VĚSTNÍK
ÚŘADU PRO OCHRANU OSOBNÍCH ÚDAJŮ
2006

Částka 43 | **15. prosince 2006** | **Cena 77,– Kč**

OBSAH

ÚVOD

Částka 43 Věstníku Úřadu pro ochranu osobních údajů obsahuje přehled zrušených registrací za období od 11. 9. 2006 do 25. 11. 2006.

Rubrika Stanoviska Úřadu obsahuje tři oficiální stanoviska Úřadu: „Nahlížení do kandidátních listin a poskytování informací o kandidátech voleb do obecních zastupitelstev“, „Dozorové pravomoci Úřadu pro ochranu osobních údajů v souvislosti s výkonem advokacie“ a stanovisko „K využívání elektronických karet“.

V rubrice Sdělení Úřadu je publikována informace „Registrační povinnost správce a připravované změny“ upozorňující na zavedení nového elektronického registračního systému pro správce osobních údajů, který slouží k plnění oznamovací povinnosti podle § 16 zákona o ochraně osobních údajů. Další součástí této rubriky je materiál „Závazná podniková pravidla (Binding Corporate Rules) jako nástroj bezpečného předávání osobních údajů do třetích zemí“. Předávání osobních údajů v rámci nadnárodních společností se stalo každodenní potřebou. Je v zájmu nejen podnikatelského sektoru, ale také dozorových úřadů, vytvořit fungující a životaschopný nástroj zajišťující dostatečnou ochranu osobních údajů při jejich zpracování a předávání do třetích zemí. Takovým nástrojem mohou být i závazná podniková pravidla, tzv. Binding Corporate Rules - BCR.

Rubrika Sdělení Úřadu přináší také materiály Pracovní skupiny pro ochranu dat zřízené podle článku 29 směrnice 95/46/ES. Prvním materiálem je „Pracovní dokument o otázkách ochrany údajů, které souvisejí s technologií RFID“. Vzhledem k rostoucímu používání technologie RFID pro různé účely a aplikace, z nichž některé s sebou nesou obrovské důsledky pro ochranu údajů, se Úřad rozhodl, že je nezbytné zveřejnit tento pracovní dokument a přispět k probíhající diskuzi o otázkách RFID. Dalšími materiály jsou dvě stanoviska této pracovní skupiny. Jsou jimi Stanovisko č. 3/2006, které pojednává o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a na závěr Stanovisko 6/2005 zaměřené na oblast Schengenského informačního systému druhé generace (SIS II).

Přehled zrušených registrací

Číslo registrace	Subjekt	Datum zrušení
00000058/001	CONTACTEL S.R.O.	23. 9. 2006
00000524/001	MĚSTSKÁ KNIHOVNA	28. 9. 2006
00003849/001	MND STAVOTRANS A.S.	22. 9. 2006
00003849/002	MND STAVOTRANS A.S.	22. 9. 2006
00003929/001	KPNQWEST CZECHIA S.R.O.	23. 9. 2006
00004882/001	FC LEASING, K.S.	6. 10. 2006
00005342/002	PLZEŇSKÉ MĚSTSKÉ DOPRAVNÍ PODNIKY, A.S.	28. 9. 2006
00005755/001	ŽDB, A.S.	20. 9. 2006
00005755/002	ŽDB, A.S.	20. 9. 2006
00005755/003	ŽDB, A.S.	20. 9. 2006
00005755/004	ŽDB, A.S.	20. 9. 2006
00018010/001	CV BOHEMIA SPOL. S R. O.	15. 11. 2006
00018631/001	NEXTRA CZECH REPUBLIC S.R.O.	23. 9. 2006
00018926/001	TOURINVEST A.S. PRAHA	16. 11. 2006
00019842/001	GTS CZECH A.S.	23. 9. 2006
00025974/001	DOMOV SV. ALŽBĚTY	14. 9. 2006

II. STANOVISKA ÚŘADU

Stanovisko č. 6/2006

říjen 2006

Nahlížení do kandidátních listin a poskytování informací o kandidátech voleb do obecních zastupitelstev

V souvislosti s volbami do obecních zastupitelstev předkládá Úřad pro ochranu osobních údajů stanovisko týkající se poskytování informací o kandidátech do zastupitelstev a nahlížení do kandidátních listin.

Obecně lze říci, že souhlasem s kandidaturou se kandidát částečně vzdává svého soukromí. Tento zásah do soukromí je však nezbytné omezit v souladu s platnou právní úpravou. Informace ve věci kandidátů či kandidátních listin jsou požadovány na základě zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů (dále jen „zákon o svobodném přístupu k informacím"), který byl několikrát novelizován, naposled v letošním roce.

Poslední novela přinesla nový § 8a, který stanoví, že „informace týkající se osobnosti, projevů osobní povahy, soukromí fyzické osoby a osobní údaje povinný subjekt poskytne jen v souladu s právními předpisy, upravujícími jejich ochranu." Uvedenými předpisy jsou především ustanovení § 11-16 zákona č. 40/1964 Sb., Občanský zákoník, ve znění pozdějších předpisů a ustanovení § 5 a § 10 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „zákon o ochraně osobních údajů").

Poskytování informací o jednotlivých kandidátech a nahlížení do kandidátních listin, kdy se nepochybně jedná o zpracování osobních údajů, podléhá úpravě podle § 5 zákona o ochraně osobních údajů. V daném případě ovšem nelze aplikovat žádné z ustanovení § 5 odst. 2 písm. a) – g) tohoto zákona, ani ustanovení § 5 odst. 2 písm. f) zákona o ochraně osobních údajů, neboť se nejedná o informace o veřejně činné osobě, funkcionáři či zaměstnanci veřejné správy, které vypovídají o jeho veřejné nebo úřední činnosti, o jeho funkčním nebo pracovním zařazení. Informace se týkají osobních údajů konkrétní osoby a lze je poskytnout či umožnit nahlédnutí v souladu s ustanovením § 5 odst. 2 zákona o ochraně osobních údajů pouze se souhlasem této osoby.

V této souvislosti je nezbytné uvést, že je vždy třeba určit okamžik, kdy je již možné osobní údaje poskytnout bez souhlasu osoby, jejíž údaje mají být poskytnuty. Takto je míněn právě okamžik, kdy se požadované osobní údaje stávají údaji zveřejněnými a je možné je jako takové poskytovat. Vyplývá to z ustanovení § 23 odst. 3 a odst. 4 zákona č. 491/2001 Sb., o volbách do zastupitelstev obcí a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „zákon o volbách do zastupitelstev obcí").

Podle ustanovení § 23 odst. 3 uvedeného zákona registrační úřad rozhodne ve lhůtě 48 dnů před dnem voleb do zastupitelstva obce o registraci kandidátní listiny splňující náležitosti podle § 23 odst. 4 téhož zákona. Současně toto rozhodnutí vyvěsí na úřední desce registračního úřadu a vyznačí den vyvěšení. Registrace je rovněž podle ustanovení § 23 odst. 7 zákona o volbách do zastupitelstev podmínkou pro vytištění hlasovacích lístků. Tento postup je také v souladu s ustanovením § 11 odst. 1 písm. b) zákona o svobodném přístupu k informacím, podle kterého „povinný subjekt může omezit poskytnutí informace, pokud jde o novou informaci, která vznikla při přípravě rozhodnutí povinného subjektu, pokud zákon nestanoví jinak; to platí jen do doby, kdy se příprava ukončí rozhodnutím".

