozeslalo zastupitelům k předmětné problematice vysvětlující dopis. Správní orgán se nemůže ztotožnit ani s názorem obviněného, že jeho jednání bylo vynuceným rizikem pro řádný výkon jeho funkce zastupitele vzhledem k jednání města. *(zn. 2/06/PŘ)*

4. K porušení povinnosti mlčenlivosti zaměstnancem

Družstvo v souvislosti se správou domů nakládá, především za účelem správy domů a zajištění služeb spojených s užíváním bytových jednotek, s osobními údaji obyvatel těchto domů (jak nájemníků, tak vlastníků jednotek), a to buď v roli správce osobních údajů ve smyslu § 4 písm. j) zákona č. 101/2000 Sb. nebo jejich zpracovatele podle § 4 písm. k) tohoto zákona. Zaměstnanci družstva jsou tak bezpochyby vázáni povinností mlčenlivosti podle § 15 zákona č. 101/2000 Sb. ve vztahu k osobním údajům, ke kterým získají při výkonu své činnosti pro družstvo přístup.

Družstvo může v souladu s § 5 odst. 2 písm. a) zákona č. 101/2000 Sb. zpracovávat (tj. i prostřednictvím svých zaměstnanců) osobní údaje nezbytné k dosažení uvedeného účelu (správy domů a zajištění služeb spojených s užíváním bytových jednotek) i bez souhlasu dotčených subjektů údajů (nájemníků a vlastníků), přičemž v souladu s tímto účelem je i pravidelné informování o činnosti družstva o majetkových poměrech v družstvu a v jednotlivých společenstvích vlastníků, neboť členové družstva a vlastníci bytů mají právo tyto

údaje, včetně nezbytných osobních údajů ostatních členů družstva a vlastníků, znát mj. proto, aby mohli řádně vykonávat svá práva a povinnosti při rozhodování na shromáždění vlastníků jednotek či na členské schůzi. Je však nezbytné zdůraznit, že tyto informace lze zpřístupnit pouze osobám, které jsou majetkově zainteresovány v tomtéž subjektu.

Zpřístupnění informací o existenci a výši dluhu váznoucím na určité bytové jednotce tak může být v souladu s právním řádem, tj. zákonem č. 101/2000 Sb., pouze za předpokladu, že byla tato informace zpřístupněna pouze omezenému okruhu oprávněných osob, v daném případě zjevně pouze ostatním vlastníkům bytových jednotek v domě. Vzhledem k tomu, že z pohledu družstva tvoří jednotlivé domy, v nichž vykonává správu, samostatná hospodářská střediska, je zjevné, že majetkově propojení jsou pouze vlastníci bytů v jednotlivých domech (tj. spoluvlastníci a družstvo), nikoli vlastníci všech bytů spadajících pod správu družstva. Informace o hospodaření společenství vlastníků tak mohou být sdělovány pouze vlastníkům jednotek v daném domě.

Jestliže byla tedy zpřístupněna informace o dluhu váznoucím na bytové jednotce na schůzi, které se mohli zúčastnit vlastníci jednotek ze všech uvedených domů a i další osoby (nájemníci), nelze tento postup považovat za jednání v souladu se zákonem č. 101/2000 Sb. Vzhledem k okolnostem, při nichž došlo ke zpřístupnění předmětné informace (k čemuž došlo náhodně v rámci vyhrocené diskuze), je zřejmé, že ke zpřístupnění osobních údajů týkajících se dluhu nedošlo na základě pokynu družstva, ale z rozhodnutí obviněné, která tuto informaci získala v rámci svého zaměstnání u družstva. *(zn. 4/06/PŘ)*

5. K provozování kamerového systému na pracovišti[1)]

Vzhledem k tomu, že záznamy pořízené kamerovým systémem umožňují identifikaci jednotlivých osob, je nutno veškeré informace o konkrétních osobách tímto způsobem zaznamenané považovat za osobní údaje ve smyslu § 4 písm. a) zákona č. 101/2000 Sb. Jestliže byl kamerový systém v prostorách kanceláře a sekretariátu instalován osobou v pozici statutárního orgánu účastníka řízení, je účastník řízení ve vztahu k těmto osobním údajům (shromážděným prostřednictvím kamerového systému) jejich správcem ve smyslu § 4 písm. j) zákona č. 101/2000 Sb. a odpovídá za dodržení veškerých povinností stanovených tímto zákonem při zpracování osobních údajů.

Jednou ze základních povinností správce osobních údajů podle zákona č. 101/2000 Sb. je povinnost vyjádřená v § 5 odst. 2 tohoto zákona, tedy povinnost zpracovávat osobní údaje zásadně pouze se souhlasem subjektu údajů, o jehož údaje se jedná. Bez takového souhlasu je možné osobní údaje zpracovávat pouze v případech zákonem č. 101/2000 Sb. taxativně vyjmenovaných v § 5 odst. 2 písm. a) až g). Žádnou z těchto výjimek však na popsané zpracování osobních údajů prostřednictvím kamerového systému aplikovat nelze a účastník řízení byl tedy povinen disponovat souhlasem osob, které byly kamerami zachyceny, tj. osob, jejichž osobní údaje zpracovával. Z vyjádření statutárního orgánu, že zaměstnanci účastníka řízení nebyli o existenci instalovaného systému informováni, je však zjevné, že účastník řízení zpracovával osobní údaje těch, kteří procházeli kanceláří či sekretariátem statutárního orgánu účastníka řízení (tj. zaměstnanců i osob mimo organizační struktury účastníka řízení), bez jejich souhlasu.

Důvod instalace kamerového systému prezentovaný statutárním orgánem, tj. prevence protiprávního jednání v jeho kanceláři a sekretariátu v mimopracovní době, sice zřejmě směřuje k aplikaci výjimky podle § 5 odst. 2 písm. e) zákona č. 101/2000 Sb., který umožňuje zpracovávat osobní údaje bez souhlasu subjektu údajů, jedná-li se o nezbytnou ochranu práv a právem chráněných zájmů správce, nicméně na toto ustanovení se v daném případě nelze odvolávat. Podmínkou postupu podle § 5 odst. 2 písm. e) zákona č. 101/2000 Sb. je totiž ve větě druhé vyjádřená povinnost nezasahovat takovým zpracováním do práva subjektů údajů na ochranu soukromého a osobního života. Utajená instalace kamerového systému (pouze na základě rozhodnutí statutárního orgánu účastníka řízení a bez jednoznačného stanovení pravidel provozu, využívání dat a správy tohoto systému) v prostorách kanceláří, v nichž jsou i v souladu s ustálenou judikaturou Evropského soudu pro lidská práva[2)] zaměstnanci oprávněni očekávat jistou míru soukromí, je v rozporu s uvedenou podmínkou, a to zejména za situace, kdy tento systém zaznamenával dění v uvedených prostorách v pracovní době a fakticky tak sloužil k monitorování zaměstnanců.

Smyslem právní úpravy ochrany osobních údajů obsažené v zákoně č. 101/2000 Sb. je ochrana subjektu údajů před újmou na jeho právech (zejména právu na zachování lidské důstojnosti a soukromí), před neoprávněným zasahováním do jeho soukromého a osobního života a před neoprávněným zpracováním osobních údajů. Tato základní práva, která jsou zakotvena v čl. 7 odst. 1 a 10 usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení Listiny základních práv a svobod, jako součásti ústavního pořádku České republiky, musí mít přednost před jinými než výše uvedenými zájmy správce na zpracování osobních údajů. V případě kamerového sledování je tedy nezbytné striktně uplatňovat zásadu přiměřenosti jeho využití, tj. tyto systémy lze použít pouze v případě, když se jiná opatření směřující k prevenci ukáží být nedostatečnými. Rozsah zpracovávaných údajů musí být současně přiměřený sledovaným účelům. Riziko zásahu do právem chráněných zájmů správce, opravňující k aplikaci výjimky stanovené v § 5 odst. 2 písm. e) zákona č. 101/2000 Sb., by muselo být takové intenzity, aby dokázalo převýšit zájem na ochraně soukromí subjektu údajů, což v tomto případě nebylo splněno.

[1)] Rozhodnutí vychází z právního stavu k 13. říjnu 2006. Problematika používání kamerových systémů zaměstnavatelem je přitom v současné době řešena odlišně, viz zejména § 316 odst. 2 zákona č. 262/2006 Sb., zákoník práce.

[2)] viz např. rozhodnutí Evropského soudu pro lidská práva ve věci Niemietz v. Německo z roku 1992

Účastník řízení, jako správce osobních údajů shromážděných prostřednictvím předmětného kamerového systému, je dále na základě § 13 odst. 1 zákona č. 101/2000 Sb. povinen všechny zpracovávané osobní údaje zabezpečit takovým způsobem, aby nemohlo dojít k jejich neoprávněnému zpracování či jinému zneužití. Ze skutečnosti, že došlo k odcizení pevného disku obsahujícího záznamy z kamer, jednoznačně vyplývá, že pořizované záznamy (tedy i osobní údaje v nich obsažené) nebyly dostatečně chráněny. Instalace kamerového systému, vzhledem k tomu, že takové opatření představuje již významný zásah do soukromí sledovaných osob, musí být z hlediska principů ochrany osobních údajů a soukromí vždy až krajním řešením a musí být vždy provázena přijetím jednoznačných pravidel pro jeho provoz, tedy mj. i pravidly pro zabezpečení zpracovávaných dat, včetně pravidelné kontroly funkčnosti systému. Pokud není kamerový systém řádně nastaven a kontrolován, vystavuje se správce, který jej instaloval, riziku, že pochybením systému nebo nezaregistrovanou změnou nastavení dojde ke zpracování osobních údajů v rozsahu, který již nezamýšlel a který překračuje stanovený účel, a tedy riziku, že za takové zpracování ponese plnou odpovědnost. Na tomto místě je také nutno uvést, že k naplnění správního deliktu porušením povinnosti stanovené v § 13 odst. 1 zákona č. 101/2000 Sb. postačí již jen existence stavu, kdy jsou zpracovávané osobní údaje vystaveny riziku ztráty či zneužití. Jestliže účastník řízení instaloval kamerový systém a současně nepřijal přiměřená opatření technického i organizačního charakteru zahrnující mj. i pravidelnou údržbu a správu instalovaného zařízení, včetně náležité dokumentace přijatých opatření v souladu s § 13 odst. 2 zákona č. 101/2000 Sb., vystavil zpracovávané osobní údaje nedůvodnému riziku neoprávněného zpracování či ztráty, a postupoval tedy v rozporu s tímto zákonem.

Nelze souhlasit ani s tvrzením zástupce účastníka řízení, že v daném případě se jednalo o nahodilé shromáždění osobních údajů bez jejich dalšího zpracování podle § 3 odst. 4 zákona č. 101/2000 Sb. Instalace kamerového monitorovacího systému za účelem pravidelného monitorování určitých prostor bezpochyby směřuje k systematickému zpracování osobních údajů těch, kteří budou na záznamech kamer případně zachyceni. Situaci, kdy správce osobních údajů stanoví účel zpracování, provede instalaci prostředků zpracování a následně jejich prostřednictvím shromáždí osobní údaje, nelze hodnotit jako nahodilé shromáždění dat. Obdobně nelze souhlasit s tvrzením, že instalaci kamer provedl statutární orgán účastníka řízení jako soukromá fyzická osoba pro svou osobní potřebu. Zpracování osobních údajů prostřednictvím monitorovacího zařízení instalovaného na pracovišti, kde se oprávněně pohybují i třetí osoby, nelze považovat za zpracování osobních údajů pro osobní potřebu ve smyslu § 3 odst. 3 zákona č. 101/2000 Sb., zejména jestliže deklarovaným účelem bylo zabránění krádeži majetku ve vlastnictví účastníka řízení z prostor jeho sídla. *(zn. 42/06/SŘ)*

6. Ke zpracování rodného čísla exekutorem

Účastník řízení při výkonu své činnosti soukromého exekutora shromažďuje a dále zpracovává osobní údaje účastníků exekučního řízení a je tedy správcem osobních údajů ve smyslu § 4 písm. j) zákona č. 101/2000 Sb. Jedním z takto zpracovávaných údajů je také rodné číslo, které je nepochybně osobním údajem ve smyslu § 4 písm. a) zákona č. 101/2000 Sb. Podle § 13 odst. 7 zákona č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel), je oprávněna užívat nebo rozhodovat o jeho využívání výlučně fyzická osoba, které bylo rodné číslo přiděleno, nebo její zákonný zástupce; jinak lze rodné číslo využívat jen v případech stanovených v § 13c tohoto zákona. Podle § 13c odst. 1 písm. a) zákona č. 133/2000 Sb. lze rodné číslo využívat, jen jde-li o činnost ministerstev, jiných správních úřadů, orgánů pověřených výkonem státní správy, soudů, vyplývající z jejich zákonem stanovené působnosti, nebo notářů pro potřebu vedení Centrální evidence závětí. Podle § 28 zákona č. 120/2001 Sb., o soudních exekutorech a exekuční činnosti (exekuční řád) a o změně dalších zákonů, se úkony exekutora při provádění exekuce považují za úkony soudu, proto lze konstatovat, že soudní exekutor je oprávněn využívat při své činnosti rodná čísla. Tento závěr vyplývá také z ustanovení § 33a odst. 3 písm. a), b) i c) zákona č. 120/2001 Sb., podle kterých lze soudním exekutorům pro vedení exekuce poskytnout z informačního systému evidence obyvatel a z registru rodných čísel mimo jiné právě rodné číslo fyzické osoby. Současně je ale nutné konstatovat, že ačkoliv mají správní orgány a soudy podle § 13c odst. 1 písm. a) zákona č. 133/2000 Sb. obecné zmocnění k využívání rodných čísel, nelze jej vykládat tak, že by mohly s rodným číslem neomezeně nakládat, ale musejí při jeho používání současně respektovat ustanovení § 5 odst. 1 písm. f) zákona č. 101/2000 Sb., podle něhož je správce povinen zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly při výkonu činnosti exekutora shromážděny. Žádný právní předpis přitom nepředpokládá, že by rodné číslo bylo zpracováváno za účelem zveřejnění, současně ani žádný právní předpis, konkrétně zákon č. 99/1963 Sb., občanský soudní řád, nestanoví, že by usnesení nebo rozsudek měly obsahovat v označení účastníků jejich rodné číslo.

V předmětné věci uvedl účastník řízení rodné číslo povinného v usnesení o ceně nemovitosti podle § 336a zákona č. 99/1963 Sb. Náležitosti usnesení jsou stanoveny v § 169 odst. 1 zákona č. 99/1963 Sb., podle kterého se v usnesení uvede mimo jiné označení účastníků. V souladu s ustanovením § 167 odst. 2 zákona č. 99/1963 Sb. lze poté na usnesení užít ustanovení o rozsudku; § 157 odst. 1 zákona č. 99/1963 Sb. vyžaduje „přesné označení účastníků“, podle věty poslední tohoto ustanovení se, je-li to možné uvede v označení účastníků též jejich datum narození (identifikační číslo). Logickým výkladem lze poté dospět k jednoznačnému závěru, že požadavek na uvedení data narození vedle požadavku na „přesné označení účastníků“ v rozsudku (a tedy i v usnesení) znamená, že ono „přesné označení účastníků“ nezahrnuje uvedení jejich rodného čís-

la, neboť poté by bylo uvádění data narození účastníků řízení naprosto nadbytečné. Lze odkázat také na komentář k občanskému soudnímu řádu (Bureš J. a kol.: Občanský soudní řád: Komentář, C.H.Beck, Praha 2003, 6. vydání[3)], který v případě označení účastníků řízení v rozsudku odkazuje na označení účastníků v žalobě; zde se uvádí, že fyzickou osobu jako účastníka řízení je třeba označit jménem, příjmením a bydlištěm. Je-li to potřebné nebo nutné (ten, kdo podává návrh, například nezná bydliště nebo se účastník v místě bydliště nezdržuje, ve stejném místě bydlí více osob, které mají stejné jméno a příjmení apod.), je potřebné uvést i další údaje (datum narození, rodné číslo, místo kde se zdržuje, místo podnikání). K tomuto je nutné dodat, že rodné číslo, jakožto obecný identifikátor fyzické osoby požívající zvláštní právní ochrany podle zákona č. 133/2000 Sb. lze použít až jako poslední možnost, přičemž v naprosté většině případů bude dostačovat identifikace účastníka řízení prostřednictvím jména, příjmení, bydliště a data narození.

Argumentaci účastníka řízení, že v exekučním řízení je nutné, či snad dokonce jedině možné, naprosto přesně identifikovat povinného prostřednictvím rodného čísla, je s ohledem na shora uvedené v rozporu se současnou platnou právní úpravou, mimo jiné také proto, že požadavek na identifikaci účastníka řízení před soudem je vždy stejný, bez ohledu na to, zda se jedná o běžné civilní nalézací řízení, trestní řízení nebo o exekuční řízení, přičemž v prvních dvou případech není v rozsudku rodné číslo účastníků běžně uváděno. Současně by totiž ad absurdum bylo možné dospět k závěru, že nelze nařídit exekuci na základě rozsudku, který neobsahuje rodné číslo účastníků, neboť by soud neměl jistotu, že bude exekuce nařízena skutečně proti povinnému, který má povinnost uloženou rozsudkem plnit, protože by nebyl v rozsudku dostatečně přesně identifikován.

Pokud se jedná o další možnosti využití rodného čísla podle § 13c zákona č. 133/2000 Sb., tak v případě uvedeném v § 13c odst. 1 písm. b) tohoto zákona, tedy stanoví-li tak zvláštní zákon, vyplývá ze shora uvedeného, že žádný zvláštní zákon uvádění rodného čísla ve výroku usnesení nestanovuje. Podle § 13c odst. 1 písm. c) zákona č. 133/2000 Sb. lze také rodné číslo využívat se souhlasem jeho nositele nebo jeho zákonného zástupce, tento souhlas ovšem účastník řízení v průběhu správního řízení nedoložil, přestože k tomu byl správním orgánem vyzván. Souhlasem s využitím rodného čísla podle tohoto ustanovení je, s ohledem na absenci zvláštní úpravy, nutno rozumět souhlas se zpracováním osobních údajů podle zákona č. 101/2000 Sb., který musí být účastník řízení po celou dobu zpracování schopen prokázat.

Obdobně nelze oprávnění k využívání rodných čísel pro identifikaci žalovaných vyvozovat ani ze skutečnosti, že jak katastr nemovitostí, jenž je veřejnou evidencí dostupnou i ve formě dálkového přístupu, tak i list vlastnictví, jako veřejná listina, rodná čísla obsahují a tak je zpřístupňují široké veřejnosti. Zpracování rodných čísel v souvislosti s vedením katastru nemovitostí je v souladu s § 13c odst.1 písm. a) zákona č. 133/2000 Sb. Avšak ani zákon č. 344/1992 Sb., o katastru nemovitostí České republiky (katastrální zákon), ani jiný právní předpis neobsahuje oprávnění uživatelů této evidence volně disponovat se zde uvedenými rodnými čísly.

K uveřejnění usnesení o ceně na internetových stránkách exekutorského úřadu lze konstatovat, že i tento způsob zpracování osobních údajů povinného je v rozporu s § 5 odst. 1 písm. f) zákona č. 101/2000 Sb., neboť žádný právní předpis neukládá soudnímu exekutorovi usnesení o ceně podle § 336a zákona č. 99/1963 Sb. tímto způsobem zveřejnit. Podle § 336a odst. 4 zákona č. 99/1963 Sb. se usnesení o ceně doručí oprávněnému, těm, kdo do řízení přistoupili jako další oprávnění, povinnému a osobám, o nichž je známo, že pro ně váznou na nemovitosti práva nebo závady. Toto usnesení se proto nijak dále veřejně nepublikuje oproti např. usnesení o nařízení dražebního jednání (dražební vyhlášce), kdy § 336c zákona č. 99/1963 Sb. naopak přímo stanoví, že se vyvěsí na úřední desce soudu, obecního úřadu, v jehož obvodu se nemovitost nachází, příslušného katastrálního úřadu, a lze ji také v odůvodněných případech uveřejnit v celostátním nebo místním tisku nebo jiným vhodným způsobem. Proto správní orgán ve smyslu čl. 2 odst. 3 zákona č. 1/1993 Sb., Ústava České republiky, podle kterého lze státní moc uplatňovat jen v případech, v mezích a způsoby, které stanoví zákon, považuje uveřejnění usnesení o ceně na internetových stránkách účastníka řízení za zpracování osobních údajů, které není v souladu s účelem, pro který byly shromážděny. *(zn. 43/06/SŘ)*

7. Ke zpracování osobních údajů dlužníků

D. shromažďuje ve smyslu § 4 písm. f) zákona č. 101/2000 Sb. osobní údaje osob, vůči nimž má pohledávku, a je tedy podle § 4 písm. j) tohoto zákona správcem těchto osobních údajů. K tomuto účelu také provádí další zpracování osobních údajů těchto osob ve smyslu § 4 písm. e) zákona č. 101/2000 Sb., např. osobní údaje uchovává, třídí nebo předává. Účastník řízení má s D. uzavřenu mandátní smlouvu, podle které vymáhá pohledávky D. vůči těmto osobám, jestliže ji nezaplatily podle pracovníků D. řádně a včas, a to ani poté, co v souvislosti s tímto zjištěním byly k zaplacení vyzvány. Na základě pověření v této smlouvě proto zpracovává účastník řízení osobní údaje osob, vůči nimž pro D. vymáhá pohledávky.

V daném případě je jednoznačné, že účastník řízení provádí zpracování těchto osobních údajů ve smyslu § 4 písm. e) zákona č. 101/2000 Sb., neboť tyto osobní údaje např. používá, předává, uchovává, třídí. Současně považuje správní orgán za prokázané, že je naplněna i druhá podmínka definice zpracování, na které se vztahuje zákon č. 101/2000 Sb., a to požadavek, aby shora uvedené operace s osobními údaji byly prováděny systematicky. Prvek systematičnosti je dán tím, že některá z operací charakterizujících pojem zpracování podle ustanovení § 4 písm. e) zákona č. 101/2000 Sb. je prováděna s určitým záměrem. V případě účastníka řízení je také prvek

[3)] strana 244

systematičnosti obsažen v samotném způsobu, jakým jsou osobní údaje D. vedeny a účastníku řízení předávány, kdy se jedná o společnou počítačovou síť. Dále lze uvést, že účastník řízení se v mandátní smlouvě zavazuje, že povede evidenci všech převzatých pohledávek, a to jednak ve formě dokumentace a jednak ve formě počítačové dokumentace (vedení evidence pohledávek nepochybně odpovídá pojmu uchovávání v definici zpracování podle § 4 písm. e) zákona č. 101/2000 Sb.), přičemž esenciální složkou vedení každé dokumentace je prvek systematičnosti.

Na základě shora uvedeného považuje správní orgán činnost účastníka řízení v souvislosti s vymáháním pohledávek pro D. podle mandátní smlouvy za zpracování osobních údajů ve smyslu § 4 písm. e) zákona č. 101/2000 Sb. prováděnou v postavení zpracovatele těchto osobních údajů podle § 4 písm. k) tohoto zákona. K tomu je třeba konstatovat, že je právně irelevantní ustanovení mandátní smlouvy, ve kterém se uvádí, že na informace, které D. předává pro účely vymáhání pohledávek, se v žádném případě nevztahuje režim stanovený zákonem č. 101/2000 Sb. Zákon č. 101/2000 Sb. je předpisem veřejného práva, jehož aplikaci strany nemohou smluvně vyloučit a vyhnout se tím povinnostem z něj vyplývajících.