Zveřejnění rozhodnutí o registraci kandidátní listiny je provedeno dle platné právní úpravy, neboť je naplněno ustanovení § 5 odst. 2 písm. a) zákona o ochraně osobních údajů, které správci umožňuje zpracovávat, v souladu s ustanovením § 4 písm. e) zákona o ochraně osobních údajů (tedy i zveřejňovat), osobní údaje bez souhlasu subjektu údajů, jestliže provádí zpracování nezbytné pro dodržení právní povinnosti správce.

Úřad pro ochranu osobních údajů zastává názor, že právě den vyvěšení je dnem, kdy již lze údaje považovat za údaje zveřejněné ve smyslu ustanovení § 4 písm. l) zákona o ochraně osobních údajů, a od tohoto data mohou být informace o kandidátech uvedené na registrované kandidátní listině poskytovány. Při poskytování informací musejí příslušné úřady splňovat příslušná ustanovení zákona o ochraně osobních údajů týkající se např. rozsahu poskytovaných informací. Úřady by měly při poskytování informací vycházet z rozsahu údajů, které obsahuje hlasovací lístek. Podle ustanovení § 25 odst. 3 zákona o volbách do zastupitelstev hlasovací lístek obsahuje následující údaje kandidáta: Jméno, příjmení, věk, část obce či obec, ve které je kandidát přihlášen k trvalému pobytu, a název politické strany nebo politického hnutí, jejímž členem kandidát je, případně údaj o tom, že je bez politické příslušnosti.

Před zveřejněním rozhodnutí o registraci kandidátní listiny se žadatelé mohou obracet s žádostmi o informace přímo na politické strany a samotné kandidáty. Registrační úřady, jak výše uvádíme, mohou v této době poskytovat informace pouze na základě souhlasu uděleného jim samotným kandidátem a v rozsahu, ke kterému byl souhlas kandidátem dán. Souhlas však musí splňovat veškeré náležitosti stanovené zákonem o ochraně osobních údajů a registrační úřad je jako správce osobních údajů povinen splnit i další ustanovení, která zákon o ochraně osobních údajů správci osobních údajů ukládá.

Závěr :

Ustanovení výše uvedených právních předpisů znamenají, že informace o kandidátech lze poskytovat až po rozhodnutí o registraci kandidátní listiny a po zveřejnění tohoto rozhodnutí v souladu se zvláštní právní úpravou, tj. zákonem o volbách do zastupitelstev obcí.

Poznámka: Výše uvedený dokument je dostupný na internetové adrese Úřadu http://www.uoou.cz/index.php?l=cz&m=top&mid=02:01&u1=&u2=&t= .

Stanovisko č. 7/2006

říjen 2006

Dozorové pravomoci Úřadu pro ochranu osobních údajů v souvislosti s výkonem advokacie

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 či zákon) je již sedmým rokem součástí našeho právního řádu jako komplexní a univerzální norma upravující institut ochrany osobních údajů a současně i výkon státní správy v této oblasti. Působnost zákona je vymezena zejména prostřednictvím ustanovení v § 3 tak, aby zákon dopadal na jakékoliv zpracování osobních údajů. V souvislosti s výkonem advokacie se však opakovaně objevují názory a vyjádření, popírající dopad zákona na tuto oblast včetně pravomoci Úřadu pro ochranu osobních údajů (dále jen „Úřad“) vykonávat dozor nad zpracováním osobních údajů v rámci advokacie. Úřad proto zpracoval přístupové stanovisko, které by mělo přispět k objasnění a pochopení hlavních aspektů této problematiky a zejména by mělo zabránit vzniku jiných názorů týkajících se činnosti podobného charakteru (například činnost notářů, exekutorů apod.), a které nyní předkládá veřejnosti.

Zákon o ochraně osobních údajů žádnou speciální výjimku ve vztahu k výkonu advokacie nezakotvuje. Naopak lze konstatovat, že na exempce ze své působnosti je značně skoupý; vyjma zpravodajských služeb, které však mají pouze výjimku z dozorové působnosti Úřadu, nikoli z působnosti zákona jako takového, neexistuje žádná ucelená oblast či obor, ve kterém by neměl být zákon o ochraně osobních údajů uplatňován. Možné výjimky se týkají pouze jednotlivých zákonných povinností správců nebo zpracovatelů a platí pouze pro oblasti taxativně vyjmenované zejména v ustanovení § 3 odst. 6 zákona (bezpečnost a obrana České republiky, veřejný pořádek, vnitřní bezpečnost a další). Komplexní a universální dopad zákonné úpravy však není ryze českým specifikem; shodné principy vyplývají i z Úmluvy č. 108 Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních dat a směrnice 95/46/ES Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů , které byly východiskem národní úpravy. Vzhledem k tomu, že ochrana osobních údajů se stala již dlouho před přijetím zákona v České republice fenoménem mezinárodním a zejména evropským a jeho odpovídající vnitrostátní úprava včetně podmínek vymahatelnosti byla také v oblasti harmonizace právního řádu předpokladem přistoupení České republiky k Evropské unii, je *apriori* nemožné, aby se pouze, či speciálně v advokacii, neuplatňovaly podmínky a principy ochrany osobních údajů a aby fyzická osoba – subjekt údajů požívající obecně určitého standardu práv – jich pozbyl či se jich nemohl domoci při kontaktu s činností advokáta. Současně ani zákon č. 85/1996 Sb., o advokacii, ve znění pozdějších předpisů (dále jen zákon o advokacii), neobsahuje žádnou ucelenou úpravu ochrany osobních údajů, kterou by bylo možno považovat za *lex specialis* vylučující aplikaci obecné úpravy zákona o ochraně osobních údajů.

Argumentace popírání dopadu zákona o ochraně osobních údajů a dozorové pravomoci Úřadu na zpracování osobních údajů při výkonu advokacie se soustřeďuje na dva okruhy námitek. Prvním z nich je názor, že při výkonu advokacie nedochází ke zpracování osobních údajů ve smyslu zákona, tzn. systematické činnosti, jak vymezuje obsah tohoto pojmu ustanovení § 4 písm. e) zákona; podle těchto námitek jde v případě výkonu advokacie jen – pokud vůbec advokát s osobními údaji přichází do styku – o nahodilé shromažďování informací ve smyslu ustanovení § 3 odst. 4 zákona, tedy jde o činnost, na kterou se tento zákon nevztahuje. Druhým okruhem námitek je princip povinné mlčenlivosti advokáta, který by dle námitek byl nezákonně narušen připuštěním možné aplikace zákona o ochraně osobních údajů na činnost advokáta, zejména zřejmě v souvislosti s dozorovými a kontrolními pravomocemi Úřadu.

K názoru, že při výkonu advokacie nedochází ke zpracování osobních údajů, tzn. systematické činnosti, je třeba konstatovat, že podle dosavadních zkušeností Úřadu není vždy nutné, aby systematické shromažďování osobních údajů bylo samotným cílem dané aktivity (hlavní činností) správce nebo zpracovatele. I když advokát přichází často k osobním údajům klienta a případně údajům třetích osob bez jakéhokoliv systému, nebo je do systému nezařazuje, nevkládá je do žádného speciálního archivu apod., půjde o systematické zpracování již za situace, stanou-li se osobní data součástí nebo obsahem dokumentu, který je uchováván v rámci klientského spisu nebo jakékoliv jiné evidence či datového souboru (vedeného jak v listinné podobě, tak i např. za použití technických prostředků), neboť jde o postup nebo operace, které jsou ve smyslu ust. § 4 písm. e) zákona považovány za systematické uchovávání dat. Přitom prvek systematičnosti je dán už tím, že každá z fází (operací) je správcem nebo zpracovatelem prováděna s určitým záměrem. Samo rozhodnutí advokáta o uchování konkrétního údaje či údajů pro další průběh poskytované právní služby nebo provedení jiné operace, kdy bývají jednotlivé, klientem sdělené či jinak získané osobní údaje zřejmě tříděny, možná kombinovány, upravovány či pozměněny a pravděpodobně budou někdy použity nebo i zpřístupněny (např. uvedením v soudním či jiném řízení), je velmi významnou součástí jeho práce; to vše zákon označuje za jednotlivé formy zpracování, přičemž postačí, je-li dána i jen jedna z nich /ustanovení § 4 písm. e) však není taxativním výčtem/. Opominout nelze ani druhou část ustanovení § 3 odst. 4 zákona o ochraně osobních údajů, a to podmínku, že údaje nesmějí být dále zpracovávány. Definici zpracování přitom naplňuje již i pouhá pracovní složka s úvodní informací klienta o požadované právní službě či databáze klientů advokátní kanceláře.

Podle názoru Úřadu také sám zákon o advokacii prostřednictvím ustanovení § 1 odst. 2 zákona o advokacii, kde je definováno poskytování právních služeb, se k tomuto možnému problému vyslovuje tím, že jedním ze základních znaků výkonu právní služby je skutečnost, že právní služby jsou poskytovány soustavně, tedy jako výkon samostatné činnosti, resp. profese. Soustavný výkon činnosti, která s sebou nutně nese zpracování osobních údajů, tak zcela jednoznačně vylučuje nahodilost při shromažďování osobních údajů, i když existenci nahodilého

shromáždění osobních údajů není možné zcela z činnosti advokáta vyloučit, stejně tak jako z činnosti každého dalšího subjektu. Výkon advokacie tedy s sebou *apriori* nese (jako *conditio sine qua non*) zpracování osobních údajů nejen klientů, ale i třetích osob.

Systematičnost do nakládání s osobními údaji u advokáta tedy vnáší již samotné zahájení poskytování právních služeb, jehož nedílnou součástí je vedení spisové a jiné dokumentace, která nutně obsahuje osobní údaje ve smyslu jejich zákonné definice zakotvené v ustanovení § 4 písm. a) zákona. Vedení přiměřené dokumentace je také zákonnou povinností advokáta, uloženou ustanovením § 25 zákona o advokacii a specifikované ve stavovských předpisech. Vedle toho všechny pojmové znaky stanovené zákonem o ochraně osobních údajů naplňuje činnost advokáta dle ustanovení § 25a zákona o advokacii. Kniha o prohlášeních o pravosti podpisu je pak dalším příkladem zpracování, které advokátu výslovně ukládá zákon. Systematický charakter operací s osobními údaji tedy nevylučuje *apriori* ani skutečnost, že advokát s nimi nakládá podle pokynu klienta. Je tedy nutné zcela popřít výklad, že nahodilé shromažďování je takové shromažďování, kdy popud nevzniká u správce dat (v tomto případě advokáta), ale objeví se neplánovaně, nepředvídatelně, nikoliv na základě volního rozhodnutí advokáta, ale klienta.

Druhým argumentem zpochybňujícím dozorovou pravomoc Úřadu při zpracování osobních údajů při výkonu advokacie je princip povinné mlčenlivosti advokáta. Povinnost mlčenlivosti, uložená ust. § 21 zákona o advokacii, je představiteli profesní skupiny chápána velice ortodoxně. Dle názoru České advokátní komory působí povinnost mlčenlivosti vůči každému, pokud nedojde ke zproštění ze strany klienta; nakládání s osobními údaji klienta se může proto uskutečňovat jen na základě dohody s ním a nemůže být regulováno žádnými právními ani jinými předpisy. Rovněž se dovozuje, že „žádný právní předpis nemůže být interpretován tak, aby toto právo sebemenším způsobem omezoval. To může být omezeno pouze zákonem o advokacii, jak se také výslovně děje v ust. § 21 odst. 2, kde je tato povinnost redukována v případě zvláštních předpisů o správě daní a poplatků.“ Úřad pro ochranu osobních údajů však zastává názor, že rozhodně není nutné, aby všechna přípustná omezení povinnosti mlčenlivosti stanovoval pouze zákon o advokacii; tak tomu ostatně není ani v dalších oblastech, na které dopadá minimálně stejně přísná povinnost mlčenlivosti (např. lékařské, bankovní, poštovní či listovní tajemství a mnohé další). K výkonu kontroly u advokáta proto Úřad považuje za zcela postačující oprávnění, které mu dává zákon o ochraně osobních údajů v ustanovení § 37 písm. c), které zní: Kontrolující jsou při provádění kontroly oprávněni seznamovat se s utajovanými informacemi za podmínek stanovených zvláštním právním předpisem, jakož i dalšími skutečnostmi, které jsou chráněny povinností mlčenlivosti.

Negativní přístup představitelů advokacie je zřejmě důsledkem nedocenění podstaty ochrany osobních údajů a z toho vyplývající domněnky, že inspektor Úřadu může při své kontrolní činnosti nějakým způsobem advokátní povinnost mlčenlivosti narušit. Již ze samotného pojmu však vyplývá, že cílem práce inspektora je naopak ochrana údajů. Úřad tedy sleduje shodný cíl jako povinnost mlčenlivosti, avšak v mnohem širším rozsahu. Hovoříme-li o fyzických osobách (právnickými osobami se Úřad nezabývá, neboť u nich nejde o osobní údaje), pak Úřadu přísluší dohlížet nejen na to, zda údaje klienta nejsou neoprávněně zpřístupňovány, jak koresponduje povinnosti mlčenlivosti, ale dohlíží také na dodržování řady dalších práv klienta souvisejících s údaji, o nichž se advokát dozvěděl. Nadto Úřad sleduje dodržování těchto práv nejen u klientů advokáta, ale i u dalších fyzických osob, subjektů údajů, s jejichž osobními daty advokát v průběhu případu (někdy ovšem i mimo něj) operuje, a kdy advokát sám je vázán povinností mlčenlivosti pouze ohledně osobních údajů samotného klienta. A konečně Úřad musí zajímat i možné neoprávněné zpřístupnění osobních údajů ze strany samotného advokáta. Současně je na místě připomenout, že inspektoři a další zaměstnanci Úřadu jsou taktéž vázáni přísnou povinností mlčenlivosti v souvislosti se svou činností. Dle ustanovení § 38 odst. 5 písm. b) zákona o ochraně osobních údajů jsou kontrolující povinni zachovávat mlčenlivost o skutečnostech zjištěných při výkonu kontroly a nezneužít znalosti těchto skutečností. Tato povinnost trvá i po skončení pracovněprávního vztahu k Úřadu. Argument vyloučení dopadu zákona na oblast advokacie z důvodu vázanosti advokáta povinností mlčenlivosti nelze tedy přijmout.