D. zpracovává osobní údaje F. za účelem vymáhání svých pohledávek, přičemž účastníka řízení pověřil v mandátní smlouvě zpracováním těchto osobních údajů za totožným účelem. Podle § 7 zákona č. 101/2000 Sb. platí povinnosti stanovené v § 5 obdobně také pro zpracovatele. Podle ustanovení § 5 odst. 1 písm. f) zákona č. 101/2000 Sb. je správce povinen zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny. Účastník řízení přesto zpracovával osobní údaje F. i po zaplacení dlužné částky, kdy z celkové evidence pohledávek vybral ty, které se jí týkají, a poté je zveřejnil v tiskovém prohlášení; zveřejnění je přitom jedním ze způsobů zpracování ve smyslu ustanovení § 4 písm. e) zákona č. 101/2000 Sb. Toto zpracování osobních údajů neodpovídá žádnému z účelů, pro který je účastník řízení na základě mandátní smlouvy oprávněn osobní údaje dlužníků D. zpracovávat, současně lze konstatovat, že neodpovídá ani účelu, pro který osobní údaje zpracovává D. *(zn. 47/06/SŘ)*

8. Ke zpracování osobních údajů žadatelů podle zákona č. 106/1999 Sb.

Účastník řízení je ve smyslu § 4 písm. j) zákona č. 101/2000 Sb. správcem osobních údajů žadatelů o poskytnutí informací podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, a to za účelem řádného vyřízení jejich žádosti podle citovaného zákona a případného poskytnutí požadované informace. Rozsah zpracovávaných osobních údajů je pro tento účel vymezen v § 14 odst. 2 zákona č. 106/1999 Sb., který stanovuje náležitosti žádosti. Podle § 5 odst. 1 písm. f) zákona č. 101/2000 Sb. je správce osobních údajů povinen zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny. Zpracovávat k jinému účelu lze osobní údaje jen v mezích ustanovení § 3 odst. 6 zákona č. 101/2000 Sb., které na tento případ nedopadá, nebo pokud k tomu dal subjekt údajů předem souhlas, nebo v případech vymezených v § 5 odst. 2 písm. a) až g) zákona č. 101/2000 Sb. Pokud tedy účastník řízení zveřejnil na tiskové konferenci údaj o tom, kolik žádostí podle zákona č. 106/1999 Sb. podal F., mohl tak učinit pouze se souhlasem tohoto subjektu údajů nebo v případech uvedených v § 5 odst. 2 písm. a) až g) tohoto zákona, které upravují výjimky ze shora uvedeného pravidla a umožňují zpracování osobních údajů bez souhlasu subjektu údajů.

Pokud se jedná o možnost zpracovávat osobní údaje bez souhlasu subjektu údajů na základě ustanovení § 5 odst. 2 písm. f) zákona č. 101/2000 Sb., tedy pokud správce poskytuje osobní údaje o veřejně činné osobě, funkcionáři či zaměstnanci veřejné správy, které vypovídají o jeho veřejné nebo úřední činnosti nebo o jeho funkčním zařazení, tak je nutno uvést, že se tato výjimka vztahuje pouze na úzce vymezený způsob zpracování osobních údajů, kterým je poskytnutí osobních údajů. Pojem poskytnutí osobních údajů je přitom nutno chápat úžeji než zveřejnění; v případě zveřejnění se jedná o zpřístupnění osobních údajů neurčitému počtu adresátů, zatímco v případě poskytnutí jsou osobní údaje zpřístupněny jednomu, případně většímu, vždy však přesně vymezenému okruhu adresátů. Z tohoto důvodu se na jednání účastníka řízení nemůže použít výjimka uvedená v § 5 odst. 2 písm. f) zákona č. 101/2000 Sb., a dle správního orgánu je tedy nerozhodné, zda je F. osobou veřejně činnou ve smyslu tohoto zákona a zda se zveřejněný údaj týkal jeho veřejné činnosti.

Výjimku uvedenou v § 5 odst. 2 písm. e) zákona č. 101/2000 Sb., dle které lze bez souhlasu subjektu údajů zpracovávat osobní údaje, pokud je to nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby, přičemž takové zpracování nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života, nelze na zveřejnění údaje na tiskové konferenci účastníkem řízení použít. Základním kritériem, dle kterého lze určit, zda jde o zpracování nezbytné pro ochranu práv a právem chráněných zájmů správce je to, zda je takovéto zpracování schopno vůbec dosáhnout zamýšleného účelu, tedy ochrany práv správce. Dle názoru správního orgánu zpřístupnění údaje o počtu žádostí podaných F. podle zákona č. 106/1999 Sb. veřejnosti nemůže nijak omezit jeho právo tyto žádosti dále podávat a uplatňovat tak svoje zákonná práva. Ostatně i sám účastník řízení ve svém vyjádření uvádí, že se počet žádostí od listopadu 2005 podaných F. nijak nesnížil, ale má naopak stoupající tendenci. Současně lze konstatovat, že veškeré negativní články, stejně jako udělení ceny „Zavřeno“ účastníkovi řízení, následovalo až po zveřejnění předmětné informace na tiskové konferenci, a nemohly být způsobilé poškodit dobré jméno účastníka řízení před tímto zveřejněním.

Správní orgán dále posoudil možnost aplikace ostatních zákonných výjimek z povinnosti zpracovávat osobní údaje pouze se souhlasem subjektů údajů, zejména poté s ohledem na zákon č. 106/1999 Sb., ve znění účinném ke dni 18. listopadu 2005, ve vztahu k ustanovení § 5 odst. 2 písm. a) zákо-

na č. 101/2000 Sb. Ze zákona č. 106/1999 Sb. vyplývá, že každý povinný subjekt poskytuje informace podle tohoto zákona buď na základě žádosti nebo zveřejněním. Jelikož v tomto případě došlo k poskytnutí informací zveřejněním, je pro posouzení jednání účastníka řízení relevantní ustanovení § 5 zákona č. 106/1999 Sb., které vymezuje rozsah povinně zveřejněných údajů. Pod toto ustanovení nelze dle správního orgánu předmětné zveřejnění informace na tiskové konferenci podřadit. Dále je pak nutné podotknout, že ačkoliv ustanovení § 5 odst. 4 zákona č. 106/1999 Sb. připouští možnost s výjimkami uvedenými v tomto zákoně zveřejnit i další informace, za uvedenou výjimku je nutno chápat tehdy platné a účinné ustanovení § 2 odst. 3 tohoto zákona (nyní ustanovení § 8a), dle kterého se zákon nevztahuje na poskytování osobních údajů a informací podle zvláštního předpisu. I v tomto případě je proto nutné respektovat povinnost zpracovávat osobní údaje pouze se souhlasem subjektu údajů. Stejně tak ustanovení § 18 odst. 1 zákona č. 106/1999 Sb. upravující výroční zprávu o činnosti v oblasti poskytování informací vyžaduje zveřejnit celkový počet podaných žádostí, tj. údaj bez identifikace jednotlivých žadatelů. Závěrem lze tedy konstatovat, že ani ze zákona č. 106/1999 Sb. nevyplývá oprávnění účastníka řízení zveřejnit informaci, kolik žádostí podle tohoto zákona podala konkrétní fyzická osoba, bez jejího souhlasu.

V případě ústavněprávní roviny tohoto správního řízení, jak ji uvádí účastník řízení ve svém vyjádření, je nutno konstatovat, že vždy vedle práva na svobodu projevu a informace je nutno zvažovat také právo každého na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě zakotveným v čl. 10 odst. 3 Listiny základních práv a svobod, jako jedno ze základních lidských práv. K provedení tohoto práva byl zákonodárcem přijat zákon č. 101/2000 Sb. Ostatně, dle správního orgánu, je nutné na tento případ pohlížet především z hlediska ustanovení čl. 17 odst. 5 Listiny základních práv a svobod, dle kterého jsou státní orgány a orgány územní samosprávy povinny přiměřeným způsobem poskytovat informace o své činnosti, přičemž podrobnosti jsou upraveny v zákoně č. 106/1999 Sb. *(zn. 51/06/SŘ)*

9. Ke zpracování rodných čísel klientů v souvislosti s dodávkami elektřiny

Správce osobních údajů má podle § 5 odst. 1 písm. d) zákona č. 101/2000 Sb. povinnost shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění tohoto účelu. V případě účastníka řízení byl v předmětném období rozsah osobních údajů, které lze za účelem uzavření a plnění smlouvy o dodávkách elektřiny shromažďovat, vymezen vyhláškami Energetického regulačního úřadu č. 18/2002 Sb., o podmínkách připojení a dopravy elektřiny v elektrizační soustavě, vyhláškou č. 297/2001 Sb., kterou se stanoví podmínky připojení a dodávek elektřiny pro chráněné zákazníky, které byly účinné v době spáchání správního deliktu. Oprávnění shromažďovat rodná čísla nevyplývá ani z vyhlášky č. 51/2006 Sb., o podmínkách připojení k elektrizační soustavě, účinné od 1. března 2006, která nahradila obě shora uvedené vyhlášky. Současně lze konstatovat, že ani žádný jiný právní předpis nestanoví obecně povinnost využívat rodná čísla v souvislosti s uzavřením smlouvy.

Nakládat s rodným číslem lze pouze v případech stanovených v § 13 odst. 7 a § 13c odst. 1 zákona č. 133/2000 Sb.. Oprávnění stanovené pro orgány státní správy v § 13c odst. 1 písm. a) zákona č. 133/2000 Sb. se na účastníka řízení jednoznačně nevztahuje, oprávnění v § 13c odst. 2 písm. b) tohoto zákona v daném případě také nelze použít, neboť žádný zvláštní zákon nestanovuje povinnost provozovateli distribuční soustavy elektrické energie identifikovat svého zákazníka rodným číslem. Nakládat s rodným číslem by tak účastník řízení mohl v předmětné věci pouze se souhlasem nositele rodného čísla, kterým je nutno rozumět souhlas ve smyslu § 4 písm. n) zákona č. 101/2000 Sb., tj. svobodný a vědomý projev vůle nositele rodného čísla. Zároveň je nutné konstatovat, že tento souhlas musí splňovat obsahové náležitosti stanovené v § 5 odst. 4 zákona č. 101/2000 Sb., tj. vymezení účelu a doby zpracování, stanovení k jakým osobním údajům se vztahuje a jakému správci je poskytován, současně mu musí předcházet splnění informační povinnosti podle § 11 odst. 1 a 2 tohoto zákona, zejména poučení o tom, zda je poskytnutí rodného čísla povinné nebo dobrovolné. Souhlas nositele rodného čísla nebo jeho zákonného zástupce podle § 13c odst. 1 písm. c) zákona č. 133/2000 Sb. v dokumentech, jejichž prostřednictvím účastník řízení rodná čísla shromažďoval, tj. zejména v žádosti o stanovení podmínek připojení, žádosti o distribuci, dodávce nebo sdružených službách dodávky elektřiny, ani ve smlouvě o dodávce elektřiny, obsažen není, účastník řízení v rámci provedené kontroly souhlas neprokázal ani jiným způsobem. *(zn. 55/06/SŘ)*

10. Ke zpracování osobních údajů zaměstnavatelem

Zaměstnavatel může zpracovávat osobní údaje svých zaměstnanců bez jejich souhlasu pouze za účelem dodržení svých právních povinností uložených mu zvláštními zákony. Pokud zpracovává jejich osobní údaje k jinému účelu, než ukládají zvláštní zákony, pak je k takovému zpracování nutný souhlas subjektu údajů, kterým je nutno rozumět souhlas ve smyslu § 4 písm. n) zákona č. 101/2000 Sb., tj. svobodný a vědomý projev vůle subjektu údajů resp. nositele rodného čísla, jehož obsahem je jeho svolení se zpracováním daného osobního údaje ke konkrétnímu účelu.

Ze spisového materiálu však vyplývá, že jméno, příjmení a rodné číslo stěžovatelky bylo využito na pověření bez jejího souhlasu. K vyjádření účastníka řízení lze konstatovat, že to, že zaměstnanec ví, že bylo vystaveno hromadné pověření obsahující rodná čísla i na jeho jméno a jak a proč je s ním dále nakládáno (o čemž jsou zaměstnanci školeni a informováni na pracovních školeních svého oddělení), nelze považovat za vyslovení souhlasu ve smyslu § 4 písm. n) zákona č. 101/2000 Sb., tj. za svobodný a vědomý projev vůle nositele rodného čísla. Takovým souhla-

sem není ani vědomí zaměstnanců o skutečnostech na pověření uvedených a o veškerých souvislostech nakládání a používání tohoto pověření a tedy i údajů uvedených na tomto dokumentu, ani podpis tohoto pověření, když navíc lze z vyjádření účastníka řízení dovodit, že souhlasem zaměstnance byl podmiňován výkon zaměstnání resp. dané činnosti v rámci zaměstnání, i když právní předpisy uvádění rodného čísla zaměstnance jednajícího za účastníka řízení při právních úkonech spojených s řízením o povolení vkladu zástavního práva či s jeho výmazem z katastru nemovitostí nevyžadují. K tomu lze také konstatovat, že i pokud by existoval souhlas zaměstnance se zpřístupněním jeho osobních údajů, vztahoval by se na tento případ konstantní názor Pracovní skupiny pro ochranu jednotlivců v souvislosti se zpracováním osobních údajů, jako poradního orgánu zřízeného podle čl. 29 Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995, o ochraně jednotlivců v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, vyjádřený mj. i ve stanovisku č. 8/2001 ze dne 13. září 2001, týkající se zpracování osobních údajů v pracovněprávních vztazích, že zpracování osobních údajů v rámci pracovněprávních vztahů na základě souhlasu by se mělo omezit zásadně na situace, kdy má zaměstnanec skutečně svobodnou volbu s postupem zaměstnavatele nesouhlasit a možnost následně svůj souhlas odvolat, a to bez jakýchkoli následků. V situaci, kdy je zaměstnanec žádán o poskytnutí souhlasu se zpracováním osobních údajů, přičemž ale existuje riziko jakékoli újmy v případě odmítnutí souhlasu, nelze ani udělený souhlas považovat za platný právní úkon.

K vyjádření účastníka o souhlasu stěžovatelky a novém textu souhlasu, kde je uvedeno explicitně také rodné číslo, lze konstatovat, že v obou těchto souhlasech subjekty údajů souhlasí se zpracováním osobních údajů k účelům tam uvedeným, nikoliv k využití na pověřeních sloužících k podepisování smluv o zřízení zástavního práva k nemovitostem, návrhů na zahájení řízení o povolení vkladu zástavního práva účastníka řízení a veškerých právních úkonů spojených s řízením o povolení vkladu zástavního práva do katastru nemovitostí. Dále lze konstatovat, že účastník řízení také nevyvrátil stěžovatelkou uváděnou skutečnost, že používal pověření s jejím rodným číslem i po skončení jejího pracovního poměru, ale naopak z jeho vyjádření vyplývá, že takový stav, kdy na pověření jsou osobní údaje osob, které již nejsou jeho zaměstnanci, je s ohledem na frekvenci aktualizací údajů v pověření pravidlem. *(zn. 56/06/SŘ)*

Poznámka:

[1] Za jednotlivými texty, které jsou rozděleny do tématických okruhů, jsou vždy kurzívou uvedeny interní čj. nebo zn., pod kterými jsou jednotlivé případy v Úřadu evidovány.

[2] Materiál je také k dispozici na internetové adrese Úřadu www.uoou.cz v rubrice Správní řízení.

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ K PROBLÉMŮM Z PRAXE

č. 2/2007

listopad 2007

Možnost použití osobních údajů z veřejných telefonních seznamů

Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „zákon o ochraně osobních údajů“) v § 5 odst. 5 mj. stanoví, že při zpracování (tedy např. i shromažďování, používání atd.) osobních údajů za účelem nabízení obchodu nebo služeb může správce či zpracovatel použít jméno, příjmení a adresu subjektu údajů bez jeho souhlasu v případě, že údaje byly získány z veřejného seznamu.

Jeden typ veřejných seznamů, s nimiž řada správců pro výše uvedené účely pracuje, upravuje zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů. Dle § 95 citovaného zákona je veřejným seznamem i seznam účastníků telefonické sítě. Podle § 41 zákona o elektronických komunikacích je povinností podnikatelů zajišťujících veřejně dostupné sítě a poskytujících veřejně dostupné služby elektronických komunikací vést, distribuovat, vydávat a nejméně jednou ročně aktualizovat telefonní seznam účastníků všech podnikatelů poskytujících veřejně dostupné telefonní služby.

Pro vydávání telefonních seznamů zákon o elektronických komunikacích stanoví několik pravidel, z nichž z pohledu ochrany osobních údajů jsou důležitá pravidla vyplývající z § 88 odst. 1 a § 95 zákona o elektronických komunikacích.

Podle uvedeného § 88 odst. 1 je podnikatel poskytující veřejně dostupnou službu elektronických komunikací povinen technicky a organizačně zajistit bezpečnost poskytované služby s ohledem na ochranu osobních údajů fyzických osob. Jedná se o promítnutí požadavku, který na správce a zpracovatele osobních údajů klade § 13 zákona o ochraně osobních údajů, tedy povinnosti přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu, zneužití či k manipulaci se zpracovávanými osobními informacemi.

V § 95 zákona o elektronických komunikacích jsou uvedeny povinnosti toho, kdo osobní údaje účastníků pro potřeby vydání jejich seznamu shromažďuje. Z nich je v kontextu výše uvedeného ustanovení zákona o ochraně osobních údajů důležité zejména to, že ten, kdo hodlá seznam vydat, je povinen zajistit,

aby účastníci mohli u svých osobních údajů uvést, že si nepřejí být kontaktováni za účelem marketingu. Ustanovení § 96 zákona o elektronických komunikacích stanoví, že je zakázáno nabízet marketingovou reklamu nebo jiný způsob nabídky zboží a služeb těm účastníkům, kteří podle § 95 citovaného zákona uvedli, že si to nepřejí.

Zákon o elektronických komunikacích nabyl účinnosti v roce 2005 a od té doby platí uvedené povinnosti těch, kteří shromažďují osobní údaje pro vydání seznamu účastníků. Úřad se však ve své činnosti setkal s případy, kdy si občané stěžovali, že byli osloveni za účelem nabídky obchodů či služeb, přestože v aktuálním účastnickém seznamu je uvedeno, že si tak nepřejí, a nebo již jejich osobní údaje v tomto seznamu vůbec nejsou.

Přestože společnost rozesílající nabídky může disponovat telefonním seznamem, jež byl vydán před účinností zákona o elektronických komunikacích a nenaplňuje tedy výše uvedenou podmínku § 95 tohoto zákona, nelze na základě této skutečnosti zasílat nabídky obchodu a služeb těm účastníkům telefonické sítě, kteří na základě § 95 zákona o elektronických komunikacích u svých údajů v telefonním seznamu uvedli, že si nepřejí být za tímto účelem kontaktováni, nebo jejichž údaje již v seznamu nejsou.

Citovaná ustanovení §§ 95 a 96 zákona o elektronických komunikacích byla podle důvodové zprávy k tomuto zákonu přijata proto, že právo na soukromí fyzických osob a oprávněné zájmy právnických osob vyžadují, aby účastníci mohli určit, zda a které jejich osobní údaje budou v seznamu uvedeny. Pokud konkrétní účastník uvede, že si nepřeje být oslovován za účelem marketingu, nebo již nadále své osobní údaje v seznamu účastníků neuvádí, tak by nabízení služeb a obchodu se zdůvodněním, že nabízející disponuje starším seznamem, bylo jednoznačným a nepřípustným obcházením zákona. Jednalo by se tak o správní delikt dle § 45 odst. 1 písm. e) zákona o ochraně osobních údajů a mohlo by jít i o správní delikt dle § 118 odst. 1 písm. j) zákona o elektronických komunikacích.

V návaznosti na shora uvedené je tedy dle názoru Úřadu nezbytné, aby ty subjekty, které hodlají používat osobní údaje získané z telefonních seznamů k nabízení obchodu nebo služeb, používaly jako zdroj těchto údajů telefonní seznamy aktuální, tedy poslední vydanou verzi. V opačném případě se vystavují riziku postihu dle výše uvedených sankčních ustanovení.

Poznámka: Materiál je také k dispozici na internetové adrese Úřadu www.uoou.cz v rubrice K problémům z praxe.

Závěry jednání 29. mezinárodní konference komisařů pro ochranu dat a soukromí

Montreal (25. – 28. září 2007)

Ve dnech 25. – 28. září 2007 se v Kanadě, v Montrealu, konala 29. mezinárodní konference komisařů pro ochranu osobních údajů. Pro letošní výroční setkání bylo zvoleno motto „Horizonty ochrany soukromí: Terra Inkognita“. Jednání se zúčastnili předsedové akreditovaných orgánů ochrany osobních údajů v doprovodu řídících pracovníků. Pozvání přijali i představitelé státní správy a podnikatelské sféry, kteří se zabývají problematikou ochrany osobních údajů. Nosnými tématy konference byly problémy zpracování dat v oblasti veřejné bezpečnosti s ohledem na nárůst světového terorismu, problémy globalizace z pohledu ochrany soukromí jednotlivce, rozvoj technologií ovlivňujících podmínky pro zpracování osobních dat, otázky zpracování dat z pohledu ochrany soukromí dětí, možnosti standardizace v této oblasti a společné aktivity úřadů a jejich komisařů. Program byl členěn na společná zasedání všech účastníků, doprovázená řadou workshopů a paralelních jednání expertů na konkrétní problematiku a na uzavřené zasedání předsedů úřadů jednotlivých států. Výsledkem spolupráce bylo přijetí tří společných usnesení.

Rezoluce o naléhavé potřebě celosvětových standardů pro ochranu dat cestujících, které by vlády uplatňovaly pro účely vymáhání práva a zabezpečení hranic

Navrhovatel: Spolkový komisař pro ochranu dat a svobodu informací, Německo

Přispěvatelé: Rakouská komise pro ochranu dat
Kanadský komisař pro ochranu soukromí
Komisař pro informace a ochranu soukromí, Britská Kolumbie
Komisař pro informace a ochranu soukromí, Ontario
Evropský inspektor ochrany údajů, Evropská unie
Národní komise pro informatiku a svobody, Francie
Zemský komisař pro ochranu dat a svobodu informací, Severní Porýní-Vestfálsko, Německo
Komisař pro ochranu osobních údajů, Itálie
Úřad pro ochranu osobních údajů, Nizozemí
Národní úřad pro dozor nad zpracováním osobních údajů, Rumunsko
Agentura pro ochranu dat, Španělsko
Federální komisař pro ochranu dat, Švýcarsko
Komisař pro informace, Velká Británie

Konference připomíná:

- komuniké přijaté na 24. mezinárodní konferenci v Cardiffu v roce 2002;
- usnesení o předávání dat cestujících přijaté na 25. mezinárodní konferenci v Sydney v roce 2003; a
- deklaraci o ochraně osobních údajů a soukromí v globalizovaném světě přijatá na 27. mezinárodní konferenci v Montreux v roce 2005;

ve kterých se uvádí potřeba nastolit rovnováhu mezi oprávněným bojem proti terorismu a mezinárodnímu zločinu a právem jednotlivce na ochranu dat a soukromí.

Konference konstatuje, že:

- vlády usilují stále více o data cestujících, aby je využily v boji proti terorismu, nezákonné imigraci a dalším zločinům, aniž by přitom braly dostatečný ohled na soukromí a lidská práva cestujících;
- z některých dat cestujících je možné odvodit informace o náboženství, etnické příslušnosti a jiných vysoce citlivých věcech;
- mnoho vlád po celém světě rostoucím způsobem požaduje od dopravců více a více údajů;
- dopravci shromažďují data cestujících pro obchodní účely a požaduje se na nich, aby je poskytovali za účelem prosazování práva;
- dopravci musejí stále více plnit řadu různých žádostí o údaje a vyrovnávat se s mnoha odlišnými systémy pro přenos dat, což jednak vyvolává nejistotu mezi dopravci a cestujícími ohledně jejich práv a povinností, neboť je pro cestující těžké pochopit, jak se s jejich údaji nakládá, a také vytváří riziko, že dopravci budou data předávat nepatřičným způsobem;
- tyto četné a různorodé požadavky a systémy vyvolávají náklady jak aeroliniím, tak cestujícím;
- vypořádat se s těmito požadavky znamená pro dopravce nároky na právní a technickou konzistenci;
- někteří dopravci stále ještě zcela neplní povinnost informovat cestující o používání a zpřístupňování jejich údajů; a
- byla zavedena další globální opatření, která mají usnadnit mezinárodní leteckou dopravu a existuje naléhavá potřeba vypracovat globální řešení, která by usnadňovala leteckou dopravu a současně respektovala práva cestujících na soukromí.