Advokát je ve většině případů při výkonu své praxe v postavení správce osobních údajů ve smyslu ustanovení § 4 písm. j) zákona o ochraně osobních údajů, tedy jako subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Je zde však také možnost, že se advokát, který zpracovává osobní údaje podle míry odpovědnosti a nastavení smluvního vztahu s klientem, ocitne v postavení zpracovatele ve smyslu § 4 písm. k) zákona o ochraně osobních údajů. Vzhledem k ustanovení § 7 zákona o ochraně osobních údajů, který uvádí, že povinnosti stanovené správci v § 5 platí obdobně také pro zpracovatele, není v zásadě rozhodné, zda bude v tom kterém konkrétním případě advokát v postavení správce, nebo zpracovatele. Na advokáty tedy dopadají zákonem předvídané povinnosti; je však nutno konstatovat, že pro některé z nich obsahuje zákon o advokacii či stavovské předpisy jejich zvláštní úpravu.

Týká se to například ustanovení § 5 odst. 1 písm. a) zákona, dle kterého je správce povinen stanovit účel zpracování. Ten je ovšem vymezen především účelem samotného zákona o advokacii, který dle svého ustanovení § 1 upravuje předmět, tedy poskytování právních služeb advokáty a charakterizuje rovněž, co se poskytováním právních služeb rozumí. Touto definicí je zároveň nutno považovat zčásti za stanovené také prostředky a způsob zpracování ve smyslu ustanovení § 5 odst. 1 písm. b) zákona.

Obzvlášť pečlivě musí advokát postupovat s ohledem na dopad ustanovení § 5 odst. 1 písm. c), tedy na povinnost zpracovat pouze přesné údaje, které získal v souladu se zákonem. Zvláštní úprava ji ovlivní pouze částečně; advokát sice dle čl. 6 odst. 3 etického kodexu může pravdivost skutkových informací (tedy i takových, které jsou zároveň osobními údaji) ověřovat jen se souhlasem klienta, současně však dle čl. 17 odst. 2 téhož stavovského předpisu nesmí v řízení uvádět údaje, o nichž ví, že jsou nepravdivé nebo klamavé. Je tedy mj. nutno rozlišovat mezi shromažďováním a dalšími formami zpracování těchto údajů.

Na výkon advokacie dopadají ustanovení § 5 odst. 1 písm. d) a e) zákona, i když např. určení rozsahu údajů nezbytných pro naplnění účelu bude vyplývat vždy ze svrchovaného individuál-

ního posouzení samotným advokátem. Je možné, že kontrola dodržení tohoto ustanovení je zde vzhledem k charakteru poskytované služby poněkud omezena. V případě, že se klient se svou stížností obrátí na Úřad, a ten zahájí prověření stížnosti, by bylo zřejmě nutné využít pro odborné posouzení tohoto problému stavovské orgány.

Na rozdíl od mnoha jiných profesí nestíhá advokáta povinnost získat souhlas subjektu údajů ve smyslu ustanovení § 5 odst. 2 zákona, a to ani ohledně svého klienta, ani při zpracování osobních údajů třetích osob, neboť bude naplněna hypotéza ust. § 5 odst. 2 písm. a) a b); shromáždění či využití osobních údajů klienta, který je smluvní stranou, bude nezbytné pro poskytnutí kvalitní právní služby, což je právní povinnost advokáta. Řadu zvláštních úprav lze v zákoně o advokacii či stavovských předpisech vyčíst i k povinnostem predikovaným ustanovením § 5 odst. 1 zákona o ochraně osobních údajů[1)]. Jejich rozbor však již přesahuje účel tohoto stanoviska. Podobný přístup lze aplikovat také na dodržení povinností správce nebo zpracovatele podle § 11 a 12 zákona, kdy advokát má plnit informační povinnost vůči subjektu údajů za situace, kdy zpracovává jeho osobní údaje. Tuto povinnost opět uznává zákon jako povinnost vůči osobě, od které jsou její osobní údaje přímo shromažďovány (§ 11 odst. 1 a 2) na rozdíl od povinnosti nebo výjimky z této povinnosti za situace, kdy jsou osobní údaje shromážděny z jiného pramene nebo zdroje (§ 11 odst. 3 a 4).

Další povinností dopadající i na oblast advokacie představuje například ustanovení § 13 týkající se zabezpečení osobních údajů před neoprávněným či nahodilým přístupem, změnou, zničením, ztrátou, neoprávněnými přenosy či jiným neoprávněným zpracováním či zneužitím. Nebo § 18 odst. 1, obsahující výjimku pro oznámení zpracování osobních údajů advokátem pro poskytování právních služeb klientům, tedy výjimku obsaženou v § 18 odst. 1 písm. b).

Závěrem lze konstatovat, že dodržování povinností týkajících se ochrany osobních údajů při jejich zpracování v souvislosti s výkonem advokacie a jejich možná kontrola ze strany Úřadu neznamená žádnou újmu či riziko pro práva a ochranu klienta, ale právě naopak může přispět k jejich důslednějšímu prosazování. Pokud jde o práva třetí osoby, je role Úřadu, zejména při vyřizování stížností na porušení zásad ochrany osobních údajů, zcela nezastupitelná.

1) *Např. čl. 17 etického kodexu, čl. 3 Usnesení představenstva ČAK č. 9/99, kterým se stanoví některé podrobnosti o dokumentaci advokáta vedené při poskytování právních služeb.*

Poznámka: Výše uvedený dokument je dostupný na internetové adrese Úřadu http://www.uoou.cz/index.php?l=cz&m=top&mid=02:01&u1=&u2=&t= .

Stanovisko č. 8/2006

říjen 2006

K využívání elektronických karet

Poslední dobou se v různých institucích a v mnoha oblastech běžného života rozšířilo vydávání elektronických (čipových) karet, které např. umožňují uplatňovat slevy, vstupy do budov, či využívání různých služeb. Při výrobě těchto karet dochází téměř ve všech případech ke shromažďování osobních údajů. V souvislosti s touto skutečností se Úřad pro ochranu osobních údajů rozhodl vydat následující stanovisko, které vyjadřuje základní postoj Úřadu k této problematice.

V současné době je vydáváno několik typů elektronických karet. Nejjednodušší je tzv. „bílá“ čipová karta, která často bývá nesprávně označovaná jako anonymní. Její anonymita spočívá v tom, že na kartě nejsou viditelně uvedeny identifikační údaje držitele karty (např. jméno, příjmení, fotografie). Z pohledu zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „zákon o ochraně osobních údajů“), by o anonymitě držitele karty bylo možné hovořit jen v případě, že by karta pouze umožňovala jejímu nositeli vstup do budovy, přístup do informačního systému (popř. využití nějaké služby), aniž by při jejím použití byl majitel jednoznačně identifikován. Systém by neidentifikoval držitele, ale pouze úroveň přístupových práv, které karta svému držiteli umožňuje, tedy v souvislosti s užíváním karty by nebyly zpracovávány žádné osobní údaje ve smyslu § 4 písm. a) a e) zákona o ochraně osobních údajů. Většina těchto „bílých“ karet je však personalizovaná. Znamená to, že umožňuje využívání specifických služeb jen konkrétnímu uživateli, např. vydávání obědů, zpětnou kontrolu oprávněnosti vstupu apod. Systém je pak schopen sledovat činnosti držitele „bílé“ karty stejným způsobem, jako činnosti majitele jakékoli jiné karty. V takovém případě je tedy nepochybně naplněno ustanovení § 4 písm. e), podle něhož se zpracováním osobních údajů rozumí jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky, a dochází tak ke zpracování osobních údajů.

Dalším typem jsou jednoúčelové personalizované karty, jako jsou např. zákaznické, benefitní nebo předplatní. Při vydávání těchto karet rovněž dochází ke zpracování osobních údajů, neboť tyto karty jsou vázány na konkrétního uživatele, který je na kartě jednoznačně identifikován – většinou pomocí jména, příjmení, popř. fotografie.

Posledním, v současnosti nejužívanějším typem elektronických karet, jsou multifunkční karty, jež umožňují využívat více druhů služeb, poskytovaných různými subjekty.

V souvislosti se zpracováním osobních údajů v rámci poskytovaného produktu (služby), představuje karta vnější prostředek vzhledem k různě definovaných účelům. Podstatné je zpracování (databáze) osobních údajů, v souvislosti s nímž je karta vydána, a především účel tohoto zpracování, tedy nikoli karta sama. Ve většině případů jsou karty nástrojem sloužícím k provedení

služby, tedy nástrojem zvoleným pro účely plnění smlouvy (smlouva o poskytnutí služby), která je uzavírána mezi poskytovatelem služby a subjektem údajů. Vydání karty a zpracovávání osobních údajů je tak výrazem smluvního vztahu uzavíraného z iniciativy subjektu údajů (podání žádosti o vydání karty), který spadá do výjimky § 5 odst. 2 písm. b) zákona o ochraně osobních údajů. Podle něj může správce osobní údaje zpracovávat bez souhlasu subjektu údajů, jestliže je zpracování nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro jednání o uzavření či o změně smlouvy uskutečněné na návrh subjektu údajů. Jedná se o akceptaci nabídky produktu se stanovenými parametry.

Existuje-li alternativní možnost, tedy možnost produkt využívat i bez čipové karty, zpracování osobních údajů je možné bez formálního souhlasu subjektu údajů, neboť výběrem produktu tak zákazník přistupuje na podmínky poskytovatele služby. V případě, že poskytování produktu je striktně vázáno na podmínku pořízení karty, je nutné rozlišovat zpracování osobních údajů pro různé účely.

Pro zpracování údajů nezbytně nutných pro vydání karty a pro plnění smlouvy platí výše uvedené, tedy možnost zpracování bez souhlasu. Pro zpracování údajů, které jde nad rámec nezbytnosti zpracování pro plnění smlouvy (zaznamenávání informací typu odkud a kam subjekt údajů cestuje, v kolik hodin chodí na obědy atd.), je, podle názoru Úřadu pro ochranu osobních údajů, třeba souhlasu subjektu údajů. Avšak i v případě získání souhlasu je nutné respektovat zásadu ochrany soukromí a osobního života, která stanoví hranici rozsahu zpracovávaných osobních údajů.

Vzhledem ke skutečnosti, že nabízený produkt (službu) lze využít pouze s kartou a bude-li rozsah zpracovávaných údajů zcela zjevně nepřiměřený stanovenému účelu, je možné zpochybnit svobodu poskytovaného souhlasu. A právě svoboda je podle § 4 písm. n) zákona o ochraně osobních údajů nezbytným atributem tohoto úkonu. Souhlas musí být také informovaný, jak ukládá § 5 odst. 4 zákona o ochraně osobních údajů, podle něhož musí být při udělení souhlasu subjekt údajů informován o tom, pro jaký účel zpracování a k jakým osobním údajům je souhlas dáván, jakému správci a na jaké období.

Informování subjektu údajů však není vázáno pouze na úkon souhlasu. Informování subjektu údajů je nutné i v případech, kdy zákon o ochraně osobních údajů umožňuje zpracování bez souhlasu. Tuto povinnost stanoví § 11 zákona o ochraně osobních údajů. Splnění informační povinnosti vůči subjektům údajů, uživatelům karet, pak nabývá na významu zvláště tam, kde dané prostředí prakticky „nutí“ fyzické osoby si kartu pořídit a využívat ji v rámci daného systému nebo komunity.

V souvislosti s vydáváním a následným využíváním karet dochází, nebo může docházet, v drtivé většině případů k vytváření rozsáhlé databáze. Ta může, kromě identifikačních údajů potřebných pro vydání karty, obsahovat i údaje o využívání jednotlivých služeb, jež karta poskytuje, a to prostřednictvím počítačových systémů zapojených do daného projektu. Systém je pak schopen uchovávat všechny informace o činnosti držitele karty, které tato technologie umožňuje; např. údaje o tom, kdy nebo jak často chodí majitel karty (žák nebo student) do školy, ve škole dále na obědy, jak často a jak dlouho se držitel karty pohybuje po určité budově (nejen školy, ale třeba i kolejní budovy, knihovny atd.) – systém tak umožňuje velmi průkaznou možnost evidence docházky apod.

Shromažďování osobních údajů, k němuž dochází v souvislosti s vydáváním karet, popřípadě shromažďováním dalších údajů, týkajících se využívání karty, a jejich následné další zpracování podléhá nepochybně režimu zákona o ochraně osobních údajů. Z toho důvodu je třeba věnovat pozornost následujícím okruhům problémů.

V prvé řadě je třeba vymezit základní vztahy při zpracování osobních údajů, tedy kdo je v daném případě správcem a kdo zpracovatelem ve smyslu § 4 písm. j) a k) zákona o ochraně osobních údajů. Tento krok bude komplikovanějším u „multifunkčních“ karet. Musí být jednoznačně určeno, zda je vydavatel karty správcem a majitelé jednotlivých aplikací nebo funkcí karty a počítačových systémů zapojených do daného projektu jsou zpracovatelé, nebo zda všichni účastníci budou ve vztahu správce – správce, tedy že jedna (multifunkční) karta bude mít z pohledu zákona o ochraně osobních údajů několik správců osobních údajů, zpracovávaných při využívání karty jejím držitelem.

Nastavení vzájemných vztahů mezi vydavatelem karty a dalšími účastníky je plně v jejich rukou, nelze proto předjímat, doporučovat či dokonce nařizovat, kdo bude v postavení správce, případně zpracovatele. Ve velké většině případů platí, že vydavatel karty je správcem. Jednotliví účastníci zapojení do systému mohou mít postavení zpracovatele, nebo také všichni účastníci budou ve vztahu správce – správce, popřípadě je možné, že vydavatel karty bude v postavení správce a zároveň i zpracovatele pro další subjekty – samostatné správce.

Pokud by se ve vztahu objevil zpracovatel, bylo by nutné uzavřít mezi správcem a zpracovatelem zpracovatelskou smlouvu podle § 6 zákona o ochraně osobních údajů, která musí být písemná a musí v ní být zejména výslovně uvedeno, v jakém rozsahu, za jakým účelem a na jakou dobu se uzavírá. Tato smlouva také musí obsahovat záruky zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů.

Musí být také zajištěno, aby osobní údaje, zpracovávané v rámci aplikací, byly chráněny tak, že k údajům z jednotlivých aplikací budou mít přístup pouze jejich správci, že každý správce bude mít přístup pouze do své aplikace. Je zcela nepřípustné, aby údaje byly přístupné v plném rozsahu všem správcům, jejichž aplikace se na kartě vyskytuje, či dokonce, aby údaje byly nějakým způsobem sdružovány. Nastavení přístupů vždy musí odpovídat nastavení vzájemných vztahů, a to tak, aby byla naplněna všechna ustanovení zákona o ochraně osobních údajů, v tomto případě především § 13. Správce, popřípadě zpracovatel, musí také zajistit, aby výrobce karty zlikvidoval po skončení prací veškeré poskytnuté údaje a zpracování tak ukončil.