Konference znovu zdůrazňuje, že:

- právo na ochranu dat a právo na soukromí, jak jsou zakotvena v článku 12 Všeobecné deklarace lidských práv a dalších právních instrumentech, chrání jednotlivce a jejich osobní údaje a musejí být zohledněna vedle dalších práv v jakémkoli návrhu zahrnujícím předávání a používání dat cestujících pro účely prosazování práva;
- zpracování osobních údajů cestujících by se mělo provádět s přihlédnutím k uznávaným principům a normám ochrany dat;
- každý vládní návrh na využití údajů cestujících by měl prokázat, že je:
  - prokazatelně nutný pro řešení konkrétního problému;
  - prokazatelně vhodný k vyřešení daného problému;
  - proporcionální vůči bezpečnostnímu přínosu; a
  - zasahuje do soukromí prokazatelně méně než alternativní možnosti; a

  měl by být pravidelně revidován, aby se zajistilo, že opatření budou stále proporcionální;
- potřeba chránit soukromí osob, ať už vývojové trendy budou jakékoli, zůstává základním úkolem nejenom pro ochránce dat na celém světě, ale také pro ty, kterým leží na srdci základní práva a svobody; a
- pokud vlády nezaujmou přístup, který korektním způsobem nebude brát v úvahu obavy o ochranu dat a soukromí, bude existovat skutečné nebezpečí, že začnou podkopávat nejzákladnější svobody, které se snaží chránit.

Při hledání celosvětových standardů ochrany dat pro zabezpečení údajů cestujících, které by vlády uplatňovaly pro účely vymáhání práva a zabezpečení hranic, Konference vyzývá:

- mezinárodní organizace (jako jsou IATA[1] a ICAO[2], vlády a dopravce, aby pracovali s komisaři pro ochranu dat a soukromí na přijetí celosvětově závazných řešení, která budou zahrnovat náležitá opatření z hlediska ochrany dat;
- aby jakýkoli vládní návrh na využití dat cestujících zajišťoval, že je:
  - prokazatelně nutný pro řešení konkrétního problému;
  - prokazatelně vhodný k vyřešení daného problému;
  - proporcionální vůči bezpečnostnímu přínosu; a
  - zasahuje do soukromí prokazatelně méně než alternativní možnosti; a

  měl by být pravidelně revidován, aby se zajistilo, že opatření budou stále proporcionální;
- aby jakýkoli vládní program využívající data cestujících pamatoval na minimalizaci dat; jasná omezení jejich použití, zpřístupnění a uchovávání přiměřená účelu programu; přesnost dat; právo přístupu a opravy; nezávislý dohled;
- aby jakékoli řešení bralo v úvahu právní, technické, finanční a ekonomické aspekty na straně dopravců a úřadů;
- vlády, aby byly otevřené a transparentní ve věci účelů, pro které jsou data shromažďována a využívána a aby zajistily všem cestujícím, bez ohledu na jejich občanství nebo zemi původu, přístup k jejich osobním informacím a poskytovaly náležité opravné mechanismy;
- dopravce, aby odpovídajícím způsobem informovali cestující o jakémkoli použití a zpřístupnění jejich úda-

---

[1] International Air Transport Association (Mezinárodní asociace leteckých dopravců)

[2] ICAO kódy, které definuje Mezinárodní organizace pro civilní letectví.

jů vládám a orgánům pro vymáhání práva, o jakýchkoli seznamech osob vyloučených z přepravy nebo sledovaných a o možnosti nápravy s ohledem na použití a přesnost dat cestujících a souvisejících osobních informací; a

- komisaře pro ochranu dat a soukromí, aby dále spolupracovali na zajištění odpovídajících opatření v oblasti ochrany dat a soukromí a aby usilovali o závazná globální řešení.

Poznámka na vysvětlenou

Vlády různých států se rostoucí měrou snaží vyžadovat údaje cestujících jako nástroj ke zvládnutí terorismu, mezinárodního zločinu a jiné kriminality. To vede k rozdílnosti v požadovaných datových položkách, ve využívání těchto dat a úrovni ochranných opatření.

Povaha mezinárodního cestování vyžaduje celosvětový přístup a globální řešení je naléhavě nutné k zajištění náležité úrovně bezpečnosti a k probuzení důvěry cestujících za současného zajištění proporcionálních opatření, která budou zahrnovat nezbytné pojistky pro ochranu dat a soukromí.

Ačkoli starost o ochranu dat a soukromí je nadmíru důležité téma, kterým se musí zabývat jakékoli globální řešení, nabízí se zde také příležitost vzít v úvahu další aspekty právní, technické, finanční a ekonomické povahy na straně dopravců a cestujících.

Celosvětové standardy mohou cestujícím i dopravcům zajistit spravedlivost, shodnost, právní jistotu a ochranná opatření. Je jasné, že dopravci, orgány pro prosazování práva, mezinárodní organizace, uskupení v rámci občanské společnosti a odborníci na ochranu dat a soukromí, se všichni musejí zapojit, aby se dospělo ke globálnímu řešení. Pro dosažení pokroku v tomto smyslu je nezbytné, aby komisaři pro ochranu dat a soukromí převzali vedoucí úlohu.

Rezoluce o mezinárodní spolupráci

Navrhovatel: Kanadský komisař pro ochranu soukromí

Přispěvatelé: Komisař pro ochranu informací, Velká Británie
Komisař pro ochranu soukromí, Nový Zéland
Komisař pro ochranu informací a soukromí, Alberta
Komisař pro ochranu informací a soukromí, Saskatchewan

Připomínajíce deklaraci z Montreux vyzývající Spojené národy k vypracování právně závazného nástroje k ochraně soukromí a potvrzujíce připravenost komisařů ochrany dat podporovat vzájemnou spolupráci i spolupráci s dalšími institucemi, které se věnují ochraně dat a soukromí;

vyjadřujíce uznání četným mezinárodním organizacím, které aktivně podporují spolupráci v ochraně soukromí, a mezi něž patří i tato konference, Rada Evropy, Organizace pro hospodářskou spolupráci a rozvoj (OECD), Rada pro ekonomickou spolupráci Asie a Tichomoří (APEC), fórum úřadů pro ochranu soukromí v tichomořské Asii (APPA), Iberoamerická síť pro ochranu dat, Asociace frankofonních úřadů pro ochranu dat a Pracovní skupina podle článku 29 v Evropské Unii;

oceňujíce úsilí vynaložené po 28. konferenci na seminářích v Paříži a Bruselu v rámci londýnské iniciativy za účelem sdílení praktických informací s cílem učinit ochranu dat efektivnější cestou lepší komunikace a aplikace;

konstatujíce, že globální toky osobních informací, jejichž množství a složitost narůstá, nastolují nové výzvy ve vztahu k ochraně osobních údajů; a

poznávajíce, že stále se zvyšující počet zemí uznává význam ochrany dat a rychle postupuje k zajištění ochrany osobních informací způsobem, který odpovídá jejich právní, politické a kulturní realitě;

Komisaři pro ochranu dat a soukromí, shromáždění na 29. mezinárodní konferenci, z těchto důvodů:

1. Respektují, že jednotlivé země přijaly různé přístupy k ochraně osobních informací a posilování práva na soukromí;
2. Vyzývají komisaře ochrany dat, aby dále zvyšovali úsilí při podpoře mezinárodní spolupráce a aby spolupracovali s mezinárodními organizacemi při posilování ochrany dat po celém světě;
3. Vítají, že Rada OECD v červnu 2007 přijala Doporučení k přeshraniční spolupráci při prosazování zákonů na ochranu soukromí a vyzývají vlády v členských zemích OECD, aby toto doporučení uplatňovaly;
4. Vyzývají komisaře, aby pokračovali v hodnotné práci v rámci londýnské iniciativy a podporovali sdílení prostředků, rámcových podmínek a zkušeností při vyhodnocování účinnosti a hospodárnosti našich aktivit a zásahů na vnitrostátní i mezinárodní úrovni; a
5. Doporučují komisařům, aby pokračovali v úsilí zaměřeném na zvyšování povědomí o ochraně dat a soukromí prostřednictvím takových iniciativ, jako je Týden povědomí o ochraně soukromí pořádaný fórem APPA nebo Den ochrany dat vyhlášený Radou Evropy.

Rezoluce o rozvoji mezinárodních standardů

Navrhovatel: Kanadský komisař pro ochranu soukromí

Přispěvatelé: Spolkový komisař pro ochranu dat, Německo
Komise pro ochranu soukromí, Belgie
Komisař pro ochranu dat a svobodu informací, Berlín
Komisař pro informace a ochranu soukromí, Ontario
Agentura pro ochranu dat, Španělsko
Federální komisař pro ochranu dat, Švýcarsko

Usnesení

Rozvoj standardů v oblasti ochrany soukromí uplatnitelných pro využívání a zavádění nových a stávajících technologií je už několik let předmětem rozsáhlých debat a diskuzí jak mezi institucemi pro mezinárodní standardy tak ochránci dat a soukromí. Standardy byly také předmětem konkrétních rozhovorů na minulých mezinárodních konferencích, včetně 25., 26. a 28. mezinárodní konference, které se konaly postupně v Sydney (Austrálie), Wroclawi (Polsko) a Londýně (Velká Británie).

Tyto diskuze svědčí o stále rostoucím poznání ochránců dat a soukromí, že legislativa v oblasti ochrany dat a soukromí, byť pro ochranu osobních informací nezbytná, sama o sobě nepostačuje. Rovněž mezinárodní standardy hrají svou roli jako mechanizmus pomáhající zúčastněným stranám ustavit a demonstrovat shodu s právními požadavky, které se týkají ochrany dat a soukromí.

Vývoj norem v oblasti ochrany soukromí uplatnitelných pro využívání a zavádění nových a stávajících technologií by neměl být vnímán jako proces, který narušuje základní funkci příslušných národních komisí pro ochranu dat a soukromí. Jedním ze způsobů, jak aplikovat technické a organizační specifikace jsou standardy, které dokážou převést legislativní požadavky do konkrétních postupů. Doposud se stávalo, že legislativa byla v souvislosti s technologickými standardy vykládána z velké části bez aktivního zapojení ochránců dat a soukromí. Tato situace se musí změnit, aby se zajistilo dosažení jednotného pojetí a shody.

Mezinárodní organizace pro normy (ISO) dala najevo záměr dále pracovat na přípravě standardů souvisejících s ochranou soukromí tím, že vytvořila Pracovní skupinu 5 (Řízení identity a technologie pro ochranu soukromí) v rámci Podvýboru 27 (Bezpečnost informačních technologií). Tato pracovní skupina vyzvala k navázání kontaktů s Mezinárodní konferencí komisařů pro ochranu dat a soukromí (dále jen „Konference"), přičemž zejména vyzdvihla „vzájemné zájmy obou organizací v oblasti ochrany dat a soukromí, stejně jako cíl Pracovní skupiny uvést do souladu se souborem mezinárodních norem jisté aspekty řízení identity, biometrie a ochrany soukromí v kontextu informačních technologií".

I když rozvoj standardů v oblasti ochrany soukromí[1)] pod hlavičkou bezpečnostně orientované skupiny není ideálním řešením, je to, alepoň v dané chvíli, struktura schválená ISO. Základním krokem k tomu, aby se zajistilo, že vyvíjené normy budou respektovat ochranu soukromí, je odpovědět na tento přístup tvůrců norem aktivnějším zapojením do procesu přípravy standardů. Jde současně o přirozené rozšíření pracovního záběru, které už Konference uskutečňuje v podobě konzultací s obhájci práva na soukromí z jiných jurisdikcí na mezinárodní úrovni – například s Organizací pro hospodářskou spolupráci a rozvoj a skupinou pro ekonomickou spolupráci Asie a Tichomoří – s cílem dotknout se otázek ochrany soukromí, které vyvstávají v souvislosti s přeshraničními toky dat. Jednoduše řečeno, je v nejlepším zájmu Konference i normotvorných institucí, aby členové Konference vynakládali více vzájemné pomoci a spolupráce při rozvoji norem.

Konference proto přijímá následující usnesení:

1. Konference si přeje podporovat rozvoj efektivních a všestranně uznávaných mezinárodních standardů pro ochranu soukromí a poskytne ISO svoje znalosti a zkušenosti pro rozvoj takových norem;
2. Konference vyzývá své členy, aby se prostřednictvím příslušných národních standardizačních organizací aktivněji zúčastnili normotvorného procesu ISO;
3. Vzhledem k možné omezenosti zdrojů u mnohých členů, vyzývá je Konference, aby zvážili, jak nejlépe sdílet znalosti a zkušenosti za účelem jejich poskytnutí ISO;
4. Konference vyzývá své členy, aby přemýšleli o možném mechanizmu jak jménem Konference udržovat vztahy s ISO; a
5. Konference vyzývá své členy, aby aktivněji podporovali účast dalších zainteresovaných skupin (z akademických kruhů, nevládních organizací a výzkumných středisek) na vytváření standardů ISO a aby jim doporučili zapojit se prostřednictvím příslušných národních standardizačních institucí.

Poznámka: Rezoluce jsou k dispozici na internetových stránkách Úřadu www.uoou.cz v rubrice Zahraničí/Mezinárodní aktivity Úřadu a také na webových stránkách organizátora konference www.privacyconference2007.gc.ca .

[1)] Mezi standardy, které nová pracovní skupina ISO právě připravuje, patří ISO 29101 – Referenční architektura ochrany soukromí (nejlepší postupy pro důsledné technické zavádění principů ochrany soukromí); ISO 29100 – Rámec ochrany soukromí (definující z hlediska ochrany soukromí požadavky na zpracování osobních informací v libovolném informačním systému pod jakoukoli jurisdikcí); a ISO 24760 – Rámec pro řízení identity (rámec pro bezpečné, spolehlivé a soukromí respektující řízení informací o totožnosti).

Pracovní skupina pro ochranu údajů zřízená podle článku 29

01646/07/CS
WP 138

Stanovisko 5/2007 k další dohodě mezi Evropskou unií a Spojenými státy americkými o zpracování údajů jmenné evidence cestujících (PNR) a jejich předávání leteckými dopravci Ministerstvu vnitřní bezpečnosti Spojených států uzavřené v červenci 2007

Přijaté dne 17. srpna 2007

Tato pracovní skupina byla zřízena na základě článku 29 směrnice 95/46/ES. Je nezávislým evropským poradním subjektem pro ochranu údajů a soukromí. Její úkoly jsou popsány v článku 30 směrnice 95/46/ES a článku 15 směrnice 2002/58/ES.

Sekretariát poskytuje ředitelství C (Občanská spravedlnost, práva a státní občanství) Evropské komise, Generálního ředitelství pro spravedlnost, svobodu a bezpečnost, B-1049 Brussels, Belgie, kancelář č. LX-46 01/43.

Internetová stránka: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

Shrnutí

Cílem tohoto stanoviska je analyzovat dopad nové, třetí dohody o předávání údajů jmenné evidence cestujících (PNR) americkému ministerstvu vnitřní bezpečnosti na práva a svobody, zejména na právo cestujících na soukromí.

Dosažení nové, dlouhodobé dohody poskytuje právní základ pro předávání údajů o cestujících. Pracovní skupina vždy podporovala boj proti mezinárodnímu terorismu a mezinárodnímu organizovanému zločinu a považuje ho za nezbytný a oprávněný. Jakékoli omezení základních práv a svobod fyzických osob, včetně práva na soukromí a ochranu údajů, však musí být řádně odůvodněno a musí se nalézt správná rovnováha mezi požadavky na ochranu veřejné bezpečnosti a mezi dalšími veřejnými zájmy, například právy fyzických osob na soukromí. Pracovní skupina není přesvědčena, že se v této dohodě podařilo správné rovnováhy dosáhnout.

Témata, která se v nové dohodě týkají ochrany údajů, lze v tomto stanovisku shrnout pomocí dvou následujících zjištění:

1. Obecně lze konstatovat, že opatření na ochranu údajů obsažená v předchozí dohodě byla výrazně oslabena.

2. Nová dohoda ponechává otevřené vážné otázky a nedostatky a obsahuje příliš mnoho mimořádných výjimek.

K bodu 1:

a Počet předávaných prvků údajů se zvýšil a zahrnuje informace o třetích stranách, které nejsou subjektem údajů.
b I v systému uvolňování údajů bude citlivé údaje vyřazovat ministerstvo vnitřní bezpečnosti.
c Ministerstvo vnitřní bezpečnosti nyní může v mimořádných případech používat citlivé údaje, což bylo v předchozí dohodě vyloučeno.
d Další předávání údajů domácím a zahraničním agenturám je jednodušší a už nepodléhá stejným opatřením na zajištění ochrany údajů.
e Doba uchovávání údajů byla rozšířena na nejméně patnáct let a mohla by být dokonce delší.
f Mechanismus pro společný přezkum nepočítá se zapojením nezávislých orgánů na ochranu údajů.

K bodu 2:

a Opatření na zajištění ochrany údajů obsažená v této dohodě a v dopise ministerstva vnitřní bezpečnosti nejsou formulována přesně a ponechávají prostor pro příliš velký počet výjimek, o jejichž využití rozhodují výlučně orgány Spojených států.
b Účely, za nimiž lze údaje předávat, včetně obecných výjimek pro tyto účely, nejsou dostatečně vymezeny a jsou širší než účely uznávané v normách na ochranu údajů.
c Převod ze systému vyhledávání na systém uvolňování údajů je nakonec plánován na 1. ledna 2008, ale není jasné, zda a za jakých podmínek bude tento nový způsob předávání skutečně vypracován.

d Zůstává nejasné, jak bude ministerstvo vnitřní bezpečnosti, které má v mimořádných případech právo získat jiné než vyjmenované údaje, tyto údaje vyhledávat po přechodu ze systému vyhledávání na systém uvolňování údajů.
e Zůstává nejasné, kdy a za jakých okolností se uskuteční společný přezkum.
f Dohoda nestanoví žádný mechanismus řešení sporů a ponechává řešení sporů na smluvních stranách. Platí to zvláště pro společný přezkum.
g Není jasné, jaký režim se vztahuje na údaje, které třetí agentury předaly dalším oddělením.
.
h Není jasné, jaké účinky mají ustanovení o reciprocitě na úroveň ochrany údajů v režimu PNR v EU.
i Dohoda obsahuje riziko, že by určité změny v právních předpisech USA mohly
jednostranně ovlivnit úroveň ochrany údajů stanovenou v nové dohodě o PNR
.

Pracovní skupina je zklamána, že nebyla využita příležitost přijmout vyváženější přístup založený na skutečných potřebách. Vzhledem k tomu, že dohoda vyvolala řadu připomínek, pracovní skupina by uvítala jiný výsledek jednání mezi EU a USA a domnívá se, že v nové dohodě nebyla nalezena správná rovnováha, která by chránila základní práva občanů v oblasti ochrany údajů.

Vzhledem k tomu, že dohoda obsahuje řadu nejasných prvků, požádá pracovní skupina Komisi o písemné objasnění následujících bodů:

- Oblast působnosti dohody: na které letecké společnosti se vztahuje?
- Okolnosti, za nichž lze údaje využívat k účelům, které nejsou uvedeny v bodech 1, 2 a 3 článku I dopisu ministerstva vnitřní bezpečnosti.
- Jak bude fungovat výjimečné vyhledávání údajů, včetně toho, jak se budou kontrolovat tyto výjimečné pravomoci v jurisdikci EU.
- Ujištění, že lhůta, která je nyní stanovena na 1. ledna 2008, nebude znovu odložena, například kvůli jednání o požadavcích.
- Třináct leteckých společností, které podle článku VIII dopisu ministerstva vnitřní bezpečnosti již údaje uvolňují, a jakým požadavkům podléhají.
- Kdy a jak bude připraven a proveden přezkum.
- Článek 5 nové dohody a článek IX dopisu ministerstva vnitřní bezpečnosti (o vzájemnosti), který obsahuje nejednoznačné prohlášení o očekávání ze strany USA.

Pracovní skupina rovněž lituje, že nebyla konzultována ani požádána o poradenství ohledně prvků dohody, které se týkají ochrany údajů, a to tím spíše, že je oficiálním poradním orgánem EU v oblasti ochrany údajů a že pro činnosti ve třetím pilíři neexistuje ekvivalentní rámec nebo skupina. Lituje této skutečnosti tím více, že se pracovní skupina skládá z orgánů, které dohlížejí na plnění požadavků na ochranu údajů leteckými dopravci, kteří budou muset dohodu provádět v úzké spolupráci právě s orgány EU na ochranu údajů.

Pracovní skupina by ráda pokračovala ve své konstruktivní spolupráci s Radou Evropské Unie a s Evropskou komisí, zejména v oblasti provádění nové dohody. Pracovní skupina zejména očekává, že bude zapojena do přípravy a konkrétního provádění přezkumu. Rovněž očekává, že bude zapojena do veškerých jednání o vymezení citlivých údajů a do navazujících činností.

STANOVISKO 5/2007 PRACOVNÍ SKUPINY PRO OCHRANU FYZICKÝCH OSOB V SOUVISLOSTI SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ

k dohodě mezi Evropskou unií a Spojenými státy americkými o zpracování údajů jmenné evidence cestujících (PNR) leteckými dopravci a o jejich předávání Ministerstvu vnitřní bezpečnosti Spojených států uzavřené v červenci 2007

I Úvod

Nová dohoda

V červenci 2007[1] Evropská unie uzavřela se Spojenými státy americkými další dohodu o předávání údajů jmenné evidence cestujících (PNR) a o jejich zpracování Ministerstvem vnitřní bezpečnosti Spojených států (DHS), která nahrazuje předchozí prozatímní dohodu o PNR ze dne 19. října 2006, jež pozbyla účinnosti dne 31. července 2007.

Dokud dohoda nevstoupí v členských státech EU v platnost, bude prozatímně uplatňována ode dne svého podpisu a její platnost skončí v den vzájemně uzavřené nahrazující dohody a v každém případě ne později než sedm let po podpisu dohody.

Cílem dohody je poskytnout právní jistotu leteckým dopravcům provozujícím lety do a ze Spojených států amerických, cestujícím a orgánům členských států EU působícím v oblasti ochrany údajů tím, že nahradí prozatímní dohodu mezi EU a USA z října 2006. Prozatímní dohody bylo dosaženo po rozsudku Evropského soudního dvora ze dne 30. května 2006, který zrušil rozhodnutí Rady 2004/496/ES ze dne 17. května 2004 (o schválení Evropským společenstvím dohody o zpracování a předávání údajů jmenné evidence cestujících (PNR) leteckými dopravci Úřadu pro cla a ochranu hranic Spojených států) a rozhodnutí Komise 2004/535/ES ze dne 14. května 2004 (tzv. rozhodnutí o odpovídající úrovni ochrany) z důvodu nesprávného právního základu.

Nové ujednání se skládá z:

– dohody podepsané oběma stranami
– dopisu (dopis DHS), v němž Ministerstvo vnitřní bezpečnosti USA poskytuje záruky ohledně způsobu, jímž hodlá chránit údaje PNR
– dopisu, v němž EU potvrzuje přijetí záruk a to, že na základě záruk považuje úroveň ochrany údajů v USA za dostatečnou.

Souvislosti

Pracovní skupina uvítala, že bylo dosaženo nové, dlouhodobé dohody, která poskytuje právní základ pro předávání údajů o cestujících. Rovněž oceňuje úsilí vyjednavačů EU, jimž se i přes zdráhavý přístup na straně USA podařilo dohodu vyjednat, a vyhnout se tak právnímu vakuu.

[1] Dohodu podepsala EU dne 23. července a USA 26. července 2007, je k dispozici na internetové stránce: http://www.dhs.gov/xnews/releases/pr_1185470531857.shtm Dohoda byla rovněž zveřejněna v Úředním věstníku dne 4. srpna (OJ L 204, 4.8.2007, s.18) http://eur-lex.europa.eu/JOHtml.do?uri=OJ:L:2007:204:SOM:EN:HTML

Pracovní skupina se domnívá, že je její povinností vyjádřit své stanovisko k záležitostem týkajícím se soukromí souvisejícím s předáváním osobních údajů orgánům USA, protože cestující, politici i orgány pověřené ochranou údajů musí znát současnou úroveň ochrany údajů zajištěnou v nové dohodě. Kromě toho údaje PNR nejprve shromažďují a poté předávají letečtí dopravci, nad nimiž vykonávají dohled vnitrostátní orgány pro ochranu údajů.

Pracovní skupina vždy podporovala boj proti mezinárodnímu terorismu a mezinárodnímu organizovanému zločinu. Domnívá se, že tento boj je nezbytný a oprávněný. Uznává, že osobní údaje mohou sloužit jako cenný nástroj, ale zastává názor, že získávání a zpracovávání osobních údajů nemůže samo o sobě stačit k potlačení tohoto jevu a že by se k tomuto účelu i ke zvýšení bezpečnosti a efektivnosti letecké dopravy měly využívat rovněž všechny ostatní dostupné prostředky.