Správné určení postavení jednotlivých účastníků projektu je východiskem pro plnění dalších povinností podle zákona o ochraně osobních údajů. Zpracování osobních údajů při vydávání karet ve většině případů podléhá oznamovací povinnosti podle § 16 zákona o ochraně osobních údajů, kterou je povinen splnit správce osobních údajů. Oznamovací povinnost nemusí správce plnit pouze v případě, že je možné na jím prováděné zpracování uplatnit některou z výjimek stanovenou § 18 odst. 1 zákona o ochraně osobních údajů (např. v případě, kdy zaměstnatel vydá kartu svým zaměstnancům za účelem kontroly docházky. Zaměstnavatel tak plní svou zákonnou

povinnost a karta je pouze zvoleným prostředkem zákonného zpracování).

Je tedy zjevné, že elektronické karty jsou ve většině případů pouze prostředkem nebo nástrojem pro zpracování osobních údajů, a to v souvislosti s poskytováním služeb. Jsou-li pak jakékoli osobní údaje v souvislosti s touto službou dále zpracovávány, musejí osoby, které tyto technické prostředky svým zákazníkům (klientům) nabízejí, mít na zřeteli, že se jedná o zpracování osobních údajů, které je zcela podřízeno režimu zákona o ochraně osobních údajů. Musejí si být také vědomy skutečnosti, že z toho pro ně vyplývají jejich povinnosti. V konkrétních případech se může jednat o získání souhlasu se zpracováním osobních údajů. Je třeba mít na paměti, že informační povinnost takové osoby postihuje v každém případě, a samozřejmě musejí být respektovány také další povinnosti vyplývající pro správce, resp. zpracovatele osobních údajů, a to zejména podle ustanovení § 5 odst. 1 a 2 zákona o ochraně osobních údajů.

Poznámka: Výše uvedený dokument je dostupný na internetové adrese Úřadu http://www.uoou.cz/index.php?l=cz&m=top&mid=02:01&u1=&u2=&t= .

III. SDĚLENÍ ÚŘADU

Registrační povinnost správce a připravované změny

Registrační povinnost je upravena § 16 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, podle něhož oznamovací povinnosti podléhá každé zpracování osobních údajů prováděné správcem, na které není možné aplikovat některou z výjimek z této povinnosti upravených v § 18 zákona. Je nutno zdůraznit, že povinností správce je zpracování (podléhající oznamovací povinnosti) oznámit Úřadu ještě před jeho samotným zahájením.

Dnem 27. listopadu 2006 došlo ke změně ve způsobu plnění oznamovací povinnosti správce. Úřad na základě zkušeností z předešlých let a za účelem vyšší efektivity práce v oblasti registrační činnosti přistoupil k zavedení elektronického způsobu přijímání registračních oznámení a k úpravě registračních formulářů. Nová podoba registračního formuláře především zahrnuje všechny informace důležité pro posouzení daného oznámení z hlediska rizik zamýšleného zpracování a tudíž lépe odpovídá potřebám Úřadu pro další výkon dozorové činnosti. Správcům by mělo zavedení elektronického formuláře přinést podstatné zjednodušení plnění registrační povinnosti.

Původní registrační formuláře, které byly k dispozici na vybraných finančních úřadech, byly staženy z oběhu. Správcům bude nadále k dispozici registrační formulář v elektronické podobě na webových stránkách Úřadu a bude tak umožněno podat registrační oznámení elektronicky prostřednictvím Internetu. Podrobné pokyny k vyplnění jsou součástí elektronického registračního formuláře.

Poznámka: Více informací je k dispozici na internetové adrese Úřadu http://www.uoou.cz/index.php?l=cz&m=left&mid=05&u1=&u2=&t= v rubrice Registr.

Závazná podniková pravidla (Binding Corporate Rules) jako nástroj bezpečného předávání osobních údajů do třetích zemí

V současném globalizovaném světě je mezinárodní předávání osobních údajů důležitou součástí fungování každé nadnárodní společnosti. Předávaní osobních údajů v rámci nadnárodních společností se stalo každodenní potřebou. Je v zájmu nejen podnikatelského sektoru, ale také dozorových úřadů, vytvořit fungující a životaschopný nástroj zajišťující dostatečnou ochranu osobních údajů při jejich zpracování a předání do třetích zemí. Takovým nástrojem mohou být i závazná podniková pravidla (tzv. Binding Corporate Rules – dále jen BCR).

Směrnice Evropského parlamentu a Rady 95/46/ES o ochraně jednotlivců v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen směrnice) v čl. 25 stanovila zásadu, že do třetích zemí mohou být osobní údaje předány pouze za předpokladu, že dotyčná třetí země zajistí odpovídající úroveň ochrany. V případě předání osobních údajů do třetí země, která nezajišťuje odpovídající úroveň ochrany, může být takové předání uskutečněno, pokud náležitá opatření směřující k ochraně osobních údajů poskytne sám správce. Jednou z možností, jak lze zajistit ochranu a legálnost zpracování a přenosu osobních údajů do třetích zemí je, v souladu s čl. 26 (2) směrnice, přijetí BCR.

V poslední době získává tento způsob zajištění legálnosti přenosu dat do třetích zemí ze strany nadnárodních společností stále více na oblibě. Zvláště velké nadnárodní společnosti tuto možnost vítají, neboť BCR pro ně představují nejschůdnější a nejlevnější cestu k legálnímu zpracování a přenosu dat v rámci celé společnosti. Podrobné informace o BCR poskytují doporučení Pracovní skupiny pro ochranu dat podle článku 29 (Working party 29), která jsou publikována v pracovních dokumentech WP 74, WP 107 a WP 108[1)]. Každá společnost, která se rozhodne vytvořit a následně předložit dozorovému úřadu ke schválení BCR, by se měla nejprve seznámit s těmito pracovními dokumenty a v dalším postupu z nich vycházet. Poskytují totiž návod, jakým způsobem dosáhnout toho, aby BCR mohly být skutečně považovány za nástroj poskytující dostatečná ochranná opatření. Obecně platí, že principy ochrany osobních údajů obsažené v BCR musejí být v souladu se základními principy zpracování osobních údajů, vyjádřenými ve směrnici a samozřejmě i s právními předpisy všech zemí EU, ve kterých má nadnárodní společnost své pobočky, poskytující osobní údaje k využití uvnitř společnosti. Výhodou BCR pro nadnárodní společnosti je skutečnost, že usnadňují vnitřní toky osobních údajů, obvykle buď zaměstnanců, nebo klientů, bez nadměrných rizik pro subjekty těchto údajů.

V této souvislosti je nutné zdůraznit, že BCR platí pouze pro přenos osobních údajů v rámci jedné nadnárodní společnosti, nikoli již pro předání mimo tuto společnost. Pro tyto

[1)] *Pracovní skupina pro ochranu jednotlivců s ohledem na zpracování osobních údajů (WP 29), je nezávislý poradní orgán Evropské komise sdružující zástupce národních dozorových orgánů jednotlivých členských států EU. Pracovní dokumenty WP 74 ze dne 3. června 2003, WP 107 a WP 108 ze dne 14. dubna 2005 jsou k dispozici na webových stránkách http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm .*

případy (tzv. „onward transfer“) je možné použít např. standardní smluvní doložky. Společnost, která se rozhodne zavést BCR, se mj. musí zavázat, že stanovená pravidla ochrany osobních údajů budou přijata v celé společnosti (tedy všemi organizačními složkami), a že bude zajištěno jejich dodržování prostřednictvím zavedených dozorových mechanismů. Skutečná závaznost tj. vymahatelnost přijatých principů, je jedním z hlavních závazků a zároveň „stavebním kamenem“ každých BCR.

Vytvoření a konečné schválení BCR je poměrně složitý a časově náročný proces. V rámci zemí EU je určen dozorový úřad, který je nejvhodnější autoritou pro předložení žádosti (většinou se jedná o dozorový úřad země, která je zároveň sídlem mateřské společnosti), a která následně koordinuje celý schvalovací proces. Žadatel, na základě jednání s odpovědným dozorovým úřadem (tzv. lead authority), vytvoří návrh BCR, který je zaslán k připomínkám dozorovým úřadům v EU působícím v zemích, z nichž jsou data předávána. Přijaté připomínky jsou předány zpět žadateli k vyjádření. Po vypořádání připomínek je připraven finální návrh, který je schválen relevantními dozorovými úřady.

Zavedení BCR do praxe by mělo vést k vytvoření komplexní ochrany soukromí v rámci nadnárodní společnosti, k vytvoření jakéhosi „bezpečného přístavu“ (obdoba tzv. „Safe Harbour“ pro předávání dat z EU společnostem v USA)[2)] uvnitř organizace umožňující volnou výměnu osobních údajů mezi jednotlivými pobočkami této společnosti, aniž by přitom bylo porušeno právo na ochranu soukromí a základní práva a svobody subjektů údajů. Zároveň je nutné, aby BCR byly „živé“, aplikovatelné pro každodenní obchodní praxi. Měly by zejména obsahovat praktické informace např. jakým způsobem jsou zaměstnanci informováni o závaznosti a nutnosti dodržovat přijatá pravidla (např. prostřednictvím speciálního vzdělávacího programu), jakým způsobem mohou subjekty údajů efektivně uplatňovat svá práva, jakým způsobem je kontrolováno dodržování závaznosti BCR v praxi (systém prováděných auditů) apod.

Dosavadní zkušenosti ze zemí EU hovoří ve prospěch zavádění BCR do praxe. Některé dozorové úřady (Nizozemí, Velká Británie, Španělsko) se velmi intenzivně věnují této problematice a v několika případech již přijaly roli tzv. vedoucí autority, která koordinuje celý schvalovací proces. Nejčastějším (nikoliv však jediným) kritériem pro přiznání úlohy vedoucí autority ostatními dozorovými orgány je umístění sídla nadnárodní společnosti v příslušném členském státě EU. Úřad zatím vystupoval pouze v roli připomínkového místa, kterému byly BCR předloženy ke schválení. Již nyní je možné předpokládat, že BCR bude postupně zavádět stále více společností a jejich význam a role v systému mezinárodního předávání bude narůstat.

---

2) *Rozhodnutí komise ze dne 26. července 2000 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně poskytované podle zásad „bezpečného přístavu“ a s tím souvisejících „často kladených otázek“ vydaných Ministerstvem obchodu Spojených států amerických - případy „Safe Harbour“. Rozhodnutí komise je k dispozici na webových stránkách Úřadu http://www.uoou.cz/rk_26-07-00.pdf .*

PRACOVNÍ SKUPINA PRO OCHRANU DAT PODLE ČLÁNKU 29

10107/05/CS
WP 105

Pracovní dokument o otázkách ochrany údajů, které souvisejí s technologií RFID

Přijato dne 19. ledna 2005

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

Sekretariát poskytuje Evropská komise, Generální ředitelství pro vnitřní trh, Ředitelství E (služby, autorské právo, průmyslové vlastnictví a ochrana dat), B-1049 Brusel, Belgie, kancelář č. C100-6/136.

Internetová stránka: www.europa.eu.int/comm/privacy

PRACOVNÍ SKUPINA PRO OCHRANU FYZICKÝCH OSOB PŘI ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

zřízená podle směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995[1)],s ohledem na článek 29, čl. 30 odst. 1 písm. c) a čl. 30 odst. 3 výše uvedené směrnice, s ohledem na svůj jednací řád a zejména na články 12 a 14 uvedeného jednacího řádu,

PŘIJALA TENTO PRACOVNÍ DOKUMENT:

1. Úvod

Používání radiofrekvenční identifikace (běžně známé jako „technologie RFID“) pro různé účely a aplikace může být přínosem pro podniky, fyzické osoby i veřejné služby (včetně orgánů státní správy). Jak dále dokládá tento dokument, RFID může pomáhat maloobchodníkům řídit jejich

---

1) *Úř. věst. L 281, 23.11.1995, s. 31, dostupné na adrese: http://europa.eu.int/comm/internal_market/privacy/law_fr.htm*

zásoby, zlepšovat zkušenosti spotřebitelů s nakupováním, zvyšovat bezpečnost u léků i umožňovat lepší kontrolní přístup osob do zakázaných oblastí.

I když se výhody spojené s používáním technologie RFID zdají být očividné, široké nasazení technologie s sebou nese potenciální úskalí. V oblasti ochrany údajů má pracovní skupina obavy ze skutečnosti, že některé způsoby používání technologie RFID mohou narušit lidskou důstojnost a porušovat práva na ochranu údajů. Obavy se týkají zejména možnosti podniků a orgánů státní správy využívat technologii RFID ke zjišťování údajů o soukromí fyzických osob. Příklady využívání technologie RFID, které vzbuzují obavy o soukromí, jsou schopnost tajně shromažďovat různé údaje, které se týkají téže osoby, sledovat osoby na veřejných prostranstvích (na letištích, železničních nádražích, v obchodech), zlepšovat profily sledováním chování spotřebitelů v prodejnách nebo číst údaje o oděvech, doplňcích a lécích, které zákazníci nesou. Problém zhoršuje skutečnost, že vzhledem k poměrně nízkým nákladům bude tato technologie dostupná nejen hlavním aktérům, ale také menším hráčům a jednotlivým občanům.

Vědomí tohoto nového rizika přimělo pracovní skupinu zabývat se důsledky technologie RFID pro právo na soukromí a další základní práva. Za tímto účelem pracovní skupina mj. konzultovala se zainteresovanými stranami, včetně výrobců a uživatelů technologie i obhájců soukromí. Výsledkem následné analýzy provedené pracovní skupinou je tento pracovní dokument, který má dva hlavní účely: Zaprvé je jeho cílem poskytnout uživatelům RFID návod k používání základních zásad stanovených ve směrnicích ES, zejména ve směrnici o ochraně údajů[2)] a ve směrnici o soukromí a elektronických komunikacích[3)], a zadruhé, pracovní skupina chce tímto pracovním dokumentem poskytnout výrobcům technologie (štítků, čteček a aplikací RFID) i orgánům pro normalizaci RFID pokyny k jejich povinnosti vytvořit technologii, která respektuje soukromí, aby uživatelé technologie mohli plnit své povinnosti podle směrnice o ochraně údajů.