Každý rok přeletí Atlantský oceán miliony cestujících a očekává se, že v důsledku uzavření dohod o otevřeném nebi tento počet rychle poroste. Letečtí dopravci získávají a využívají osobní údaje cestujících pro své vlastní podnikatelské účely a je třeba opět zdůraznit, že v boji proti terorismu a souvisejícím zločinům musí být zajištěno dodržování základních práv a svobod fyzických osob, včetně práva na soukromí a ochranu osobních údajů, a že dodržování těchto práv a svobod nelze zpochybnit.

Jakékoli jejich omezení musí být řádně odůvodněno a musí při něm být dosaženo správné rovnováhy mezi požadavky na ochranu veřejné bezpečnosti a dalšími veřejnými zájmy, například právem fyzických osob na soukromí. Veškerý neodůvodněný a nepřiměřený obecný dohled ze strany třetí země by nebyl slučitelný s lidskou důstojností a s právem na soukromí.

V této souvislosti je nutné posoudit novou, dlouhodobou dohodu podle základních zásad ochrany údajů, například podle zásady přiměřenosti, zásady minimalizace údajů, odpovědnosti správce údajů a práva subjektů údajů na informace a nápravu, aby bylo možné řádně vyhodnotit úroveň ochrany údajů, kterou dohoda poskytuje.

Vyhodnocení provedené pracovní skupinou zřízenou podle článku 29

Cílem tohoto stanoviska pracovní skupiny, jejímiž členy jsou nezávislí evropští komisaři pro ochranu údajů, je pečlivě analyzovat úroveň ochrany údajů v nové, dlouhodobé dohodě srovnáním jejích ustanovení s ustanoveními předchozí dohody ve světle uznávaných norem ochrany údajů, například norem uvedených ve směrnici 95/46/ES[2] a v úmluvě Rady Evropy č. 108[3], a stanovisek, která k tomuto tématu pracovní skupina již v minulosti přijala. Stanovisko by mělo rovněž vyhodnotit, jaké dopady bude mít dohoda na soukromí osob cestujících z a do Spojených států.

Na rozdíl od předchozích ujednání nová dohoda o PNR neodkazuje na tzv. závazky, které Úřad pro cla a ochranu hranic poskytl v květnu 2004, čímž ukončuje jejich platnost. Přestože tyto závazky byly podle právní definice jednostranným závazkem USA, byly ve skutečnosti výsledkem zdlouhavých a komplikovaných jednání zaměřených

[2] Směrnice 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.

[3] Úmluva o ochraně osob s ohledem na automatizované zpracování osobních údajů přijatá ve Štrasburku dne 28. ledna 1981.

na zajištění dostatečné úrovně ochrany při využívání údajů PNR a Evropská komise z nich vycházela v tzv. rozhodnutí o dostatečné úrovni ochrany č. 2005/535/ES. Pracovní skupina přijala během těchto jednání i po jejich skončení řadu stanovisek k úrovni ochrany údajů[4].
Nová dohoda a zejména dopis ministerstva vnitřní bezpečnosti poskytují tzv. záruky, které mají zajistit ochranu údajů při využívání osobních údajů cestujících z EU. Tyto záruky tedy nahrazují závazky.

Toto stanovisko proto rovněž důkladně porovná záruky obsažené v dopise ministerstva vnitřní bezpečnosti se zárukami z roku 2004 a vyvodí závěry o úrovni ochrany soukromí, kterou poskytují.

II Nová dohoda o PNR

Rozsah a právní povaha

V nové dohodě se uvádí, že se použije na letecké dopravce, kteří provozují lety z a do USA. Není jasné, zda jsou zahrnuti např. letečtí dopravci, kteří provozují lety ze třetí země s tranzitem přes EU. Není jasné, kde jsou limity jurisdikce EU. Jedná se o proces zpracování nebo o správce údajů, který sídlí v EU? Dohoda tyto otázky neřeší a pracovní skupina očekává, že Evropská komise tyto body písemně vysvětlí.

Podle článku 1 jsou dohoda i dopis ministerstva vnitřní bezpečnosti závazné pro obě strany. Jak dohoda, tak dopis budou zveřejněny v Úředním věstníku EU (řadě L). Není však jasné, zda bude dopis ministerstva vnitřní bezpečnosti zveřejněn ve Federálním rejstříku Spojených států. V případě neplnění dohody ze strany USA může EU dohodu ukončit podle článku 8. Dohoda a dopis se nepoužijí přímo na soukromé subjekty, například letecké dopravce nebo občany. Tato dohoda se použije v členských státech s výhradou ustanovení vnitrostátního práva.

2 Omezení účelu

Nová, dlouhodobá dohoda o PNR se skládá z řady bodů odůvodnění a 9 článků a upravuje předávání údajů PNR leteckými dopravci Ministerstvu vnitřní bezpečnosti USA. Účely předávání jsou stanoveny v bodech odůvodnění: předcházení terorismu a nadnárodnímu zločinu a boj s nimi. Dopis ministerstva vnitřní bezpečnosti dále vysvětluje, že se jedná o: předcházení a boj proti 1) terorismu a související trestné činnosti; 2) dalším vážným trestným činům nadnárodní povahy, včetně organizovaného zločinu; a 3) vyhýbání se soudním příkazům nebo vazbě za výše uvedené trestné činy.

Účely uvedené v nové dohodě se shodují s účely uvedenými v předchozí prozatímní dohodě. Význam pojmu trestná činnost související s terorismem a pojmu vážné trestné činy nadnárodní povahy, včetně organizovaného zločinu, není definován, čímž je ponechán volný prostor pro jeho výklad.

Pracovní skupina se stále domnívá, že toto omezení účelu je příliš široké a dala by přednost jasnějšímu vymezení trestných činů souvisejících s terorismem a vážných trestných činů.

[4] Pracovní skupina 78 ze dne 13. června 2003, pracovní skupina 87 ze dne 29. ledna 2004, P 95 ze dne 22. června 2004.

Podle dopisu ministerstva vnitřní bezpečnosti lze využívat údaje i v dalších případech, zejména pokud je to nutné pro ochranu životně důležitých zájmů subjektu údajů nebo jiných osob, což je v souladu s dřívějšími závazky. Údaje PNR lze využívat rovněž v rámci případného trestního řízení, což naznačuje, že je lze využívat i v případě drobné trestné činnosti nebo trestných činů nesouvisejících s terorismem nebo vážnými trestnými činy nadnárodní povahy. Kromě toho je lze využívat i v jiných případech stanovených zákony USA. Toto využití údajů PNR bylo zmíněno již v závazcích z roku 2004. Bylo tomu tak však pouze v souvislosti s předáváním údajů dalším subjektům. V nové dohodě se na toto využití klade větší důraz a považuje se za jeden z účelů, spíše než za dopad dalšího předávání údajů.

Pracovní skupina je touto změnou omezení účelu znepokojena tím spíše, že již omezení v minulé dohodě považovala za široké. Pracovní skupina očekává, že jí Komise předloží písemné vysvětlení, v němž upřesní, za jakých okolností lze údaje využívat k jiným účelům, než je uvedeno výše v bodech 1, 2 a 3.

3 Příjemci údajů o cestujících

Zatímco body odůvodnění předchozí dohody obsahovaly seznam určitého počtu oddělení ministerstva vnitřní bezpečnosti, která byla oprávněna k přijímání údajů PNR, a seznam oddělení, která k tomu oprávněna nebyla (např. Úřady USA pro občanství a imigraci nebo tajné služby USA), nová dohoda žádná taková ustanovení neobsahuje. Uvádí se v ní pouze, že ministerstvo vnitřní bezpečnosti zachází s údaji PNR pocházejícími z EU jako s údaji, které jsou podle práva USA citlivé a důvěrné. Oddělení ministerstva vnitřní bezpečnosti, která předtím nebyla jasně zařazena nebo která dokonce neměla právo přímo získávat PNR, se již nepovažují za „třetí agentury“ a již nepodléhají podmínkám, jimiž se řídí předávání údajů PNR dalším subjektům.

Pracovní skupina lituje, že se výrazně zvýšil počet potenciálních příjemců údajů, a domnívá se, že pro účely dohledu nad tokem údajů by bývalo důležité omezit počet oddělení oprávněných k využívání údajů PNR. Má za to, že současná situace představuje značné oslabení bezpečnostních opatření obsažených v předchozí dohodě.

4 Další předávání údajů

Další předávání údajů PNR „třetím agenturám“ uvnitř ministerstva vnitřní bezpečnosti, dalším orgánům USA a orgánům zahraničních vlád bylo upraveno výhradně závazky, zatímco předchozí prozatímní dohoda zachovávala úpravu první dohody o PNR z roku 2004.

Závazky stanovily, že údaje PNR pocházející z EU lze předat dalším vládním orgánům, včetně orgánů třetích zemí, pouze na individuálním základě pro účely předcházení a boje proti terorismu a souvisejícím trestným činům, jiným vážným trestným činům nadnárodní povahy, včetně organizovaného zločinu, a při pokusech vyhnout se zatčení nebo vzetí do vazby z důvodů zde uvedených trestných činů. Vedoucí Úřadu na ochranu soukromí ministerstva vnitřní bezpečnosti mohl vyšetřovat a ohlašovat porušení podmínek pro předávání údajů a mohl přijímajícímu orgánu odebrat oprávnění k dalším převodům údajů PNR od Úřadu pro cla a ochranu hranic.

Přestože podle článku II dopisu ministerstva vnitřní bezpečnosti platí pro šíření údajů PNR určitá omezení, skutečnost, že se klade větší důraz na obecnější účely, které opravňují ke sdílení údajů PNR, může znamenat, že údaje PNR budou s větší pravděpodobností dostávat a zpracovávat také vládní orgány, které se zabývají trestnou

činností, která nesouvisí s bojem proti terorismu a souvisejícími trestnými činy. Totéž platí v situacích, kdy jsou údaje PNR potřebné v dalších případech stanovených právem USA. Nikde již není uvedeno zvláštní omezení, podle něhož by se údaje měly předávat pouze na individuálním základě, vyvstává tedy otázka, zda by v budoucnosti nemohlo docházet k hromadnému předávání údajů.

Další šíření údajů PNR „třetími agenturami" dalším agenturám bylo v předchozí dohodě upraveno tak, že se ministerstvo pro vnitřní bezpečnost pokládalo za majitele údajů a veškeré další šíření údajů bylo možné pouze s výslovným předchozím souhlasem Úřadu pro cla a ochranu hranic, který kontroloval tok údajů. Vzhledem k tomu, že toto užitečné omezení bylo zrušeno, vznikají pochybnosti o kvalitě údajů a o době jejich uchovávaní poté, co třetí agentura předá osobní údaj dalším příjemcům. Přestalo být jasné, kdo nese odpovědnost za zpracování a další šíření těchto údajů.

Bezpečnostní opatření na ochranu údajů obsažená v nové dohodě jsou mnohem méně přísná, protože na jedné straně rozšiřují seznam agentur, kterým je možno tyto údaje poskytovat, a na druhé straně usnadňují předávání údajů dalším agenturám.

Rovněž se přestala uplatňovat dřívější bezpečností opatření uvedená v závazcích, podle nichž se při předávání údajů PNR orgánům třetích zemí muselo postupovat na individuálním základě. Na předání osobních údajů mají nárok třetí země, jejichž úroveň ochrany údajů se považuje za srovnatelnou s úrovní ochrany na ministerstvu vnitřní bezpečnosti. V této souvislosti je rovněž nutné položit otázku, jak se bude kontrolovat další předávání údajů poté, co je bude mít k dispozici třetí země.

5 Prvky údajů

Seznam prvků údajů, který byl uveden v příloze A závazku USA z května 2004, byl v nové dohodě přepracován a je nyní uveden v článku III dopisu ministerstva vnitřní bezpečnosti.

Předchozí ujednání obsahovalo seznam 34 jednotlivých prvků, které se předávají, pokud jsou obsaženy v rezervačních systémech leteckých dopravců. V nové dohodě je vyjmenováno 19 druhů souborů informací PNR, což vyvolává dojem, že došlo k významnému snížení předávaných údajů. Nový seznam skutečně neobsahuje prvek údajů „informace o případech, kdy se cestující dostavil na letiště bez rezervace a byl připraven k odletu", který se podle minulé dohody vyžadoval, ale uvádí všech ostatních 33 prvků údajů, které byly uvedeny na předchozím seznamu, i když v poněkud odlišné podobě.

Nový seznam navíc obsahuje prvky údajů, které předchozí seznam nezahrnoval, čímž rozšiřuje rozsah informací požadovaných ministerstvem vnitřní bezpečnosti. Je tomu tak u řady údajů:

a) prvek 5 (dostupné informace o často cestující osobě a výhodách): zatímco podle předchozí dohody se informace o pravidelných cestujících týkaly pouze počtu nalétaných kilometrů a adresy, podle nové dohody je nutné poskytovat rovněž údaje o čísle, které bylo pravidelnému cestujícímu přiděleno, nebo o jeho nárocích na bezplatné letenky. Předchozí dohoda nevyžadovala žádné informace o takových výhodách.

b) prvek 7 (veškeré dostupné kontaktní informace): přestože tento prvek sdružuje prvky, které byly vyžadovány i dříve: adresu (6), fakturovací adresu (8), kontaktní telefonní čísla (9) a e-mailovou adresu (17), není vyloučeno, že budou poskytnuty rovněž další informace, například e-mailová adresa zaměstnavatele.

c) údaj 15 (veškeré informace o zavazadlech): zatímco předchozí dohoda vyžadovala pouze informace o číslech zavazadlových visaček, nyní je nutné poskytovat další informace o zavazadlech cestujícího, například o jejich počtu nebo velikosti (zavazadla ve velkém), což opět ve srovnání s předchozí dohodou rozšiřuje rozsah podávaných informací.

Zatímco pracovní skupina aktivně prosazovala snížení prvků údajů, které se považují za nezbytné pro boj proti terorismu a souvisejícím trestným činům[5], nová dohoda rozšiřuje seznam prvků údajů tím, že vyžaduje více informací o subjektech údajů. Toto rozšíření nelze v žádném případě odůvodnit a je třeba ho považovat za nepřiměřené.

Osobní údaje třetích osob

Je třeba rovněž uvést, že podle minulé dohody mohlo ministerstvo vnitřní bezpečnosti požádat o informace, které se netýkaly subjektu údajů, ale třetích stran, např. v případě fakturovací adresy, e-mailové adresy, cestovní kanceláře, od koho byla získána informace atd. Nová dohoda nejenže vyžaduje více údajů o cestujících, ale také o třetích stranách, například když požaduje informace o poskytovaných výhodách, které jsou obsaženy v rezervačním systému leteckého dopravce.

Pracovní skupina je tímto vývojem znepokojena, protože je velice pravděpodobné, že třetí strana vůbec neví o předání osobních údajů ministerstvu vnitřní bezpečnosti a neví, jaká má v takovém případě práva na ochranu osobních údajů. Z tohoto důvodů nemůže třetí strana využít práva, která dohoda poskytuje subjektům údajů.

Další údaje

Dále je třeba konstatovat, že podle čl. III oddílu 3 dopisu ministerstva vnitřní bezpečnosti může toto ministerstvo ve výjimečných případech použít další prvky údajů, které sice nejsou uvedeny na seznamu, ale jsou obsaženy v rezervačních systémech leteckých dopravců, což významně rozšiřuje rozsah prvků údajů. Pracovní skupina trvá na svém názoru, že v rámci třetího pilíře[6] existují jiné právní cesty, které v takových výjimečných případech umožňují přístup k osobním informacím, aniž by se narušovalo soukromí cestujících. Pracovní skupina je rovněž znepokojena slovy, že ministerstvo vnitřní bezpečnosti informuje Evropskou komisi o využití takových údajů „zpravidla do 48 hodin“. To znamená, že ministerstvo vnitřní bezpečnosti může samo rozhodnout, kdy a zda bude o této záležitosti informovat.

Nebylo stanoveno, jakým způsobem bude ministerstvo vnitřní bezpečnosti získávat takové dodatečné prvky údajů obsažené v rezervačních systémech leteckých společností poté, co se systém předávání údajů změní ze systému vyhledávání údajů (tzv. pull system) na systém uvolňování údajů (tzv. push system). Přesný způsob není novou

[5] Pracovní skupina 78 „Stanovisko 4/2003 o úrovni ochrany zajištěné v USA při předávání údajů o cestujících“ přijaté dne 13. června 2003.

[6] Dohoda o vydávání mezi EU a USA a Dohoda o vzájemné právní pomoci mezi EU a USA, obě podepsány dne 25. června 2003.

dohodou o PNR upraven a zdá se, že i v případě aktivního systému uvolňování údajů bude za výjimečných okolností využit systém vyhledávání údajů. Pracovní skupina proto od Evropské komise očekává písemné vyjádření, v němž bude vysvětleno, jak bude fungovat výjimečné vyhledávání údajů, včetně toho, jak se budou kontrolovat tyto výjimečné pravomoci v jurisdikci EU.

6 Analytické informace

V článku IX dopisu ministerstva vnitřní bezpečnosti se uvádí, že ministerstvo bude podporovat předávání analytických informací vyplývajících z údajů PNR příslušnými orgány USA policejním a soudním orgánům členských států, případně Europolu a Eurojustu.
Není jasné, co budou takové analytické informace obsahovat a zda budou zahrnovat osobní údaje[7].

Článek IX rovněž pojednává o očekávání DHS, že EU a její členské státy budou povzbuzovat své kompetentní orgány k recipročnímu jednání a poskytování analytických informací plynoucích z údajů PNR ministerstvu vnitřní bezpečnosti a dalším orgánům USA. Na takové předávání údajů do Spojených států se však nová dohoda nevztahuje, protože se týká pouze předávání údajů PNR obsažených v rezervačních systémech leteckých dopravců.

Analytické informace nejsou součástí seznamu uvedeného v článku III dopisu ministerstva vnitřní bezpečnosti, který je vyčerpávajícím seznamem všech prvků údajů, které lze předávat. V závislosti na povaze analytických informací by jejich přímá výměna s dalšími agenturami USA značně rozšířila rozsah seznamu prvků údajů a vedla by k tomu, že by tento seznam již nebyl považován za vyčerpávající. Výměna takových informací by měla být upravena jinými právními nástroji, ale v současné době se na ni dohoda nevztahuje. Z tohoto důvodu je pracovní skupina přesvědčena, že toto očekávání uvedené v dopise ministerstva vnitřní bezpečnosti nemá žádný právní základ, a zpochybňuje jeho právní hodnotu.

7 Způsob předávání údajů PNR

Stejně jako v předchozí dohodě je i v této dohodě stanoveno, že se v pozdější fázi přejde na předávání údajů PNR systémem uvolňování, ovšem pouze v případě těch leteckých dopravců, kteří splní technické požadavky ministerstva vnitřní bezpečnosti. V ostatních případech budou údaje PNR i nadále vyhledávat samy orgány USA.

Evropští letečtí dopravci v minulosti výrazně investovali do systému uvolňování údajů a potvrzují, že takový systém je v současné době technicky proveditelný. Přepravci jednali ve snaze splnit původní termín stanovený v závazcích z roku 2004 na prosinec 2006. V této fázi je třeba znovu zdůraznit, že z hlediska ochrany údajů je systém uvolňování jediným přijatelným způsobem předávání osobních údajů a že jakékoli další odklady navozují otázku, zda ministerstvo vnitřní bezpečnosti skutečně hodlá změnit současný postup. Pracovní skupina s odkazem na svá dříve zveřejněná stanoviska s velkým politováním konstatuje, že se zavedení systému uvolňování odkládá již od podpisu první dohody o PNR v květnu 2004. Pracovní skupina očekává ujištění Evropské komise, že lhůta, která je nyní stanovena na 1. ledna 2008, nebude znovu odložena, například kvůli jednání o požadavcích. Očekává od Komise rovněž vysvětlení o tom, kterých třináct

[7] Pracovní skupina 136 „Stanovisko 4/2007 k pojmu osobní údaje“ přijaté dne 20. června 2007

leteckých společností již uvolňuje údaje, jak je uvedeno v článku VIII dopisu ministerstva vnitřní bezpečnosti, a jaké požadavky se na ně vztahují.

Pracovní skupina je znepokojena zjištěním, že přechod na funkční systém uvolňování závisí pouze na uvážení ministerstva vnitřní bezpečnosti a že nová dohoda neobsahuje ustanovení o vzájemně dohodnutém způsobu rychlého zavedení systému uvolňování údajů ani mechanismus pro řešení zbývajících problémů. Vzhledem k tomu, že technické požadavky na přenos údajů PNR se přímo týkají leteckých dopravců, měli by být dopravci zapojeni do jednání a obě smluvní strany by měly řešit jimi vznesené otázky. Skutečnost, že se jedné straně umožní jednostranně rozhodovat o tom, jaké technické požadavky jsou nezbytné pro změnu ze systému vyhledávání údajů na systém uvolňování, ohrožuje konečný přechod na systém uvolňování.

Pokud jde o počet „uvolnění“, průvodní dopis pouze uvádí, že se aktualizované údaje budou předávat podle potřeby, ale neuvádí, jak často mají letečtí dopravci předávat údaje po prvním uvolnění údajů, které provedou 72 hodin před odletem. Pracovní skupina se domnívá, že toto rozhodnutí by nemělo být ponecháno na volném uvážení ministerstva vnitřní bezpečnosti, protože aktualizace musejí být přiměřené a musejí brát v úvahu dopady na soukromí cestujících a finanční náklady leteckých dopravců. Mělo by být nalezeno vzájemně přijatelné řešení, které je vhodnější než jednostranné rozhodování.
Kromě toho ani dohoda, ani dopis ministerstva vnitřní bezpečnosti neobsahují žádné ustanovení, podle něhož by se o uvolnění nemohlo žádat dříve než 72 hodin před odletem.

8 Vytřídění citlivých údajů

S otázkou jak předávat údaje PNR úzce souvisí téma třídění údajů o cestujících (článek III dopisu ministerstva vnitřní bezpečnosti).

Jednou z hlavních zásad ochrany údajů je to, že odpovědnost za zpracování osobních údajů nese správce údajů, jak je uvedeno ve směrnici 95/46/ES (čl. 2 písm. d) ve spojení s čl. 6 odst. 2), kde je stanoveno, že osoba nebo instituce, která určuje účel a prostředky zpracování údajů se považuje za jejich správce, a je za ně tudíž odpovědná. Podobná ustanovení lze nalézt v čl. 2 písm. d) a v článku 5 úmluvy 108. Údaje o cestujících shromažďují a zpracovávají pro vlastní podnikatelské účely letecké společnosti. Proto by právě tyto společnosti měly zajišťovat, aby se ministerstvu vnitřní bezpečnosti předávaly pouze ty údaje, které jsou vyjmenovány v dohodě a v dopise ministerstva vnitřní bezpečnosti. Seznam předávaných údajů PNR uvedený v článku III dopisu ministerstva vnitřní bezpečnosti neobsahuje žádné citlivé údaje. Citlivé údaje však mohou být zahrnuty do položek vyjmenovaných v bodě 17 „obecné poznámky včetně informací OSI (další služební informace), SSI (zvláštní služební informace) a SSR (zvláštní služební požadavek)“ a v bodě 19 „všechny známé změny záznamů PNR“. Vzhledem k tomu, že citlivé údaje nejsou součástí seznamu předávaných prvků údajů, DHS se zavazuje k jejich vytřídění. Za třídění všech údajů před jejich předáním do systému uvolňování by však měl odpovídat správce, aby nedocházelo k předávání údajů, na něž se dohoda nevztahuje, včetně citlivých údajů.

Podle názoru pracovní skupiny je skutečnost, že nová dohoda zbavuje odpovědnosti subjekty shromažďující údaje a ponechává vytřídění některých údajů na ministerstvu vnitřní bezpečnosti, v rozporu se zásadami ochrany údajů. Platí to zvláště pro citlivé údaje, které budou vyloučeny ze zpracovávání. Podle nové dohody však může ministerstvo vnitřní bezpečnosti dokonce využít citlivé údaje, které má k dispozici, pokud za výjimečných okolností tyto informace potřebuje.

Přestože se ministerstvo vnitřní bezpečnosti zavazuje, že uchová záznam o přístupu k jakýmkoli citlivým údajům a že je vymaže do 30 dnů po splnění účelu, pro který byly uchovávány, není jasné, jakými prostředky se bude kontrolovat využívání a tok údajů, jakmile ministerstvo vnitřní bezpečnosti předá citlivé údaje domácím a zahraničním agenturám a už nebude vlastníkem těchto údajů.

Je rovněž nutné poznamenat, že ministerstvo vnitřní bezpečnosti určí po konzultaci s Evropskou komisí, které údaje se budou považovat za citlivé podle definice v úmluvě 108 nebo ve směrnici. Vzhledem k tomu, že pojem a význam citlivých údajů by se mohly v průběhu času měnit, je nezbytné neustále vymezovat nové relevantní citlivé údaje a pravidelně je přezkoumávat v úzké spolupráci s orgány na ochranu údajů a odvětvím letecké dopravy, aby byl seznam aktuální. Toto téma není v nové dohodě zmíněno. Pracovní skupina očekává, že bude zapojena do veškerých jednání o definování citlivých údajů.

9 Uchovávání údajů

Nová dohoda neobsahuje žádná ustanovení o době uchovávání údajů PNR ministerstvem vnitřní bezpečnosti. Režim uchovávání údajů je však upraven článkem VII dopisu ministerstva vnitřní bezpečnosti, podle něhož se rozlišuje mezi aktivní analytickou databází, v níž se údaje uchovávají 7 let, tedy dvakrát déle než podle předchozí dohody, a mezi údaji v nečinném, nepoužitelném stavu, které se uchovávají dalších 8 let. V závazcích z roku 2004 bylo výslovně stanoveno, že údaje se budou na 8 let převádět do souboru vymazaných záznamů, to se však týkalo pouze velice omezeného objemu údajů, s nimiž se manuálně pracovalo během počátečního období 3,5 let.

Z hlediska ochrany údajů neexistuje žádný rozdíl mezi aktivním a tzv. nečinným obdobím přístupu. Po celou dobu, kdy jsou osobní údaje přístupné, i když v období nečinného stavu ve velice omezených a vzácných případech, jsou dostupné v databázi a ministerstvo vnitřní bezpečnosti k nim má přístup a může je zpracovat. To znamená, že období uchovávání údajů bylo prodlouženo z 3,5 na 15 let.

Dokonce ani toto období nelze považovat za definitivní, protože dopis ministerstva vnitřní bezpečnosti zachází ještě dále a prohlašuje, že ministerstvo očekává, že údaje PNR budou na konci tohoto období vymazány a že se o otázce toho, zda a kdy zničit údaje PNR bude v budoucnosti jednat, což naznačuje, že doba uchovávání by mohla být ještě prodloužena, což je vysoce znepokojující a není to slučitelné s uznávanými normami v oblasti ochrany soukromí, např. s čl. 5 písm. e) úmluvy a čl. 6 písm. e) směrnice.

Pracovní skupina již dospěla k závěru, že s ohledem na účely, kvůli nimž se údaje o cestujících uchovávají, je období 3,5 let nepřiměřeně dlouhé. Nebyly poskytnuty žádné podstatné důkazy o tom, že stávající období je nezbytné (jak vyžaduje článek 8 Evropské úmluvy o lidských právech) nebo že je příliš krátké.

Dopis ministerstva vnitřní bezpečnosti navíc stanoví, že na údaje PNR získané na základě předchozí dohody se nyní vztahuje stejně dlouhé období uchovávání jako na údaje získané na základě nové dohody. To je v rozporu se závazkem Spojených států z května 2004, který stanovil obecné, vzájemně dohodnuté období uchovávání v délce 3,5 roku. Ministerstvo vnitřní bezpečnosti jednostranně prodloužilo dobu uchovávání údajů PNR, které byly získány na základě první dohody o PNR (od 28. května 2004 do října 2006). Veškeré údaje předané ministerstvu vnitřní bezpečnosti ve výše

uvedeném období byly předány s tím, že budou po 3,5 letech zničeny, pokud se v nich manuálně nevyhledávalo. Tato zásada je nyní zrušena dopisem ministerstva vnitřní bezpečnosti a není přijatelné, aby ministerstvo vnitřní bezpečnosti jednostranně a bez přesvědčivých důvodů dobu uchovávání údajů prodloužilo.

10 Společný přezkum

Podle článku 4 nové dohody a článku X dopisu ministerstva vnitřní bezpečnosti budou smluvní strany pravidelně přezkoumávat provádění dohody, dopis ministerstva vnitřní bezpečnosti i politiky a postupy USA a EU v oblasti PNR, aby společně zajistily efektivní fungování svých systémů a ochranu soukromí. Dopis ministerstva mimo jiné zdůrazňuje, že během tohoto přezkumu se bude jednat rovněž o všech případech, kdy byl vyžádán přístup k citlivým údajům. Přezkum bude provádět skupina složená z ministra vnitřní bezpečnosti a komisaře pro spravedlnost, svobodu a bezpečnost nebo vzájemně přijatelného úředníka, kterého může každá smluvní strana navrhnout. EU a ministerstvo vnitřní bezpečnosti společně rozhodnou o podrobném obsahu přezkumu.

V porovnání se závazky byly podstatně oslabeny normy ochrany údajů týkající se nezávislého dohledu.

Za prvé, podle závazků měl společný přezkum probíhat pravidelně každý rok nebo častěji v závislosti na dohodě stran. Z nové dohody není jasné, jak často bude plánovaný přezkum probíhat nebo zda se vůbec uskuteční. Dopis DHS nestanoví pro přezkum konkrétní datum ani neobsahuje žádné zmínky o tom, kdy by měla být zahájena jeho příprava.

Za druhé, dopis ministerstva vnitřní bezpečnosti již neuvádí, že spolu se smluvními stranami se přezkumu musejí účastnit nezávislí zástupci evropských orgánů pro prosazování práva a/nebo orgánů členských států. Nezávislé odborné znalosti a dohled nad ochranou údajů je jedním z hlavních pilířů účinné ochrany soukromí, který zajišťuje, že dojde k řádnému řešení nedostatků a že budou projednávány obavy subjektů údajů.

Vzhledem k tomu, že na základě první dohody o PNR již proběhl jeden úspěšný přezkum, který společně zorganizovaly smluvní strany včetně nezávislých orgánů ochrany údajů, pracovní skupina opětovně zdůrazňuje význam plného zapojení orgánů ochrany údajů do veškerých budoucích přezkumů. Nedostatek nezávislých účastníků potenciálně oslabuje opatření na ochranu údajů o cestujících. Pracovní skupina proto očekává, že bude zapojena do přípravy a konkrétního provádění společného přezkumu. Očekává, že Komise bezodkladně písemně objasní, kdy a jak bude přezkum připraven a proveden.

Další problém vyplývá ze skutečnosti, že k přezkumu dojde pouze tehdy, pokud se obě strany společně dohodnou na jeho podrobném obsahu. Znamená to, že pokud se strany nebudou moci dohodnout nebo pokud bude jedna strana přezkumu bránit, k přezkumu vůbec nedojde a nevyřešené problémy zůstanou bez řádné odpovědi. Nová dohoda neobsahuje mechanismus na řešení takových sporů a ponechává každé straně rozsáhlý prostor pro ovlivňování podrobností přezkumu a jeho utváření podle vlastních záměrů. Pracovní skupina očekává, že Komise objasní i toto téma, a to i vzhledem k tomu, že na základě prozatímní dohody o PNR nebyl uspořádán žádný společný přezkum, protože se smluvní strany nedohodly na jeho podrobném obsahu.

11 Práva subjektů údajů, včetně práva na nápravu

Opatření na ochranu údajů při převodu a zpracování údajů PNR orgány Spojených států nejsou součástí samotné dohody, ale jsou obsaženy v připojeném dopise ministerstva vnitřní bezpečnosti, kde jsou vysvětleny záruky, které chce ministerstvo poskytnout cestujícím.

Přestože se dohoda a dopis ministerstva považují za právně závazné, je dopis v mnoha ohledech vágní, jak bylo v tomto stanovisku vysvětleno, a používání záruk je ponecháno do velké míry na volném uvážení, pokud jde například o přechod ze systému vyhledávání na systém uvolňování údajů a o patnáctileté období uchovávání údajů. Vzniká otázka, jak lze záruky uvedené v dopise ministerstva vnitřní bezpečnosti právně vymáhat, když je tolik detailů ponecháno otevřených. Z tohoto důvodu pracovní skupina zastává názor, že právní ochrana poskytnutá dopisem ministerstva vnitřní bezpečnosti je mnohem slabší než v předchozí dohodě.

Přestože článek V dopisu ministerstva vnitřní bezpečnosti pojednává o opatřeních k prosazování práv, která jsou k dispozici cestujícím, zůstává nejasné, zda bude dopis zveřejněn ve Federálním rejstříku a zda může představovat právní základ pro prosazování práv na ochranu údajů v USA. Pracovní skupina proto vyzývá Evropskou komisi, aby naléhala na zveřejnění dopisu ve Federálním rejstříku.

Na druhou stranu pracovní skupina vítá, že ministerstvo vnitřní bezpečnosti přijalo politické rozhodnutí rozšířit správní ochranu podle zákona o ochraně soukromí na cestující, kteří nejsou občany USA ani nemají v USA uděleno povolení k pobytu. Tyto fyzické osoby, které nejsou občany USA, již nejsou diskriminovány, což je v souladu s univerzálním právem na ochranu údajů. Přestože se jedná o pozitivní krok, je nutné přijmout další opatření, která zajistí, že tato práva bude možné prakticky vykonávat, a právě zde existuje prostor pro vnitrostátní orgány ochrany údajů.

Pracovní skupina rovněž vítá, že se USA spolu s EU budou zasazovat o zviditelnění upozornění, jimiž jsou cestující informováni o systémech PNR, a o to, aby letečtí dopravci zařadili tato upozornění do svých oficiálních přepravních smluv. Toto ustanovení nové dohody jistě zvýší transparentnost tím, že poskytne cestujícím přes Atlantský oceán informace o jejich právech a mechanismech nápravy.

Pracovní skupina zastupující vnitrostátní orgány ochrany údajů hrála prvořadou roli při formulování a propagaci upozornění pro cestující, která letecké společnosti v současné době používají, a očekává, že bude v této důležité činnosti v budoucnu pokračovat.

12 Dopad dohody na režim PNR v EU

Článek 5 nové dohody a článek IX dopisu ministerstva vnitřní bezpečnosti (o vzájemnosti) obsahuje nejednoznačné prohlášení o očekávání USA ohledně opatření na ochranu údajů, která se použijí jak na režim PNR v USA, tak na jakýkoli budoucí režim PNR v EU. Zatímco se předpokládá, že toto ustanovení znamená, že Spojené státy neočekávají, že by se budoucí režim PNR v EU řídil méně náročnými normami než režim zavedený novou dohodou, mohlo by se toto ustanovení vykládat rovněž tak, že ministerstvo vnitřní bezpečnosti požaduje, aby EU ve svém režimu PNR nezavedla vyšší normy ochrany údajů, jinak pozastaví platnost dohody. Takový vývoj by byl velice znepokojivý a mohl by ovlivnit úsilí EU o zaručení vysoké úrovně ochrany v údajů v jakémkoli budoucím režimu PNR v EU. Je naprosto nutné, aby Evropská komise písemně vysvětlila přesnou podstatu tohoto bodu.

Rovněž je třeba poznamenat, že článek o vzájemnosti je nevyvážený, protože Spojené státy mají pouze povinnost „aktivně podpořit“ plnění požadavků leteckými společnostmi USA, zatímco Evropská unie musí toto plnění zajistit.

III Závěr

Pracovní skupina vítá, že byla se Spojenými státy uzavřena nová, dlouhodobá dohoda o PNR, která upravuje předávání údajů PNR ministerstvu vnitřní bezpečnosti. Pracovní skupina se domnívá, že existence takové dohody má naprosto zásadní význam proto, aby nevznikla právní nejistota pro členské státy, cestující využívající leteckou dopravu i letecké dopravce.

Pracovní skupina oceňuje, že ministerstvo vnitřní bezpečnosti zvýší transparentnost zpracování údajů tím, že bude propagovat využívání informačních oznámení pro cestující. Pracovní skupina připomíná, že v minulosti projednávala toto téma s vedoucím Úřadu na ochranu soukromí ministerstva vnitřní bezpečnosti a poté přijala dvě stanoviska[8], aby poskytla pokyny leteckým dopravcům a zvýšila povědomí veřejnosti. Pracovní skupina rovněž vítá skutečnost, že politické rozhodnutí ministerstva vnitřní bezpečnosti rozšiřuje ochranu soukromí na fyzické osoby, které nejsou občany USA a předchozí dohoda o PNR se na ně nevztahovala.

Lituje však, že tato drobná zlepšení jsou výrazně převážena celkovým snížením úrovně ochrany údajů. Záruky poskytnuté v dopise ministerstva vnitřní bezpečnosti jsou mnohem slabší než záruky, které byly obsaženy v závazcích. Lituje rovněž, že EU zaujala názor, že opatření na ochranu údajů stanovená dohodnou jsou vyhovující, aniž by konzultovala jakýkoli orgán zřízený za účelem ochrany údajů, přestože dohodu budou muset členské státy provádět v úzké spolupráci s vnitrostátními orgány dohledu.

Pracovní skupina se domnívá, že účely, kvůli nimž lze předávat údaje o cestujících, jsou příliš obecné, a lituje, že tyto účely jsou rozsáhlejší než ty, které jsou uznány v normách na ochranu údajů, a že širší výjimky z těchto účelů nejsou dostatečně upřesněny. Pracovní skupina je znepokojena skutečností, že byl zřejmě výrazně rozšířen počet agentur ministerstva vnitřní bezpečnosti oprávněných k přijímání údajů a že neexistuje jasný seznam všech subjektů ministerstva vnitřní bezpečnosti s právem na přístup k údajům PNR.

Pokud jde o metodu předávání údajů PNR, pracovní skupina s velkým znepokojením konstatuje, že provádění systému uvolňování údajů se odkládá již od podpisu první dohody o PNR v květnu 2004, a domnívá se, že další odklady již nejsou možné. Pracovní skupina nesouhlasí s ustanovením nové dohody, podle něhož lze přejít ze systému vyhledávání údajů na systém uvolňování údajů pouze na základě rozhodnutí ministerstva vnitřní bezpečnosti, aniž by se bral ohled na legitimní práva dotčených leteckých dopravců. To platí i pro počet uvolňování údajů, o němž rozhoduje ministerstvo vnitřní bezpečnosti. Vzájemně přijatelným a ekonomicky životaschopným způsobem musí být

[8] Pracovní skupina 97 „Stanovisko 8/2004 o informování cestujících o předávání údajů PNR při letech mezi Evropskou unií a Spojenými státy americkými“ přijaté dne 30. září 2004
a pracovní skupina 132 „Stanovisko 2/2007 o informování cestujících o předávání údajů PNR orgánům USA“ přijaté dne 15. února 2007 a „Krátké upozornění týkající se cest mezi Evropskou unií a Spojenými státy“.

nalezeno řešení, které chrání soukromí a které není pro nikoho, zejména pro letecké společnosti EU, diskriminující.

Výrazné prodloužení období uchovávání údajů a rozšíření seznamu prvků údajů výrazně oslabilo ochranná opatření uvedená v předchozích závazcích. Skutečnost, že ministerstvo vnitřní bezpečnosti bude i nadále vyřazovat citlivé údaje a že tyto citlivé údaje může ve výjimečných případech použít, není v souladu s uznávanými normami na ochranu údajů, například úmluvou 108 a směrnicí.

Pracovní skupina zdůrazňuje nezbytnost plného zapojení orgánů ochrany údajů do veškerých nezávislých přezkumů, a to jak při jejich přípravě, tak při jejich provádění. Je třeba, aby Evropská komise vyjasnila, kdy a jak bude přezkum připraven a proveden.

Pro předávání analytických informací neexistuje žádný právní základ a právní hodnota očekávání ministerstva vnitřní bezpečnosti v tomto ohledu je zpochybnitelná.

Na závěr lze konstatovat, že pracovní skupina nepřehlíží skutečnost, že nová dohoda o PNR obsahuje určitá drobná zlepšení oproti předchozí dohodě, ale je jednoznačně zklamána nedostatečnou úrovní ochrany údajů v nové dohodě o PNR. Nová dohoda dokonce ani nezachovává úroveň ochrany z předchozí dohody, kterou pracovní skupina ve svých předchozích stanoviscích považovala za slabou.

Z analýzy obsažené v tomto stanovisku vyplývá, že nová dohoda o PNR neplní uznávané normy na ochranu údajů, které jsou stanoveny například v úmluvě 108 a ve směrnici. Vyvolá pochopitelné znepokojení u všech cestujících přes Atlantský oceán, kteří mají obavy o své právo na soukromí.

V Bruselu dne 17. srpna 2007

Za pracovní skupinu
předseda
Peter SCHAAR

III. Materiály z Úředního věstníku Evropské unie

Příloha Věstníku Úřadu pro ochranu osobních údajů (s. 2781 – 2801)

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (ES) č. 1987/2006

ze dne 20. prosince 2006

o zřízení, provozu a využívání Schengenského informačního systému druhé generace (SIS II)

EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o založení Evropského společenství, a zejména na čl. 62 odst. 2 písm. a), čl. 63 odst. 3 písm. b) a článek 66 této smlouvy,

s ohledem na návrh Komise,

v souladu s postupem stanoveným v článku 251 Smlouvy ([1]),

vzhledem k těmto důvodům:

(1) Schengenský informační systém (dále jen „SIS“) zřízený v souladu s ustanoveními hlavy IV Úmluvy ze dne 19. června 1990 k provedení Schengenské dohody ze dne 14. června 1985 mezi vládami států Hospodářské unie Beneluxu, Spolkové republiky Německo a Francouzské republiky o postupném odstraňování kontrol na společných hranicích ([2]) (dále jen „Schengenská úmluva“) a jeho rozšířená verze SIS 1+ představují nezbytný nástroj pro uplatňování ustanovení schengenského *acquis* začleněného do rámce Evropské unie.

(2) Vývoj SIS druhé generace (dále jen „SIS II“) byl svěřen Komisi na základě nařízení Rady (ES) č. 2424/2001 ([3]) a rozhodnutí Rady 2001/886/SVV ([4]) ze dne 6. prosince 2001 o vývoji Schengenského informačního systému druhé generace (SIS II). SIS II nahradí SIS vytvořený na základě Schengenské úmluvy.

(3) Toto nařízení představuje nezbytný právní základ pro řízení SIS II s ohledem na záležitosti spadající do oblasti působnosti Smlouvy o založení Evropského společenství (dále jen „Smlouva“). Rozhodnutí Rady 2006/…/SVV ze dne… o zřízení, provozu a využívání Schengenského informačního systému druhé generace (SIS II) ([5]) představuje nezbytný právní základ pro řízení SIS II s ohledem na záležitosti spadající do oblasti působnosti Smlouvy o Evropské unii.

(4) Skutečnost, že legislativní základ nezbytný pro řízení SIS II sestává ze samostatných nástrojů, nemá dopad na zásadu, že SIS II představuje jediný informační systém, který by měl jako takový fungovat. Proto by určitá ustanovení těchto nástrojů měla být totožná.

(5) SIS II by měl představovat vyrovnávací opatření přispívající k udržení vysokého stupně bezpečnosti v rámci prostoru svobody, bezpečnosti a práva Evropské unie prostřednictvím podpory provádění politik souvisejících se součástí schengenského *acquis* týkající se pohybu osob, jak jsou začleněny do hlavy IV Smlouvy.

(6) Je nezbytné konkrétně vymezit účely SIS II, jeho technickou architekturu a financování a stanovit pravidla týkající se jeho provozu, využívání a odpovědností, kategorií údajů vkládaných do systému, účelů jejich vkládání, kritérií jejich vkládání, orgánů oprávněných k přístupu do systému, propojení záznamů, jakož i další pravidla týkající se zpracování údajů a ochrany osobních údajů.

(7) SIS II by měl zahrnovat centrální systém (dále jen „centrální SIS II“) a vnitrostátní aplikace. Výdaje spojené s provozem centrálního SIS II a komunikační infrastruktury by měly být financovány ze souhrnného rozpočtu Evropské unie.

(8) Je nutné vytvořit příručku obsahující podrobná pravidla pro výměnu určitých doplňujících informací týkajících se opatření, která záznam vyžaduje. Výměnu těchto informací by měly zajišťovat vnitrostátní orgány jednotlivých členských států.

(9) Během přechodného období by za provozní řízení centrálního SIS II a části komunikační infrastruktury měla odpovídat Komise. V zájmu zajištění hladkého přechodu na SIS II však může přenést některé nebo všechny odpovědnosti na dva vnitrostátní veřejnoprávní subjekty. Z dlouhodobého hlediska a v návaznosti na posouzení dopadu, které bude obsahovat věcnou analýzu alternativ z hlediska finančního, provozního a organizačního, a na legislativní návrhy Komise by měl být stanoven řídící orgán odpovědný za tyto úkoly. Přechodné období by mělo trvat nejdéle pět let ode dne použitelnosti tohoto nařízení.

([1]) Stanovisko Evropského parlamentu ze dne 25. října 2006 (dosud nezveřejněné v Úředním věstníku) a rozhodnutí Rady ze dne 19. prosince 2006 (dosud nezveřejněné v Úředním věstníku).

([2]) Úř. věst. L 239, 22.9.2000, s. 19. Úmluva naposledy pozměněná nařízením (ES) č. 1160/2005 (Úř. věst. L 191, 22.7.2005, s. 18).

([3]) Úř. věst. L 328, 13.12.2001, s. 4.

([4]) Úř. věst. L 328, 13.12.2001, s. 1.

([5]) Úř. věst. L …

(10) SIS II by měl obsahovat záznamy pro účely odepření vstupu nebo pobytu. Je nezbytné dále zvážit harmonizaci ustanovení o důvodech pro pořizování záznamů týkajících se občanů třetích zemí pro účely odepření vstupu nebo pobytu a vyjasnit jejich používání v rámci azylové, přistěhovalecké a návratové politiky. Proto by Komise měla tři roky ode dne použitelnosti tohoto nařízení přezkoumat ustanovení o cílech a podmínkách pořizování záznamů pro účely odepření vstupu nebo pobytu.

(11) Záznamy za účelem odepření vstupu nebo pobytu by v SIS II měly být uchovávány nanejvýš po dobu potřebnou pro splnění účelů, pro které byly tyto záznamy pořízeny. Obecnou zásadou je, že by měly být ze SIS II automaticky vymazány po uplynutí tří let. Rozhodnutí o uchování záznamu po delší dobu by mělo vycházet z komplexního individuálního posouzení. Členské státy by měly během tohoto tříletého období tyto záznamy přezkoumat a vést statistiku o počtu záznamů, u nichž byla doba uchovávání prodloužena.

(12) SIS II by měl umožnit zpracování biometrických údajů s cílem napomoci spolehlivému určení totožnosti dotyčných osob. Ve stejném smyslu by měl SIS II umožňovat rovněž zpracování údajů o osobách, jejichž totožnost byla zneužita, za účelem předcházení nepříjemnostem způsobeným chybným určením totožnosti, s výhradou odpovídajících záruk, zejména souhlasu dotyčné osoby a přísného omezení účelů, pro něž se tyto údaje mohou zákonným způsobem zpracovávat.

(13) Členským státům by mělo být umožněno zavést odkazy mezi záznamy v SIS II. Vytvoření odkazů mezi dvěma nebo více záznamy členským státem by nemělo mít dopad na přijímaná opatření, na délku doby uchovávání nebo práva přístupu k záznamům.

(14) Údaje zpracovávané v SIS II za použití tohoto nařízení by neměly být poskytovány ani zpřístupňovány žádným třetím zemím nebo mezinárodním organizacím.

(15) Na zpracování osobních údajů za použití tohoto nařízení se vztahuje směrnice 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]. To zahrnuje určení správce a možnost členských států stanovit výjimky z některých udělených práv a povinností stanovených v této směrnici nebo jejich omezení, včetně práv na přístup k údajům a sdělování informací dotyčné osobě. Pokud je to nezbytné, měly by se zásady uvedené ve směrnici 95/46/ES doplnit nebo objasnit v tomto nařízení.

(16) Nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů [2], a zejména ta jeho ustanovení, které se týkají důvěrné povahy a bezpečnosti zpracovávání, se vztahuje na zpracovávání osobních údajů orgány nebo institucemi Společenství při plnění jejich úkolů jakožto orgánů odpovědných za provozní řízení SIS II v rámci výkonu činností, z nichž všechny nebo část spadá do oblasti působnosti práva Společenství. Část zpracování osobních údajů v SIS II spadá do oblasti působnosti práva Společenství. V zájmu soudržného a stejnorodého uplatňování pravidel ochrany základních práv a svobod fyzických osob v souvislosti se zpracováním osobních údajů je třeba vysvětlit, že pokud Komise zpracovává osobní údaje za použití tohoto nařízení, vztahuje se na ni nařízení (ES) č. 45/2001. Pokud je to nezbytné, měly by se zásady uvedené v nařízení (ES) č. 45/2001 doplnit nebo objasnit v tomto nařízení.

(17) Pokud jde o důvěrnost, měla by se na úředníky nebo ostatní zaměstnance Evropských společenství zaměstnané a pracující v souvislosti se SIS II vztahovat příslušná ustanovení služebního řádu úředníků Evropských společenství a pracovní řád ostatních zaměstnanců Evropských společenství.

(18) Je vhodné, aby zákonnost zpracovávání osobních údajů členskými státy sledovaly vnitrostátní orgány dozoru, zatímco Evropský inspektor ochrany údajů, jmenovaný podle rozhodnutí Evropského parlamentu a Rady 2004/55/ES ze dne 22. prosince 2003 o jmenování nezávislého kontrolního orgánu podle článku 286 Smlouvy o ES [3], by měl sledovat činnosti orgánů a institucí Společenství související se zpracováváním osobních údajů s ohledem na omezené úkoly orgánů a institucí Společenství ve vztahu k samotným údajům.

(19) Členské státy i Komise by měly vypracovat bezpečnostní plán s cílem usnadnit provádění bezpečnostních povinností a měly by vzájemně spolupracovat s cílem společně řešit bezpečnostní otázky.

(20) Za účelem zajištění transparentnosti by měla Komise, nebo řídící orgán, je-li zřízen, každé dva roky vypracovat zprávu o technickém fungování centrálního SIS II a komunikační infrastruktury, včetně jejího zabezpečení, a o výměně doplňujících informací. Každé čtyři roky by měla Komise vydat celkové vyhodnocení.

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

[2] Úř. věst. L 8, 12.1.2001, s.1.

[3] Úř. věst. L 12, 17.1.2004. s. 47.

(21) Ustanoveními tohoto nařízení nelze vyčerpávajícím způsobem upravit některé aspekty SIS II, jako jsou technická pravidla pro vkládání údajů, včetně údajů potřebných pro vložení záznamu, aktualizace, výmaz a vyhledávání, pravidla týkající se slučitelnosti a priority záznamů, odkazy mezi záznamy a výměna doplňujících informací v důsledku jejich technické podstaty, úrovně podrobností a potřeby pravidelné aktualizace. S přihlédnutím k hladkému fungování vnitrostátních systémů je proto třeba svěřit Komisi prováděcí pravomoci, pokud jde o tyto aspekty. Technická pravidla o vyhledávání v záznamech by měla zohlednit hladké fungování vnitrostátních aplikací. Na základě posouzení dopadu předloženého Komisí by mělo být rozhodnuto, v jakém rozsahu může být řídící orgán, jakmile bude zřízen, odpovědný za prováděcí opatření.

(22) Opatření nezbytná k provedení tohoto nařízení by měla být přijata podle rozhodnutí Rady 1999/468/ES ze dne 28. června 1999 o postupech pro výkon prováděcích pravomocí svěřených Komisi [1].

(23) Je vhodné stanovit přechodná ustanovení, pokud jde o záznamy pořízené v SIS 1+, které budou přeneseny do SIS II. Některá ustanovení schengenského *acquis* by měla dále platit po omezené období, dokud členské státy nepřezkoumají slučitelnost těchto záznamů s novým právním rámcem. Přednostně je třeba přezkoumat slučitelnost záznamů o osobách. Navíc by jakákoliv změna, doplnění, oprava nebo aktualizace záznamu přeneseného ze SIS 1+ do SIS II, a jakýkoliv pozitivní nález takového záznamu, měla podnítit okamžité posouzení jeho souladu s ustanoveními tohoto nařízení.

(24) Je nezbytné stanovit zvláštní ustanovení, pokud jde o zbývající část rozpočtu vyčleněného na provoz SIS, která není součástí souhrnného rozpočtu Evropské unie.

(25) Jelikož cílů navrhované akce, zejména vytvoření a řízení společného informačního systému, nemůže být uspokojivě dosaženo na úrovni členských států, a proto jich může být z důvodu rozsahu a účinků akce lépe dosaženo na úrovni Společenství, může Společenství přijmout opatření v souladu se zásadou subsidiarity stanovenou v článku 5 Smlouvy. V souladu se zásadou proporcionality stanovenou v uvedeném článku toto nařízení nepřekračuje rámec toho, co je nezbytné k dosažení těchto cílů.

(26) Toto nařízení ctí základní práva a zachovává zásady uznávané zejména v Listině základních práv Evropské unie.

(27) V souladu s články 1 a 2 Protokolu o postavení Dánska připojeného ke Smlouvě o Evropské unii a ke Smlouvě o založení Evropského společenství se Dánsko neúčastní přijímání tohoto nařízení, a proto pro ně není závazné ani použitelné. Vzhledem k tomu, že toto nařízení navazuje na schengenské *acquis* podle hlavy IV části třetí Smlouvy, mělo by se Dánsko rozhodnout v souladu s článkem 5 uvedeného protokolu do šesti měsíců ode dne přijetí tohoto nařízení, zda je provede ve svém vnitrostátním právu.

(28) Toto nařízení rozvíjí ta ustanovení schengenského *acquis*, kterých se neúčastní Spojené království v souladu s rozhodnutím Rady 2000/365/ES ze dne 29. května 2000 o žádosti Spojeného království Velké Británie a Severního Irska, aby se na ně vztahovala některá ustanovení schengenského *acquis* [2]. Spojené království se tudíž nepodílí na jeho přijímání, a proto pro ně není závazné ani použitelné.

(29) Toto nařízení rozvíjí ta ustanovení schengenského *acquis*, kterých se neúčastní Irsko v souladu s rozhodnutím Rady 2002/192/ES ze dne 28. února 2002 o žádosti Irska, aby se na ně vztahovala některá ustanovení schengenského *acquis* [3]. Irsko se tudíž nepodílí na jeho přijímání, a proto pro ně není závazné ani použitelné.

(30) Toto nařízení se nedotýká opatření pro částečnou účast Spojeného království a Irska na schengenském *acquis*, jak jsou vymezena pro Spojené království v rozhodnutí 2000/365/ES a pro Irsko v rozhodnutí 2002/192/ES.

(31) Pokud jde o Island a Norsko, rozvíjí toto nařízení ta ustanovení schengenského *acquis* ve smyslu Dohody uzavřené mezi Radou Evropské unie a Islandskou republikou a Norským královstvím o přidružení těchto dvou států k provádění, uplatňování a rozvoji schengenského *acquis* [4], která spadají do oblasti uvedené v čl. 1 bodě G rozhodnutí Rady 1999/437/ES ze dne 17. května 1999 [5] o některých opatřeních pro uplatňování uvedené dohody.

[1] Úř. věst. L 184, 17.7.1999, s. 23. Rozhodnutí ve znění rozhodnutí 2006/512/ES (Úř. věst. L 200, 22.7.2006, s. 11).

[2] Úř. věst. L 131, 1.6.2000, s. 43.

[3] Úř. věst. L 64, 7.3.2002, s. 20.

[4] Úř. věst. L 176, 10.7.1999, s. 36.

[5] Úř. věst. L 176, 10.7.1999, s. 31.

(32) Je třeba přijmout opatření umožňující zástupcům Islandu a Norska zapojení do práce výborů, jež jsou nápomocny Komisi při výkonu jejích prováděcích pravomocí. Takové opatření je uvedeno ve výměně dopisů mezi Radou evropské unie a Islandskou republikou a Norským královstvím o výborech, které jsou nápomocny Evropské komisi při výkonu její výkonné moci [1], připojené k výše uvedené dohodě.

(33) Pokud jde o Švýcarsko, rozvíjí toto nařízení ta ustanovení schengenského *acquis* ve smyslu dohody podepsané mezi Evropskou unií, Evropským společenstvím a Švýcarskou konfederací o přidružení Švýcarské konfederace k provádění, uplatňování a rozvoji schengenského *acquis*, která spadají do oblasti uvedené v čl. 1 bodě G rozhodnutí 1999/437/ES ve spojení s čl. 4 odst. 1 rozhodnutí 2004/849/ES [2] a rozhodnutí 2004/860/ES [3],

(34) Je třeba přijmout opatření umožňující zástupcům Švýcarska zapojení do práce výborů, jež jsou nápomocny Komisi při výkonu jejích prováděcích pravomocí. Takové opatření je uvedeno ve výměně dopisů mezi Společenstvím a Švýcarskem, připojené k uvedené dohodě.

(35) Toto nařízení představuje akt navazující na schengenské *acquis* nebo s ním jinak související ve smyslu čl. 3 odst. 2 aktu o přistoupení z roku 2003.

(36) Toto nařízení by se mělo vztahovat na Spojené království a Irsko ve lhůtách určených v souladu s postupy stanovenými v příslušných nástrojích týkajících se použití schengenského *acquis* na tyto státy,

PŘIJALY TOTO NAŘÍZENÍ:

KAPITOLA I

OBECNÁ USTANOVENÍ

Článek 1

Zřízení a obecný účel SIS II

1. Zřizuje se Schengenský informační systém druhé generace (dále jen „SIS II“).

2. Účelem SIS II je zajistit v souladu s tímto nařízením na územích členských států vysokou úroveň bezpečnosti v rámci prostoru svobody, bezpečnosti a práva Evropské unie, včetně udržování veřejné bezpečnosti a veřejného pořádku a zajišťování bezpečnosti a národní bezpečnosti, a uplatňovat ustanovení Hlavy IV části třetí Smlouvy o ES, pokud jde o pohyb osob na jejich územích, s využitím informací předávaných prostřednictvím tohoto systému.

Článek 2

Oblast působnosti

1. Toto nařízení zavádí podmínky a postupy pro vkládání a zpracovávání záznamů v SIS II o státních příslušnících třetích zemí a pro výměnu doplňujících informací a dalších údajů za účelem odepření vstupu nebo pobytu na území členských států.

2. Toto nařízení též stanoví pravidla zejména o technické architektuře SIS II, o povinnostech členských států a řídícího orgánu uvedeného v článku 15, o obecném zpracování údajů, o právech dotčených osob a o zákonné odpovědnosti.

Článek 3

Definice

Pro účely tohoto nařízení se rozumí:

a) „záznamem“ soubor údajů vložených do SIS II umožňující příslušným orgánům identifikovat osobu s ohledem na konkrétní opatření, které má být přijato;

b) „doplňujícími informacemi“ informace, které nejsou uložené v SIS II, ale souvisejí se záznamy SIS II a které se vyměňují:

   i) s cílem umožnit členským státům vzájemné poskytování konzultací či informací při vkládání záznamu;

[1] Úř. věst. L 176, 10.7.1999, s. 53.

[2] Rozhodnutí Rady 2004/849/ES ze dne 25. října 2004 o podpisu dohody mezi Evropskou unií, Evropským společenstvím a Švýcarskou konfederací o přidružení Švýcarské konfederace k provádění, uplatňování a rozvoji schengenského *acquis* jménem Evropské unie a o prozatímním provádění některých jejích ustanovení (Úř. věst. L 368, 15.12.2004, s. 26).

[3] Rozhodnutí Rady 2004/860/ES ze dne 25. října 2004 o podpisu dohody mezi Evropskou unií, Evropským společenstvím a Švýcarskou konfederací o přidružení Švýcarské konfederace k provádění, uplatňování a rozvoji schengenského *acquis* jménem Evropského společenství a o prozatímním provádění některých jejích ustanovení (Úř. věst. L 370, 17.12.2004, s. 78).

ii) po pozitivním nálezu, aby se umožnilo přijetí vhodného opatření;

iii) pokud nelze požadované opatření přijmout;

iv) pokud se jedná o kvalitu údajů v SIS II;

v) pokud se jedná o slučitelnost a prioritu záznamů;

vi) pokud se jedná o práva přístupu;

c) „dalšími údaji“ údaje uložené v SIS II a související se záznamy SIS II, které jsou okamžitě k dispozici příslušným orgánům, pokud jsou na základě vyhledávání v tomto systému nalezeny osoby, jejichž údaje byly vloženy do SIS II;

d) „státním příslušníkem třetí země“ každá fyzická osoba, která není

i) ani občanem Evropské unie ve smyslu čl. 17 odst. 1 Smlouvy o ES;

ani

ii) státním příslušníkem třetí země, jejíž státní příslušníci na základě dohod mezi Společenstvím a jeho členskými státy na jedné straně a těmito zeměmi na straně druhé požívají práva volného pohybu rovnocenného právu občanů Evropské unie;

e) „osobními údaji“ veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjektu údajů“); identifikovatelnou osobou se rozumí osoba, kterou lze přímo nebo nepřímo identifikovat;

f) „zpracováním osobních údajů“ (dále jen „zpracování“) jakýkoli úkon nebo soubor úkonů, které jsou prováděny s osobními údaji pomocí automatizovaných postupů nebo bez nich, jako je shromažďování, zaznamenávání, uspořádávání, uchovávání, přizpůsobování nebo pozměňování, vyhledávání, nahlížení, používání, sdělování prostřednictvím přenosu, šíření nebo jakékoli jiné zpřístupnění, srovnávání či kombinování, jakož i blokování, výmaz nebo znehodnocení.

Článek 4

Technická architektura provozování SIS II

1. Schengenský informační systém druhé generace (SIS II) sestává z:

a) centrálního systému (dále jen „centrální SIS II“) sestávajícího z:

— technické podpůrné funkce (dále jen „CS-SIS“) obsahující databázi, dále jen „databáze SIS II“;

— jednotného vnitrostátního rozhraní (dále jen „NI-SIS“);

b) vnitrostátního systému (dále jen „N. SIS II“) v každém členském státě, sestávajícího z vnitrostátních datových systémů, které komunikují s centrálním SIS II. Vnitrostátní systém N. SIS II může obsahovat soubor údajů (dále jen „vnitrostátní kopie“) obsahující úplnou nebo částečnou kopii databáze SIS II;

c) komunikační infrastruktury mezi CS-SIS a NI-SIS (dále jen „komunikační infrastruktura“), která poskytuje šifrovanou virtuální síť vyhrazenou pro údaje SIS II a výměnu údajů mezi centrálami SIRENE uvedenými v čl. 7 odst.2.

2. Údaje SIS II se vkládají, aktualizují, vymazávají a vyhledávají prostřednictvím různých systémů N. SIS II. Vnitrostátní kopie je k dispozici za účelem automatizovaného vyhledávání na území každého členského státu, jenž takovou kopii používá. Vyhledávání v souborech údajů N. SIS II jiných členských států není umožněno.

3. Technická podpůrná funkce (CS-SIS), jež vykonává technický dohled a správu, se nachází ve Štrasburku (Francie) a záložní CS-SIS, jež je schopna zajistit všechny funkce hlavní CS-SIS v případě její poruchy, se nachází v Sankt Johann im Pongau (Rakousko).

4. Technická podpůrná funkce CS-SIS poskytuje služby nezbytné pro vložení a zpracování údajů SIS II, včetně vyhledávání v databázi SIS II. Členským státům, jež používají vnitrostátní kopii, CS-SIS poskytuje:

a) on-line aktualizaci vnitrostátních kopií;

b) synchronizaci a soulad mezi vnitrostátními kopiemi a databází SIS II;

c) počáteční nastavení a opětovné zavedení vnitrostátních kopií.

Článek 5

Náklady

1. Náklady na zřízení, provoz a údržbu centrálního SIS II a komunikační infrastruktury se hradí ze souhrnného rozpočtu Evropské unie.

2. Tyto náklady zahrnují práci vykonanou v souvislosti s CS-SIS, která zajišťuje poskytování služeb uvedených v čl. 4 odst. 4.

3. Náklady na zřízení, provoz a údržbu jednotlivých N. SIS II nese dotyčný členský stát.

KAPITOLA II

POVINNOSTI ČLENSKÝCH STÁTŮ

Článek 6

Vnitrostátní systémy

Každý členský stát je povinen zřídit, provozovat a udržovat svůj N. SIS II a připojit svůj N. SIS II k NI-SIS.

Článek 7

Úřad N. SIS II a centrála SIRENE

1. Každý členský stát určí orgán (dále jen „úřad N. SIS II"), jenž nese hlavní odpovědnost za jeho N. SIS II. Tento orgán je odpovědný za plynulý provoz a bezpečnost N. SIS II, zajišťuje přístup příslušných orgánů k SIS II a přijímá nezbytná opatření k zajištění dodržování ustanovení tohoto nařízení. Každý členský stát předává své záznamy prostřednictvím svého úřadu N. SIS II.

2. Každý členský stát určí centrálu, která zajistí výměnu veškerých doplňujících informací (dále jen „centrála SIRENE"), v souladu s ustanoveními příručky SIRENE, jak je uvedeno v článku 8.

Tyto centrály také koordinují ověřování kvality informací vkládaných do SIS II. Pro tyto účely mají přístup k údajům zpracovávaným v SIS II.

3. Členské státy uvědomí řídící orgán o svém úřadu N. SIS II a o své centrále SIRENE. Řídící orgán zveřejní jejich seznam spolu se seznamem uvedeným v čl. 31 odst. 8.

Článek 8

Výměna doplňujících informací

1. Doplňující informace se vyměňují v souladu s ustanoveními příručky SIRENE a prostřednictvím komunikační infrastruktury. Pokud by komunikační infrastruktura nebyla dostupná, členské státy mohou k výměně doplňujících informací použít jiné náležitě zabezpečené technické prostředky.

2. Doplňující informace se použijí pouze pro účely, pro které byly předány.

3. Žádosti jiných členských států o doplňující informace musí být vyřízeny co nejdříve.

4. Aniž jsou dotčena ustanovení nástroje, kterým se zřizuje řídící orgán, přijmou se postupem podle čl. 51 odst. 2 podrobná pravidla pro výměnu doplňujících informací v podobě příručky SIRENE.

Článek 9

Technický soulad

1. K zajištění okamžitého a účinného přenosu údajů postupuje každý členský stát při zřizování svého N. SIS II podle protokolů a technických postupů stanovených pro zajištění souladu CS-SIS s N. SIS II. Tyto protokoly a technické postupy se stanoví podle čl. 51 odst. 2, aniž jsou dotčena ustanovení nástroje, kterým se zřizuje řídící orgán.

2. Používá-li členský stát vnitrostátní kopii, zajistí prostřednictvím služeb, které poskytuje CS-SIS, aby údaje uložené ve vnitrostátní kopii byly prostřednictvím automatizované aktualizace uvedené v čl. 4 odst. 4 totožné a shodné s databází SIS II a aby vyhledávání v jeho vnitrostátní kopii poskytovalo rovnocenný výsledek jako vyhledávání v databázi SIS II.

Článek 10

Bezpečnost - členské státy

1. Každý členský stát přijme, ve vztahu ke své N. SIS II, nezbytná opatření, včetně přijetí bezpečnostního plánu, aby:

a) fyzicky chránil údaje mimo jiné vypracováním plánů pro mimořádné situace pro ochranu kritické infrastruktury;

b) zabránil neoprávněným osobám v přístupu k zařízení na zpracování údajů využívanému pro zpracování osobních údajů (kontrola přístupu k zařízení);

c) zabránil neoprávněnému čtení, kopírování, pozměňování či vyjímání nosičů dat (kontrola nosičů dat);

d) zabránil neoprávněnému vkládání údajů a neoprávněnému prohlížení, pozměňování či výmazu uložených osobních údajů (kontrola uchovávání);

e) zabránil neoprávněným osobám v užívání automatizovaných systémů zpracování údajů pomocí zařízení pro přenos údajů (kontrola uživatelů);

f) zajistil, aby osoby oprávněné k využívání automatizovaného systému zpracování údajů měly přístup pouze k údajům, na které se vztahuje jejich oprávnění k přístupu, a pouze s pomocí individuálních a jedinečných totožností uživatele a chráněných režimů přístupu k informacím (kontrola přístupu k údajům);

g) zajistil, aby všechny orgány s oprávněním přístupu do SIS II nebo k zařízením pro zpracování údajů vytvořily profily popisující funkce a povinnosti osob, jež jsou oprávněny k údajům přistupovat a údaje zadávat, aktualizovat, mazat a vyhledávat, a aby tyto profily bezodkladně na základě žádosti zpřístupnily vnitrostátním orgánům dozoru uvedeným v článku 44 odst. 1 (profily pracovníků);

h) zajistil, aby bylo možné ověřit a zjistit, kterým orgánům se mohou osobní údaje předávat prostřednictvím zařízení pro přenos údajů (kontrola předávání);

i) zajistil, aby bylo možné dodatečně ověřit a zjistit, které osobní údaje byly vloženy do automatizovaných systémů zpracování údajů, a kdo, kdy a za jakým účelem je vložil (kontrola vkládání);

j) zabránil neoprávněnému čtení, kopírování, pozměňování nebo výmazu osobních údajů během přenosů osobních údajů nebo přepravy nosičů dat, zejména prostřednictvím vhodných technik šifrování (kontrola přepravy);

k) sledoval účinnost bezpečnostních opatření uvedených v tomto odstavci a přijal nezbytná organizační opatření související s interním sledováním pro zajištění souladu s tímto nařízením (interní kontrola).

2. Členské státy přijmou opatření rovnocenná opatřením uvedeným v odstavci 1, pokud jde o bezpečnost v souvislosti s výměnou doplňujících informací.

Článek 11

Důvěrnost - členské státy

Každý členský stát použije v souladu se svými vnitrostátními právními předpisy svá pravidla služebního tajemství nebo jiné srovnatelné povinnosti zachování důvěrnosti na všechny osoby a subjekty, které musí pracovat s údaji SIS II a s doplňujícími informacemi. Tato povinnost trvá i poté, co dotyčné osoby opustí svůj úřad nebo zaměstnanecký poměr, nebo poté, co dotyčné subjekty ukončí svou činnost.

Článek 12

Vedení evidence na vnitrostátní úrovni

1. Členské státy, které nepoužívají vnitrostátní kopie zajistí, aby každý přístup k osobním údajům a všechny výměny osobních údajů s CS-SIS byly evidovány v N. SIS II za účelem kontroly, zda je vyhledávání zákonné či nikoli, za účelem sledování zákonnosti zpracovávání údajů, pro vlastní kontrolu, pro zajištění řádného fungování N. SIS II, neporušenosti údajů a jejich zabezpečení.

2. Členské státy, které používají vnitrostátní kopie zajistí, aby každý vstup do údajů SIS II a každá výměna těchto údajů byly zaznamenány pro účely uvedené v odstavci 1. To neplatí pro postupy uvedené v čl. 4 odst. 4.

3. Evidence obsahuje zejména historii záznamů, datum a čas předání údajů, údaje použité pro provedení vyhledávání; odkaz na předávané údaje a název jak příslušného orgánu, tak osoby odpovědné za zpracování údajů.

4. Evidenci lze použít pouze k účelu uvedenému v odstavcích 1 a 2 a vymaže se nejdříve po uplynutí jednoho roku a nejpozději po třech letech od jejího vytvoření. Evidence obsahující historii záznamů musí být smazána po uplynutí doby jednoho roku až tří let od výmazu záznamů.

5. Evidenci lze uchovat déle, je-li potřebná pro postupy kontroly, které již započaly.

6. Příslušné vnitrostátní orgány pověřené kontrolou, zda je vyhledávání zákonné či nikoli, sledováním zákonnosti zpracování údajů, vlastní kontrolou a zajištěním řádného fungování N. SIS II, neporušenosti údajů a jejich zabezpečení, mají v rozsahu své pravomoci a na základě žádosti do této evidence přístup, aby mohly plnit své úkoly.

Článek 13

Vlastní kontrola

Členské státy zajistí, aby každý orgán s oprávněním k přístupu k údajům SIS II učinil opatření nezbytná k zajištění dodržování tohoto nařízení a spolupracoval, je-li to nutné, s vnitrostátním orgánem dozoru.

Článek 14

Odborná příprava zaměstnanců

Dříve, než zaměstnanci orgánů s právem přístupu do SIS II obdrží povolení zpracovávat údaje uložené v SIS II, absolvují odpovídající odbornou přípravu týkající se zabezpečení údajů a pravidel o ochraně údajů a jsou informováni o jakýchkoliv příslušných trestných činech a sankcích.

KAPITOLA III

POVINNOSTI ŘÍDÍCÍHO ORGÁNU

Článek 15

Provozní řízení

1. Po přechodném období řídící orgán financovaný ze souhrnného rozpočtu Evropské unie, odpovídá za provozní řízení centrálního SIS II. Řídící orgán ve spolupráci s členskými státy zajistí na základě analýzy nákladů a přínosů, aby pro centrální SIS II byla vždy využívána nejlepší dostupná technologie.

2. Řídící orgán odpovídá též za následující úkoly spojené s komunikační infrastrukturou:

a) dohled;

b) zabezpečení;

c) koordinace vztahů mezi členskými státy a poskytovatelem.

3. Komise odpovídá za všechny ostatní úkoly spojené s komunikační infrastrukturou, zejména:

a) úkoly související s plněním rozpočtu;

b) pořizování a obnovu;

c) smluvní záležitosti.

4. Během přechodného období, než se řídící orgán ujme svých povinností, je za provozní řízení centrálního SIS II odpovědná Komise. Komise může v souladu s nařízením Rady (ES, Euratom) č. 1605/2002 ze dne 25. června 2002, kterým se stanoví finanční nařízení o souhrnném rozpočtu Evropských společenství [1] svěřit provádění tohoto řízení, jakož i úkolů souvisejících s plněním rozpočtu, vnitrostátním veřejnoprávním subjektům ve dvou různých zemích.

5. Každý vnitrostátní veřejnoprávní subjekt podle odstavce 4 musí splňovat zejména tato výběrová kritéria:

a) musí prokázat dlouhodobou zkušenost při provozování rozsáhlého informačního systému s funkcemi uvedenými v čl. 4 odst. 4;

b) musí mít značnou odbornou znalost, pokud jde o obsluhu a požadavky na zabezpečení informačního systému srovnatelného s funkcemi uvedenými v čl. 4 odst. 4;

c) musí mít dostatečný počet zkušených pracovníků, kteří mají odbornou a jazykovou kvalifikaci vhodnou pro práci v prostředí mezinárodní spolupráce, jakou vyžaduje SIS II;

d) musí mít k dispozici bezpečnou a na míru postavenou infrastrukturu zařízení, která je zejména schopná zálohovat a zaručit nepřetržitou funkčnost rozsáhlých IT systémů,

a

e) jeho administrativní prostředí mu musí umožňovat řádně plnit jeho úkoly a vyhnout se jakémukoli střetu zájmů.

6. Před jakýmkoli pověřením podle odstavce 4 a poté v pravidelných intervalech oznámí Komise Evropskému parlamentu a Radě podmínky pověření, přesný rozsah pověření a orgány, které jsou plněním úkolů pověřeny.

7. V případě, že Komise provede pověření podle odstavce 4 během přechodného období, zajistí, aby toto pověření plně respektovalo meze stanovené institucionálním systémem daným ve Smlouvě. Zejména zajistí, aby toto pověření nepříznivým způsobem neovlivnilo případný účinný kontrolní mechanismus podle práva Společenství, ať se jedná o Soudní dvůr, Účetní dvůr nebo Evropského inspektora ochrany údajů.

8. Provozní řízení centrálního SIS II sestává ze všech úkolů nezbytných pro zachování funkčnosti centrálního SIS II 24 hodiny denně sedm dní v týdnu v souladu s tímto nařízením, zejména z údržby a technického rozvoje nezbytného pro plynulý chod systému.

[1] Úř. věst. L 248, 16.9.2002, s. 1.

Článek 16

Bezpečnost

1. Řídící orgán ve vztahu k centrálnímu SIS II a Komise ve vztahu ke komunikační infrastruktuře přijmou nezbytná opatření, včetně bezpečnostního plánu, aby:

a) fyzicky chránily údaje mimo jiné vypracováním plánů pro mimořádné situace pro ochranu kritické infrastruktury;

b) zabránily neoprávněným osobám v přístupu k zařízení na zpracování údajů využívanému pro zpracování osobních údajů (kontrola přístupu k zařízení);

c) zabránily neoprávněnému čtení, kopírování, pozměňování či vyjímání nosičů dat (kontrola nosičů dat);

d) zabránily neoprávněnému vkládání údajů a neoprávněnému prohlížení, pozměňování či výmazu uložených osobních údajů (kontrola uchovávání);

e) zabránily neoprávněným osobám v užívání automatizovaných systémů zpracování údajů pomocí zařízení pro přenos údajů (kontrola uživatelů);

f) zajistily, aby osoby oprávněné k využívání automatizovaného systému zpracování údajů měly přístup pouze k údajům, na které se vztahuje jejich oprávnění k přístupu, a pouze s pomocí individuálních a jedinečných totožností uživatele a chráněných režimů přístupu k informacím (kontrola přístupu k údajům);

g) vytvořily profily popisující funkce a povinnosti osob, jež jsou oprávněny k údajům nebo k zařízením pro zpracování údajů přistupovat, a aby tyto profily na žádost bezodkladně zpřístupnily Evropskému inspektorovi ochrany údajů uvedenému v článku 45 (profily pracovníků);

h) zajistily, aby bylo možné ověřit a zjistit, kterým orgánům se mohou osobní údaje předávat prostřednictvím zařízení pro přenos údajů (kontrola předávání);

i) zajistily, aby bylo možné dodatečně ověřit a zjistit, které osobní údaje byly vloženy do automatizovaných systémů zpracování údajů, a kdo a kdy je vložil (kontrola vkládání);

j) zabránily neoprávněnému čtení, kopírování, pozměňování nebo výmazu osobních údajů během přenosů osobních údajů nebo přepravy nosičů dat, zejména prostřednictvím vhodných technik šifrování (kontrola přepravy);

k) sledovaly účinnost bezpečnostních opatření uvedených v tomto odstavci a přijaly nezbytná organizační opatření související s interním sledováním pro zajištění souladu s tímto nařízením (interní kontrola).

2. Řídící orgán přijme opatření rovnocenná opatřením uvedeným v odstavci 1, pokud jde o zabezpečení při výměně doplňujících informací prostřednictvím komunikační infrastruktury.

Článek 17

Důvěrnost - řídící orgán

1. Aniž je dotčen článek 17 služebního řádu úředníků Evropských společenství, řídící orgán použije odpovídající pravidla služebního tajemství nebo jiné srovnatelné povinnosti zachování důvěrnosti na všechny své zaměstnance, kteří musí pracovat s údaji SIS II s použitím norem srovnatelných s normami stanovenými v článku 11 tohoto nařízení. Tato povinnost trvá i poté, co dotyčné osoby opustí svůj úřad nebo zaměstnanecký poměr, nebo poté, co ukončí svou činnost.

2. Řídící orgán přijme opatření rovnocenná opatřením uvedeným v odstavci 1, pokud jde o důvěrnosti při výměně doplňujících informací prostřednictvím komunikační infrastruktury.

Článek 18

Vedení evidence na centrální úrovni

1. Řídící orgán zajistí, aby každý přístup k osobním údajům a všechny výměny osobních údajů v rámci CS-SIS byly evidovány pro účely uvedené v čl. 12 odst. 1 a 2.

2. Evidence obsahuje zejména historii záznamů, datum a čas přenosu údajů, údaje použité pro vyhledávání, odkaz na předávané údaje a název příslušného orgánu odpovědného za zpracování údajů.

3. Evidenci lze použít pouze k účelu uvedenému v odstavci 1 a vymaže se nejdříve po uplynutí jednoho roku a nejpozději po třech letech od jejího vytvoření. Evidence obsahující historii záznamů musí být smazána po uplynutí jednoho roku až tří let od výmazu záznamů.

4. Evidenci lze uchovat déle, je-li potřebná pro postupy kontroly, které již započaly.

5. Příslušné orgány pověřené kontrolou, zda je vyhledávání zákonné či nikoli, sledováním zákonnosti zpracování údajů, vlastní kontrolou a zajištěním řádného fungování CS-SIS, neporušenosti údajů a jejich zabezpečení, mají v rozsahu své pravomoci a na základě žádosti, do této evidence přístup, aby mohly plnit své úkoly.

Článek 19

Informační kampaň

Komise, ve spolupráci s vnitrostátními orgány dozoru a Evropským inspektorem ochrany údajů, spustí při zahájení provozu SIS II informační kampaň, která informuje veřejnost o účelech systému, o údajích, které se v něm ukládají, o orgánech, které k němu mají přístup a o právech osob. Po jeho zřízení řídící orgán, ve spolupráci s vnitrostátními orgány dozoru a Evropským inspektorem ochrany údajů tyto kampaně pravidelně opakuje. Členské státy, ve spolupráci se svými vnitrostátními orgány dozoru, navrhnou a provedou nezbytné politiky s cílem obecně informovat své občany o SIS II.

KAPITOLA IV

ZÁZNAMY POŘÍZENÉ O STÁTNÍCH PŘÍSLUŠNÍCÍCH TŘETÍCH ZEMÍ ZA ÚČELEM ODEPŘENÍ VSTUPU A ZÁKAZU POBYTU

Článek 20

Kategorie údajů

1. Aniž je dotčen čl. 8 odst. 1 nebo ustanovení tohoto nařízení, jež stanoví uchovávání doplňujících údajů, obsahuje SIS II pouze ty kategorie údajů, které dodává každý z členských států a které jsou potřebné pro účely uvedené v článku 24.

2. O osobách, o kterých byl pořízen záznam, se zanesou nanejvýš tyto údaje:

a) příjmení a jméno, rodné příjmení a dříve užívaná jména, a případně alias, které může být vedeno zvlášť;

b) jakékoli zvláštní objektivní a nezměnitelné tělesné znaky;

c) datum a místo narození;

d) pohlaví;

e) fotografie;

f) otisky prstů;

g) státní příslušnost (příslušnosti);

h) údaj o tom, zda je dotyčná osoba ozbrojena, má sklon k násilí nebo jde o uprchlou osobu;

i) důvod záznamu,

j) orgán pořizující záznam;

k) odkaz na rozhodnutí, na jehož základě byl záznam pořízen;

l) opatření, která je třeba přijmout;

m) odkaz (odkazy) podle článku 37 na další záznamy pořízené v SIS II.

3. Technická pravidla potřebná pro vložení, aktualizaci, vymazávání a vyhledávání údajů uvedených v odstavci 2 se stanoví postupem podle čl. 51 odst. 2, aniž jsou dotčena ustanovení nástroje, kterým se zřizuje řídící orgán.

4. Technická pravidla potřebná pro vyhledávání údajů podle odstavce 2 jsou podobná pro vyhledávání v CS-SIS, ve vnitrostátních kopiích i v kopiích pro technické účely podle čl. 31 odst. 2.

Článek 21

Proporcionalita

Členský stát před pořízením záznamu ověří, zda je daný případ dostatečně přiměřený, relevantní a závažný pro vložení do SIS II.

Článek 22

Zvláštní pravidla pro fotografie a otisky prstů

Fotografie a otisky prstů uvedené v čl. 20 odst. 2 písm. e) a f) se použijí podle těchto ustanovení:

a) fotografie a otisky prstů se vloží pouze po provedení zvláštní kontroly kvality s cílem zjistit, zda jsou splněny minimální normy kvality údajů. Upřesnění zvláštní kontroly kvality se stanoví postupem podle čl. 51 odst. 2, aniž jsou dotčena ustanovení nástroje, kterým se zřizuje řídící orgán;

b) fotografie a otisky prstů se použijí pouze k potvrzení totožnosti státních příslušníků třetích zemí, kteří byli nalezeni na základě alfanumerického vyhledávání v SIS II;

c) jakmile to bude z technického hlediska možné, lze též použít fotografie a otisky prstů k určení totožnosti státního příslušníka třetí země na základě jeho biometrického identifikátoru. Před zavedením této funkce do SIS II předloží Komise zprávu o dostupnosti a připravenosti potřebné technologie, kterou konzultuje s Evropským parlamentem.

Článek 23

Požadavek na vložení záznamu

1. Záznam nemůže být vložen bez údajů uvedených v čl. 20 odst. 2 písm. a), d), k) a l).

2. Dále se vloží všechny další údaje uvedené v čl. 20 odst. 2, jsou-li k dispozici.

Článek 24

Podmínky pořizování záznamů o odepření vstupu nebo pobytu

1. Údaje týkající se státních příslušníků třetích zemí, o kterých byl pořízen záznam pro účely odepření vstupu nebo pobytu, se vloží na základě vnitrostátního záznamu vyplývajícího z rozhodnutí přijatého příslušnými správními orgány nebo soudy v souladu s procesními předpisy, které stanoví vnitrostátní právní předpisy. Toto rozhodnutí může být učiněno pouze na základě posouzení jednotlivých případů. Odvolání proti těmto rozhodnutím se podávají v souladu s vnitrostátními právními předpisy.

2. Záznam se vloží, pokud se rozhodnutí uvedené v odstavci 1 zakládalo na tom, že přítomnost státního příslušníka třetí země na území členského státu může představovat ohrožení veřejného pořádku, veřejné bezpečnosti nebo bezpečnosti státu. Tato situace nastane zejména v případě

a) státního příslušníka třetí země, který byl v členském státě odsouzen pro trestný čin, na který se vztahuje trest odnětí svobody ve výši nejméně jednoho roku;

b) státního příslušníka třetí země, proti kterému existuje důvodné podezření, že spáchal závažné trestné činy, nebo ohledně kterého existují zjevné náznaky o úmyslu páchat takové trestné činy na území členského státu.

3. Záznam se může též vložit, pokud se rozhodnutí uvedené v odstavci 1 zakládalo na skutečnosti, že se na státního příslušníka třetí země vztahuje opatření směřující k vyhoštění, odepření vstupu nebo navrácení, které nebylo zrušeno ani pozastaveno, včetně, nebo spolu se zákazem vstupu, případně pobytu, a to z důvodu porušení vnitrostátních právních předpisů o vstupu nebo pobytu státních příslušníků třetích zemí.

4. Tento článek se nepoužije na osoby uvedené v článku 26.

5. Komise přezkoumá použití tohoto článku (po uplynutí tří let ode dne uvedeného v čl. 55 odst. 2. Na základě tohoto přezkumu učiní Komise, s využitím svého práva iniciativy v souladu se Smlouvou, nezbytné návrhy na změnu ustanovení tohoto článku, aby bylo dosaženo vyšší úrovně harmonizace kritérií pro vkládání záznamů.

Článek 25

Podmínky vkládání záznamů o státních příslušnících třetích zemí, kteří požívají práva na volný pohyb v rámci Společenství

1. Záznam týkající se státního příslušníka třetí země, který požívá práva na volný pohyb ve Společenství ve smyslu směrnice Evropského parlamentu a Rady 2004/38/ES ze dne 29. dubna 2004 o právu občanů Unie a jejich rodinných příslušníků svobodně se pohybovat a pobývat na území členských států [1] se zakládá na pravidlech přijatých za účelem provedení uvedené směrnice.

2. V případě pozitivního nálezu záznamu podle článku 24, týkajícího se státního příslušníka třetí země, který požívá práva na volný pohyb v rámci Společenství, členský stát, který záznam používá, konzultuje prostřednictvím své centrály SIRENE a v souladu s ustanoveními uvedenými v příručce SIRENE neprodleně členský stát, jenž záznam pořídil, s cílem neprodleně rozhodnout o opatření, které má být přijato.

[1] Úř. věst. L 158, 30.4.2004, s. 77.

Článek 26

Podmínky pro pořizování záznamů o státních příslušnících třetích zemí, na které se vztahují omezující opatření přijatá podle článku 15 Smlouvy o EU

1. Aniž je dotčen článek 25, vkládají se do SIS II za účelem odepření vstupu nebo zákazu pobytu údaje o státních příslušnících třetích zemí, kteří jsou předmětem omezujících opatření zaměřených na zamezení vstupu na území členských států nebo tranzitu přes něj, přijatých podle článku 15 Smlouvy o EU, včetně opatření, kterým se provádí zákaz cestování vydaný Radou bezpečnosti Organizace spojených národů, pokud jsou dodrženy požadavky na kvalitu údajů.

2. Článek 23 se nevztahuje na záznamy vložené na základě odstavce 1 tohoto článku.

3. Členský stát, který jménem všech členských států tyto záznamy vkládá, aktualizuje a vymazává, se určí v okamžiku přijetí příslušného opatření přijatého podle článku 15 Smlouvy o EU.

Článek 27

Orgány mající právo přístupu k záznamům

1. Přístup k údajům vloženým do SIS II a právo v těchto údajích vyhledávat přímo nebo v kopii údajů SIS II je vyhrazeno výlučně orgánům odpovědným za určení totožnosti státních příslušníků třetích zemí pro:

a) ochranu hranic, v souladu s nařízením Evropského parlamentu a Rady (ES) č. 562/2006 ze dne 15. března 2006, kterým se stanoví kodex Společenství o pravidlech upravujících přeshraniční pohyb osob (Schengenský hraniční kodex) ([1]);

b) provádění jiných policejních a celních kontrol v dotyčném členském státě, jakož i pro jejich koordinaci určenými orgány.

2. Právo na přístup k údajům vloženým do SIS II a právo v těchto údajích přímo vyhledávat mohou však při plnění svých úkolů stanovených vnitrostátními právními předpisy vykonávat i vnitrostátní justiční orgány, včetně těch, které odpovídají za zahájení trestního stíhání a za vyšetřování před podáním obžaloby, jakož i jejich koordinační orgány.

3. Právo na přístup k údajům vloženým v SIS II a k údajům týkajícím se osobních dokladů vloženým podle čl. 38 odst. 2 písm. d) a e) rozhodnutí 2006/000/SVV a právo v těchto údajích přímo vyhledávat mohou vykonávat orgány odpovědné za udělování víz, ústřední orgány odpovědné za projednávání žádostí o víza, jakož i orgány odpovědné za vydávání povolení k pobytu a provádění právních předpisů týkajících se státních příslušníků třetích zemí při uplatňování *acquis* Společenství o pohybu osob. Přístup těchto orgánů k údajům se řídí právem každého členského státu.

4. Orgány uvedené v tomto článku se zahrnou do seznamu uvedeného v čl. 31 odst. 8.

Článek 28

Rozsah přístupu

Uživatelé mají přístup pouze k údajům, které jsou nezbytné pro plnění jejich úkolů.

Článek 29

Doba uchovávání záznamů

1. Záznamy vložené do SIS II podle tohoto nařízení se uchovávají pouze po dobu nezbytnou pro splnění účelů, pro které byly vloženy.

2. Do tří let od vložení takového záznamu do SIS II přezkoumá členský stát, který záznam pořídil, nutnost jej zachovat.

3. Každý členský stát ve vhodných případech stanoví kratší doby pro přezkum v souladu se svými vnitrostátními právními předpisy.

4. Členský stát, který záznam pořídil, může v době pro přezkum na základě souhrnného individuálního posouzení, které se zaznamená, rozhodnout o delším zachování záznamu, je-li to nezbytné pro účely, pro něž byl záznam pořízen. V tomto případě se použije odstavec 2 také na toto delší zachování. Jakékoliv prodloužení záznamu musí být sděleno CS-SIS.

5. Záznamy se automaticky vymazávají po uplynutí doby pro přezkum uvedené v odstavci 2 s výjimkou případu, kdy členský stát, který záznam pořídil, informoval CS-SIS o prodloužení záznamu podle odstavce 4. CS-SIS automaticky čtyři měsíce předem uvědomí členské státy o plánovaném výmazu údajů ze systému.

([1]) Úř. věst. L 105, 13.4.2006, s. 1.

6. Členské státy uchovávají statistiky o počtu záznamů, u nichž byla doba uchovávání prodloužena v souladu s odstavcem 4.

Článek 30

Získání občanství a záznamy

Záznamy pořízené o osobě, která získala občanství kteréhokoli státu, jehož státní příslušníci požívají práva na volný pohyb v rámci Společenství, se vymažou, jakmile je členský stát, který záznam pořídil, informován podle článku 34 nebo se jinak dozví o tom, že dotyčná osoba takovéto občanství získala, nebo jakmile se o tom tento členský stát dozví.

KAPITOLA V

OBECNÁ PRAVIDLA PRO ZPRACOVÁNÍ ÚDAJŮ

Článek 31

Zpracování údajů v SIS II

1. Členské státy mohou zpracovávat údaje uvedené v článku 20 za účelem odepření vstupu nebo pobytu na svých územích.

2. Kopie údajů se mohou pořizovat pouze pro technické účely, pokud jsou potřebné k přímému vyhledávání orgány uvedenými v článku 27. Na tyto kopie se použijí ustanovení tohoto nařízení. Záznamy pořízené jinými členskými státy nesmějí být kopírovány z jejich N. SIS II do jiných vnitrostátních souborů údajů.

3. Technické kopie podle odstavce 2, které vedou ke vzniku off-line databází, lze uchovávat pouze na dobu nepřesahující 48 hodin. V mimořádných situacích může být tato doba prodloužena až do konce mimořádné situace.

Bez ohledu na první pododstavec technické kopie, jež vedou ke vzniku off-line databází, které mají být využívány orgány vydávajícími víza, nejsou povoleny po uplynutí jednoho roku od úspěšného připojení dotyčného orgánu ke komunikační infrastruktuře Vízového informačního systému, jak bude stanoveno v novém nařízení o Vízovém informačním systému (VIS) a výměně údajů mezi členskými státy o krátkodobých vízech. To se nevztahuje na pořízené kopie, které mají být použity pouze při mimořádných situacích v důsledku nedostupnosti sítě pod dobu delší než 24 hodin.

Členské státy udržují aktuální soupis těchto kopií, zpřístupňují tento soupis svým vnitrostátním orgánům dozoru a zajišťují, že se na tyto kopie použijí ustanovení tohoto nařízení, zejména článku 10.

4. Přístup k takovým údajům se povoluje pouze v mezích pravomoci vnitrostátních orgánů uvedených v článku 27 a pouze osobám vybaveným náležitým oprávněním.

5. Údaje nesmí být využívány k administrativním účelům. Odchylně mohou být údaje vložené v souladu s tímto nařízením používány v souladu s právními předpisy jednotlivých členských států orgány uvedenými v čl. 27 odst. 3 při plnění svých úkolů.

6. Údaje vložené v souladu s článkem 24 tohoto nařízení a údaje týkající se osobních dokladů vložené podle čl. 38 odst. 2 písm. d) a e) rozhodnutí 2006/…/SVVsmějí být použity v souladu s právními předpisy každého členského státu pro účely uvedené v čl. 27 odst. 3 tohoto nařízení.

7. Jakékoli využití údajů, které není v souladu s odstavci 1 až 6, je podle vnitrostátních právních předpisů každého členského státu považováno za zneužití.

8. Každý členský stát zašle řídícímu orgánu seznam svých příslušných orgánů, které jsou podle tohoto nařízení oprávněny přímo vyhledávat v údajích obsažených v SIS II, jakož i změny tohoto seznamu. V tomto seznamu je u každého orgánu uvedeno, v jakých údajích může vyhledávat a za jakými účely. Řídící orgán zajistí každoroční zveřejnění seznamu v Úředním věstníku Evropské unie.

9. Nestanoví-li právní předpisy Společenství zvláštní ustanovení, použijí se pro údaje vložené v N. SIS II právní předpisy každého příslušného členského státu.

Článek 32

Údaje SIS II a vnitrostátní soubory

1. Článkem 31 odst. 2 není dotčeno právo členského státu uchovávat ve svých vnitrostátních souborech údaje SIS II, ve spojitosti s nimiž bylo učiněno opatření na jeho území. Takové údaje se uchovávají ve vnitrostátních souborech nanejvýš po dobu tří let s výjimkou případů, kdy konkrétní ustanovení vnitrostátního práva upravují delší dobu uchovávání.

2. Článkem 31 odst. 2 není dotčeno právo členského státu uchovávat ve svých vnitrostátních souborech údaje obsažené v konkrétním záznamu, který dotyčný členský stát do SIS II vložil.

Článek 33

Informování v případě nepoužití záznamu

Nemohou-li být požadovaná opatření provedena, uvědomí o tom dožádaný členský stát neprodleně členský stát, který pořídil záznam.

Článek 34

Kvalita údajů zpracovávaných v SIS II

1. Členský stát pořizující záznam odpovídá za zajištění toho, že údaje jsou správné, aktuální a jsou vložené v SIS II v souladu se zákonem.

2. Pouze členský stát, který vložil záznam, je oprávněn měnit, doplňovat, opravovat, aktualizovat nebo mazat údaje, které vložil.

3. Má-li některý z členských států, který nepořídil záznam, důkazy naznačující, že položka údaje je věcně nesprávná nebo je uchovávána protiprávně, informuje o tom co nejdříve a nejpozději do deseti dnů poté, co se o uvedeném důkazu dozvěděl, členský stát, který záznam pořídil, prostřednictvím výměny doplňujících informací. Členský stát, který záznam pořídil, sdělení prověří a v případě potřeby dotyčnou položku neprodleně opraví nebo vymaže.

4. Nemohou-li se členské státy dohodnout ve lhůtě dvou měsíců, předloží členský stát, který nepořídil záznam, věc Evropskému inspektorovi ochrany údajů, který spolu s dotyčnými vnitrostátními orgány dozoru vystupuje jako prostředník.

5. Členské státy si vymění doplňující informace v případě, že si dotyčná osoba stěžuje, že není osobou, k níž se má záznam vztahovat. Prokáže-li kontrola, že se skutečně jedná o dvě odlišné osoby, bude osoba, která si stěžuje, informována o ustanoveních článku 36.

6. Pokud je určitá osoba již předmětem záznamu v SIS II, dohodne se o vložení tohoto záznamu členský stát, který vkládá další záznam, s členským státem, který vložil záznam první. Dohody je dosaženo na základě výměny doplňujících informací.

Článek 35

Rozlišování mezi osobami s podobnými znaky

Pokud se při vkládání nového záznamu ukáže, že v SIS II již existuje záznam o osobě se stejnými prvky popisu totožnosti, postupuje se takto:

a) centrála SIRENE kontaktuje žádající orgán s cílem objasnit, zda se záznam týká stejné osoby či nikoli;

b) v případě, že kontrola prokáže, že osoba, jež je předmětem nového záznamu, a osoba, o níž již existuje záznam v SIS II, je ve skutečnosti jedna a ta samá, centrála SIRENE použije postup vkládání vícenásobných záznamů uvedený v čl. 34 odst. 6. Prokáže-li kontrola, že se ve skutečnosti jedná o dvě různé osoby, centrála SIRENE schválí požadavek na vložení dalšího záznamu a to tak, že doplní potřebné prvky, které zabrání jakýmkoli chybným určením totožnosti.

Článek 36

Další údaje pro účely řešení zneužití totožnosti

1. Může-li dojít k záměně mezi osobou, která má být ve skutečnosti předmětem záznamu, a osobou, jejíž totožnost byla zneužita, doplní členský stát, který záznam vložil, tento záznam o údaje týkající se osoby, jejíž totožnost byla zneužita, za podmínky jejího výslovného souhlasu, aby se předešlo nežádoucím důsledkům chybného určení totožnosti.

2. Údaje týkající se osoby, jejíž totožnost byla zneužita, se použijí pouze pro tyto účely:

a) umožnit příslušnému orgánu odlišit osobu, jejíž totožnost byla zneužita, od osoby, jež je ve skutečnosti předmětem záznamu;

b) umožnit osobě, jejíž totožnost byla zneužita, prokázat svoji totožnost a dokázat, že její totožnost byla zneužita.

3. Za účelem naplnění tohoto článku lze vložit a dále zpracovávat v SIS II nanejvýš tyto osobní údaje:

a) příjmení a jméno (jména), rodné (rodná) příjmení a dříve užívaná jména, případně alias, které může být vedeno zvlášť;

b) jakékoli zvláštní objektivní a nezměnitelné tělesné znaky;

c) datum a místo narození;

d) pohlaví;

e) fotografie;

f) otisky prstů;

g) státní příslušnost (příslušnosti);

h) číslo (čísla) průkazu (průkazů) totožnosti a datum vydání.

4. Technická pravidla potřebná pro vložení a další zpracování údajů uvedených v odstavci 3 se stanoví postupem podle čl. 51 odst. 2, aniž jsou dotčena ustanovení nástroje, kterým se zřizuje řídící orgán.

5. Údaje uvedené v odstavci 3 se vymažou současně s odpovídajícím záznamem nebo dříve, pokud o to osoba požádá.

6. K údajům uvedeným v odstavci 3 mohou přistupovat pouze orgány mající právo přístupu k odpovídajícímu záznamu, a to pouze za účelem předcházení chybnému určení totožnosti.

Článek 37

Odkazy mezi záznamy

1. Členský stát může vytvořit odkaz mezi jím vloženými záznamy v SIS II. Smyslem takového odkazu je zavést souvislost mezi dvěma nebo více záznamy.

2. Vytvoření odkazu nemá dopad na konkrétní opatření, které má být provedeno na základě jednotlivého záznamu opatřeného odkazem, nebo na dobu uchovávání jednotlivých záznamů propojených odkazy.

3. Vytvoření odkazu nemá dopad na práva přístupu upravená tímto nařízením. Orgánům bez práva přístupu k některým kategoriím záznamů není umožněno vidět odkaz na záznam, ke kterému nemají přístup.

4. Členský stát vytvoří odkaz mezi záznamy pouze tehdy, je-li to z operativního hlediska zjevně potřebné.

5. Členský stát může vytvořit odkazy v souladu se svými vnitrostátními právními předpisy, pokud jsou dodržovány zásady uvedené v tomto článku.

6. Domnívá-li se členský stát, že vytvoření odkazu mezi záznamy jiným členským státem je neslučitelné s jeho vnitrostátními právními předpisy nebo mezinárodními závazky, může přijmout nezbytná opatření, která znemožní přístup k příslušnému odkazu z jeho území nebo jeho orgánům nacházejícím se vně jeho území.

7. Technická pravidla pro odkazování mezi záznamy se přijmou postupem podle čl. 51 odst. 2, aniž jsou dotčena ustanovení nástroje, kterým se zřizuje řídící orgán.

Článek 38

Účel a doba uchovávání doplňujících informací

1. S cílem podporovat výměnu doplňujících informací uchovávají členské státy v centrále SIRENE odkaz na rozhodnutí, na jejichž základě byl záznam pořízen.

2. Osobní údaje vedené v souborech centrálou SIRENE v důsledku výměny informací se uchovávají pouze po dobu potřebnou pro dosažení účelů, pro něž byly tyto údaje poskytnuty. Výmaz těchto údajů se v každém případě provede nejpozději do jednoho roku po výmazu souvisejícího záznamu ze SIS II.

3. Odstavcem 2 není dotčeno právo členského státu uchovávat ve vnitrostátních souborech údaje týkající se konkrétního záznamu, který členský stát pořídil, nebo záznamu, ve spojení s nímž bylo učiněno opatření na jeho území. Časové období, po které mohou být takové údaje vedeny v takových souborech, se řídí vnitrostátními právními předpisy.

Článek 39

Poskytnutí osobních údajů třetím stranám

Údaje zpracovávané v SIS II podle tohoto nařízení se neposkytují ani nezpřístupňují žádné třetí zemi nebo mezinárodní organizaci.

KAPITOLA VI

OCHRANA ÚDAJŮ

Článek 40

Zpracování citlivých kategorií údajů

Zakazuje se zpracování kategorií údajů uvedených v čl. 8 odst. 1 směrnice 95/46/ES.

Článek 41

Přístupové právo, oprava nepřesných údajů a výmaz protiprávně uchovávaných údajů

1. Právo osob na přístup k údajům vloženým o nich v SIS II v souladu s tímto nařízením se vykonává v souladu s právními předpisy členského státu, u kterého toto právo uplatňují.

2. Pokud to stanoví vnitrostátní právní předpisy, rozhoduje o tom, zda a jakým způsobem se tyto informace poskytují, vnitrostátní orgán dozoru.

3. Členský stát, který záznam nepořídil, může poskytnout informace o těchto údajích pouze tehdy, pokud předtím poskytl členskému státu, který záznam pořídil, příležitost zaujmout postoj. To se provádí prostřednictvím výměny doplňujících informací.

4. Informace nebude subjektu údajů poskytnuta, pokud je to nevyhnutelné pro výkon zákonného úkolu v souvislosti se záznamem nebo z důvodu ochrany práv a svobod třetích stran.

5. Každý má právo na opravu věcně nepřesných údajů nebo výmaz protiprávně uchovávaných údajů, které se jej týkají.

6. Dotyčná osoba je informována co nejdříve a v každém případě nejpozději do 60 dnů ode dne žádosti o přístup nebo dříve, stanoví-li tak vnitrostátní právní předpisy.

7. Tato osoba je o činnostech v návaznosti na výkon jejích práv na opravu a výmaz informována co nejdříve a v každém případě nejpozději do tří měsíců ode dne, kdy požádala o opravu nebo výmaz nebo dříve, stanoví-li tak vnitrostátní právní předpisy.

Článek 42

Právo na informace

1. Státní příslušníci třetích zemí, kteří jsou předmětem záznamů pořízených v souladu s tímto nařízením, se informují v souladu s články 10 a 11 směrnice 95/46/ES. Tyto informace se poskytnou písemně, společně s kopií vnitrostátního rozhodnutí, na jehož základě byl záznam pořízen, nebo s odkazem na ně podle čl. 24 odst. 1.

2. Tyto informace se neposkytnou:

a) pokud

i) osobní údaje nebyly získány od dotyčného státního příslušníka třetí země;

a

ii) poskytnutí informací se ukáže jako nemožné nebo by vyžadovalo nepřiměřené úsilí;

b) pokud dotyčný státní příslušník třetí země již informace má;

c) pokud vnitrostátní právní předpisy umožňují omezení práva na informace, zejména za účelem zajištění národní bezpečnosti, obrany, veřejné bezpečnosti a pro předcházení, vyšetřování, odhalování a stíhání trestných činů.

Článek 43

Opravné prostředky

1. Každý má právo podat žalobu u soudu nebo orgánu příslušného podle právních předpisů kteréhokoliv členského státu, zejména ve věci přístupu, opravy, výmazu či poskytnutí informace nebo odškodnění v souvislosti se záznamem, který se ho týká.

2. Aniž jsou dotčena ustanovení článku 48, zavazují se členské státy navzájem vymáhat konečná rozhodnutí vydaná soudy nebo orgány uvedenými v odstavci 1.

3. Do… Komise posoudí pravidla týkající se opravných prostředků uvedená v tomto článku.

Článek 44

Dohled nad N. SIS II

1. Orgán nebo orgány, které byly v každém členském státě určeny a které mají pravomoci uvedené v článku 28 směrnice 95/46/ES (dále jen „vnitrostátní orgány dozoru"), sledují nezávisle zákonnost zpracování osobních údajů v SIS II na svých územích a jejich předávání mimo svá území, včetně výměny a dalšího zpracování doplňujících informací.

2. Vnitrostátní orgány dozoru zajistí, aby alespoň každým čtvrtým rokem byl v souladu s mezinárodními auditorskými standardy proveden audit činností zpracování údajů v N. SIS II.

3. Členské státy zajistí, aby vnitrostátní orgány dozoru měly dostatečné zdroje pro plnění úkolů, které jim byly podle tohoto nařízení svěřeny.

Článek 45

Dohled nad řídícím orgánem

1. Evropský inspektor ochrany údajů kontroluje, zda jsou činnosti řídícího orgánu související se zpracováváním osobních údajů prováděny v souladu s tímto nařízením. Odpovídajícím způsobem se použijí povinnosti a pravomoci uvedené v článku 46 a 47 nařízení (ES) č. 45/2001.

2. Evropský inspektor ochrany údajů zajistí, aby byl alespoň každým čtvrtým rokem v souladu s mezinárodními auditorskými standardy proveden audit činností řídícího orgánu souvisejících se zpracováváním osobních údajů. Zpráva vzešlá z auditu se zašle Evropskému parlamentu, Radě, řídícímu orgánu, Komisi a vnitrostátním orgánům dozoru. Řídícímu orgánu se poskytne příležitost zprávu připomínkovat před jejím přijetím.

Článek 46

Spolupráce mezi vnitrostátními orgány dozoru a Evropským inspektorem ochrany údajů

1. Vnitrostátní orgány dozoru a Evropský inspektor ochrany údajů, každý z nich jednaje v rozsahu svých příslušných pravomocí, aktivně spolupracují v rámci svých odpovědností a zajišťují koordinovaný dohled nad SIS II.

2. Vyměňují si příslušné informace, každý z nich jednaje v rámci svých příslušných pravomocí, pomáhají si navzájem při provádění auditů a kontrol, přezkoumávají obtíže týkající se výkladu nebo použití tohoto nařízení, zabývají se problémy při výkonu nezávislého dohledu nebo při výkonu práv subjektu údajů, vypracovávají harmonizované návrhy společných řešení případných problémů a podle potřeby zvyšují povědomí o právech na ochranu údajů.

3. Vnitrostátní orgány dozoru a Evropský inspektor ochrany údajů se za tímto účelem setkávají alespoň dvakrát do roka. Náklady na tato setkání a jejich obsluhu nese Evropský inspektor ochrany údajů. Na prvním setkání se přijme jednací řád. Další pracovní metody se vypracují společně podle potřeby. Společná zpráva o činnostech se zasílá Evropskému parlamentu, Radě, Komisi a řídícímu orgánu každé dva roky.

Článek 47

Ochrana údajů během přechodného období

V případě, že Komise podle čl. 15 odst. 4 pověří jiný orgán plněním svých povinností během přechodného období, zajistí, aby měl Evropský inspektor ochrany údajů právo a možnost plně vykonávat své úkoly, včetně možnosti provádět kontroly na místě nebo vykonávat jiné pravomoci, které na něj byly přeneseny podle článku 47 nařízení (ES) č. 45/2001.

KAPITOLA VII

ODPOVĚDNOST A SANKCE

Článek 48

Odpovědnost

1. Každý členský stát odpovídá v souladu se svými vnitrostátními právními předpisy za škodu způsobenou kterékoli osobě při využívání N. SIS II. To platí i v případě škody způsobené členským státem, který záznam pořídil, tím, že tento členský stát vložil věcně nepřesné údaje nebo údaje protiprávně uchovával.

2. Není-li členský stát, proti němuž je podána žaloba, členským státem pořizujícím záznam, je členský stát pořizující záznam povinen uhradit na žádost částky vyplacené jako náhrada, ledaže členský stát, který žádá o náhradu, použil údaje v rozporu s tímto nařízením.

3. Pokud nesplnění povinností plynoucích z tohoto nařízení členským státem způsobí SIS II škodu, je daný členský stát za tuto škodu odpovědný, ledaže řídící orgán nebo jiný členský stát účastnící se na SIS II neučinily přiměřené kroky s cílem předejít této škodě nebo zmírnit její následky.

Článek 49

Sankce

Členské státy zajistí, aby jakékoli zneužití údajů vložených v SIS II nebo jakákoli výměna doplňujících informací v rozporu s tímto nařízením podléhaly účinným, přiměřeným a odrazujícím sankcím v souladu s vnitrostátními právními předpisy.

KAPITOLA VIII

ZÁVĚREČNÁ USTANOVENÍ

Článek 50

Sledování a statistika

1. Řídící orgán zajistí zavedení postupů pro sledování fungování SIS II týkajících se výstupů, účinnosti vynaložených prostředků, bezpečnosti a kvality služeb.

2. Pro účely technické údržby, vypracovávání zpráv a statistik má řídící orgán přístup k nezbytným informacím souvisejícím s operacemi zpracování prováděnými v centrálním SIS II.

3. Každým rokem zveřejní řídící orgán statistické údaje, z kterých vyplývá počet evidovaných vstupů připadajících na jednu kategorii záznamů, počet pozitivních nálezů připadajících na jednu kategorii záznamů a počet přístupů do SIS II, a to pro každý tento počet celkem a pro každý členský stát jednotlivě.

4. Dva roky po spuštění provozu SIS II a poté vždy po dvou letech předloží řídící orgán Evropskému parlamentu a Radě zprávu o technickém fungování centrálního SIS II a komunikační infrastruktury, včetně její bezpečnosti, a dvoustranné a mnohostranné výměny doplňujících informací mezi členskými státy.

5. Tři roky po spuštění provozu SIS II a poté vždy po čtyřech letech vypracuje Komise celkové vyhodnocení centrálního SIS II a dvoustranné i mnohostranné výměny doplňujících informací mezi členskými státy. Toto celkové vyhodnocení musí zahrnovat přezkoumání dosažených výsledků v porovnání s vytyčenými cíli, posouzení trvající platnosti důvodu pro vznik systému, použití tohoto nařízení ve vztahu k centrálnímu SIS II, bezpečnost centrálního SIS II, jakož i všech dopadů jeho budoucího provozování. Komise předá tato hodnocení Evropskému parlamentu a Radě.

6. Členské státy poskytnou řídícímu orgánu a Komisi informace nezbytné pro vypracování zpráv uvedených v odstavcích 3, 4 a 5.

7. Členské státy poskytnou Komisi informace nezbytné pro vypracování celkových vyhodnocení uvedených v odstavci 5.

8. Během přechodného období, než se řídící orgán ujme svých povinností, je za vypracování a podávání zpráv uvedených v odstavcích 3 a 4 odpovědná Komise.

Článek 51

Výbor

1. Komisi je nápomocen výbor.

2. Odkazuje-li se na tento odstavec, použijí se články 5 a 7 rozhodnutí 1999/468/ES s ohledem na článek 8 zmíněného rozhodnutí.

Doba uvedená v čl. 5 odst. 6 rozhodnutí 1999/468/ES je tři měsíce.

3. Výbor vykonává svou funkci ode dne vstupu tohoto nařízení v platnost.

Článek 52

Změna ustanovení Schengenského acquis

1. Pro účely záležitostí spadajících do oblasti působnosti Smlouvy nahrazuje toto nařízení, ode dne uvedeného v čl. 55 odst. 2, ustanovení článků 92 až 119 Schengenské úmluvy s výjimkou jejího čl. 102a.

2. Toto nařízení rovněž nahrazuje, ode dne uvedeného v čl. 55 odst. 2, níže uvedená ustanovení schengenského *acquis* provádějící uvedené články [1]:

a) Rozhodnutí výkonného výboru ze dne 14. prosince 1993 o finančním nařízení o nákladech na zřízení a provoz Schengenského informačního systému (C. SIS) (SCH/Com-ex (93) 16);

b) Rozhodnutí výkonného výboru ze dne 7. října 1997 o vývoji SIS (SCH/Com-ex (97) 24);

c) Rozhodnutí výkonného výboru ze dne 15. prosince 1997, kterým se mění finanční nařízení o C. SIS (SCH/Com-ex (97) 35);

d) Rozhodnutí výkonného výboru ze dne 21. dubna 1998 o C. SIS s 15/18 přípojkami (SCH/Com-ex (98) 11);

e) Rozhodnutí výkonného výboru ze dne 28. dubna 1999 o výdajích na zřízení C. SIS (SCH/Com-ex (99) 4);

f) Rozhodnutí výkonného výboru ze dne 28. dubna 1999 o aktualizaci příručky SIRENE (SCH/Com-ex (99) 5);

g) Prohlášení výkonného výboru ze dne 18. dubna 1996, kterým se vymezuje pojem cizí státní příslušník (SCH/Com-ex (96) decl. 5);

h) Prohlášení výkonného výboru ze dne 28. dubna 1999 o struktuře SIS (SCH/Com-ex (99) decl. 2 rev.);

i) Rozhodnutí výkonného výboru ze dne 7. října 1997 o příspěvcích Norska a Islandu na náklady na zřízení a provoz C. SIS (SCH/Com-ex (97) 18).

3. Pro účely záležitostí spadajících do oblasti působnosti Smlouvy se odkazy na nahrazené články Schengenské úmluvy a na příslušná ustanovení schengenského *acquis*, kterými se uvedené články provádějí, považují za odkazy na toto nařízení.

[1] Úř. věst. L 239, 22.9.2000 s. 439.

Článek 53

Ustanovení o zrušení

Nařízení (ES) č. 378/2004 a nařízení (ES) č. 871/2004, rozhodnutí 2005/451/SVV, rozhodnutí 2005/728/SVV a rozhodnutí 2006/628/ES se zrušují ode dne uvedeného v čl. 55 odst. 2.

Článek 54

Přechodné období a rozpočet

1. Záznamy se přenesou ze SIS 1+ do SIS II. Členské státy zajistí, aby byl obsah záznamů, které jsou přeneseny ze SIS 1+ do SIS II, co nejdříve a nejpozději do tří let ode dne uvedeného v čl. 55 odst. 2 uveden v soulad s ustanoveními tohoto nařízení, přičemž přednost mají záznamy o osobách. Členské státy mohou během tohoto přechodného období i nadále používat pro obsah záznamů, které jsou přeneseny ze SIS 1+ do SIS II, ustanovení článků 94 a 96 Schengenské úmluvy, a to s výhradou těchto zásad:

a) v případě změny, doplnění nebo opravy nebo aktualizace obsahu záznamu přeneseného ze SIS 1+ do SIS II členské státy zajistí, aby záznam ode dne této změny, doplnění, opravy nebo aktualizace vyhovoval ustanovením tohoto nařízení;

b) v případě pozitivního nálezu záznamu přeneseného ze SIS 1+ do SIS II členské státy posoudí soulad uvedeného záznamu s ustanoveními tohoto nařízení bezodkladně, ale bez zpoždění opatření, která mají být přijata na základě uvedeného záznamu.

2. K datu stanovenému v souladu s čl. 55 odst. 2 se zbývající část rozpočtu, která byla schválena v souladu s článkem 119 Schengenské úmluvy, členským státům vrátí. Částky, které mají být vráceny, se vypočítají na základě příspěvků členských států, jak jsou stanoveny rozhodnutím výkonného výboru ze dne 14. prosince 1993 o finančním nařízení o nákladech na zřízení a provoz Schengenského informačního systému.

3. Během přechodného období uvedeného v čl. 15 odst. 4 se odkazy na řídící orgán uvedené tomto nařízení považují za odkaz na Komisi.

Článek 55

Vstup v platnost, použitelnost a migrace

1. Toto nařízení vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

2. Vztahuje se na členské státy, které se účastní SIS 1+ ode dne, který stanoví Rada jednomyslným usnesením svých členů zastupujících vlády členských států, které se účastní SIS 1+.

3. Datum uvedené v odstavci 2 se určí:

a) po přijetí nezbytných prováděcích opatření;

b) po tom, co všechny členské státy, které se plně účastní SIS 1+ Komisi oznámí, že přijaly nezbytná technická a právní opatření pro zpracovávání údajů SIS II a výměnu dodatečných informací;

c) po tom, co Komise oznámí úspěšné dokončení souhrnného testu SIS II, který provede Komise společně s členskými státy a po tom, co přípravné orgány Rady ověří navrhovaný výsledek testu a potvrdí, že úroveň funkční způsobilosti SIS II je přinejmenším rovnocenná úrovni funkční způsobilosti, které bylo dosaženo u SIS 1+;

d) po tom, co Komise provede veškerá nezbytná technická opatření umožňující připojení centrálního SIS II k N. SIS II dotyčných členských států.

4. Komise sdělí Evropskému parlamentu výsledky testů provedených podle odst. 3 písm. c).

5. Každé rozhodnutí Rady přijaté v souladu s odstavcem 2 se zveřejní v *Úředním věstníku Evropské unie*.

Toto nařízení je závazné v celém rozsahu a přímo použitelné v členských státech v souladu se Smlouvou o založení Evropského společenství.

V Bruselu dne20. prosince 2006

Za Evropský parlament	*Za Radu*
předseda	*předseda*
J. BORRELL FONTELLES	J. KORKEAOJA

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 450 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 5, Elišky Peškové 14, tel./fax: 257 320 049, – 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