S ohledem na poměrně malé zkušenosti s využíváním technologie RFID považuje pracovní skupina tento dokument za první hodnocení situace. Pracovní skupina se bude situací nadále zabývat, a až získá více zkušeností, poskytne další pokyny. To bude zvlášť nutné, jestliže se technologie RFID stane, jak se předpokládá, jedním z hlavních „základních kamenů“ budoucího „vyzvědačského“ prostředí. Shrneme-li to, jedná se o první dokument a pracovní skupina bude na této otázce dále pracovat.

2. Technologie radiofrekvenční identifikace: přehled technologie a jejího využívání[4)]

2.1. Základy technologie radiofrekvenční identifikace

Hlavními prvky technologie *nebo* infrastruktury radiofrekvenční identifikace jsou *štítek* (tj. mikročip) a *čtečka*. Štítek se skládá z elektronického obvodu, který uchovává data, a z antény, která sděluje data rádiovými vlnami. Čtečka má anténu a demodulátor, který převádí příchozí analogové informace z rádiového spojení do digitálních dat. Digitální informace pak může zpracovat počítač.

Jak vysvětluje další oddíl, může technologie RFID fungovat různými způsoby podle typu štítku a čtečky. Subjekty, které budou technologii využívat, si budou muset vybrat z různých technických možností podle svých potřeb. Budou se muset rozhodnout, zda budou používat aktivní, nebo pasivní štítky. „Pasivní“ štítky nemají vlastní zdroj energie (baterii), a proto zůstávají ve funkčním stavu i několik desítek let poté, co byly vyrobeny. Energii štítku dodává rádiový signál. Čtečka RFID vyšle rádiové signály, které probudí štítek v oblasti akčního rádiusu a přimějí jej zareagovat přenosem informací, které jsou na něm uloženy. „Aktivní“ štítky mají vlastní baterii, která snižuje jejich životnost. Buď vysílají své informace, aniž by byly dotázány čtečkou, nebo zůstávají v klidu, dokud je čtečka neaktivuje.

2.2. Různé využívání v mnoha odvětvích – příklady

Využívání technologie RFID začíná slavit úspěch v různých odvětvích (např. ve zdravotnictví, letectví, dopravě). Zvláštní *funkce*, které mohou štítky RFID v různých odvětvích plnit, se navíc také rozšiřují a tyto možnosti nejsou zdaleka vyčerpány. Cílem tohoto oddílu je názorně vysvětlit hlavní funkce, které může technologie RFID poskytovat v různých odvětvích nebo aplikacích, tj. v dopravě nebo ve zdravotnictví. Zatímco některé níže popsané aplikace RFID jsou stále ve zkušební fázi, jiné jsou skutečností, aniž by si toho subjekty údajů někdy byly vědomy.

Doprava/distribuce. Systémy RFID jsou velmi vhodné pro využití v dopravě. Jsou-li čtečky RFID vhodně rozmístěny, lze vozidla vybavená štítkem sledovat po celou cestu do místa určení. Na technologii RFID jsou již založeny mnohé jízdenky hromadné dopravy. Podle zdrojů z tohoto výrobního odvětví existují po celém světě milióny klíčků k automobilům, které obsahují RFID.

Letectví. Technologii RFID lze využít pro účely manipulace se zavazadly. Při odbavení jsou na zavazadla umístěny štítky a čtečky instalované v různých částech letišť sledují zavazadla při pohybu z jednoho letiště na druhé i na samotném letišti. Existují projekty na vybavení palubních lístků štítky, jež umožní vyhledání cestujících, kteří se zpozdí.

Zdravotnictví. Systémy RFID se využívají ve farmaceutickém průmyslu ke snadnější lokalizaci léků a jako opatření proti padělání a ztrátám způsobeným krádežemi během přepravy. Toho lze dosáhnout, jestliže výrobci vloží do každého léku štítek potvrzující jeho původ. Lékárníci nebo sklady, které léky prodávají, budou vybaveny čtečkami, jež ověří, že lék pochází od svého údajného výrobce. Americká agentura FDA (Food and Drug Administration – Úřad pro potraviny a léčiva) již vydala pokyny ke způsobu používání

---

2) *Směrnice 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) *Směrnice 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací.*

4) *Rozsáhlejší popis technologie RFID a způsobů použití, pro které je vhodná, je připojen jako příloha na konci tohoto dokumentu.*

RFID při balení léků za účelem lokalizace a ochrany proti padělání[5]. Také v nemocnicích, když se štítky připevňují k některým předmětům, zvyšuje RFID bezpečnost pacientů a úspory nemocnic, například odstraňuje riziko ponechání nástroje v pacientovi při ukončení operace. Štítky RFID lze také vybavovat samotné pacienty, za účelem ověřování jejich totožnosti, umístění a přesné procedury, kterou má nemocniční personál vykonat. Také je možné sledovat zaměstnance nemocnice, takže je lze snadno nalézt v naléhavých případech. Agentura FDA právě povolila aplikaci jedné společnosti (VeriChip) založenou na injekci/vsazení štítku RFID pod pokožku, což umožňuje nahlédnutí do zdravotní dokumentace pacienta v naléhavých případech[6].

Bezpečnost a kontrola přístupu. Pomocí systému RFID lze sledovat pohyb a používání cenných zařízení, jelikož štítky vysílají informace o svém umístění čtečkám v příslušném akčním rádiusu. Například v automobilovém průmyslu se RFID již používá jako prvek imobilizačních systémů pro automobily. Ve spotřebním a maloobchodním odvětví lze zvláštní štítky RFID používat k ověření původu zboží. Takto lze zboží s vysokou hodnotou zajistit proti padělání. Zabezpečení bankovek pomocí RFID je téma, které se zkoumá již několik let.

Podle práce v rámci ICAO[7] se bude RFID používat také v pasech[8]. Omezený přístup osob do určitých oblastí lze také kontrolovat připevněním štítku RFID na tyto osoby nebo vybavením těchto osob bezdotykovými čipovými kartami jako na Světové vrcholné schůzce o informační společnosti nebo na kongresu čínské komunistické strany.

Použití v maloobchodě. Několik největších maloobchodníků požádalo výrobce, aby své výrobky opatřili štítkem. Maloobchodník může využít výhod výrobků opatřených štítkem v různých souvislostech. RFID například zlepšuje funkce systému řízení skladu u maloobchodníků. Jelikož každý jednotlivý výrobek je identifikován v různých fázích (tj. po přivezení do prodejny, v regále, v okamžiku prodeje), poskytuje RFID maloobchodníkovi pružný nástroj pro manipulaci s výrobky a pro sledování jejich dostupnosti v prodejně a ve skladě. RFID má potenciál zlepšit účinnost skladového hospodářství, což prospěje maloobchodníkům a případně i spotřebitelům. Například instalace čteček v místech kontroly při odchodu, které umožňují vyhnout se fyzické kontrole, zkrátí čas, který musí spotřebitel v obchodě strávit. RFID může pomoci sledovat výrobky a umožnit účinnější stahování vadných nebo nebezpečných výrobků či výrobků, u nichž uplynula doba trvanlivosti.

V souvislosti s RFID v maloobchodním sektoru je důležité vzít v úvahu normalizační práci organizace EPC Global za účelem vytvoření „elektronických kódů produktů“, které identifikují jednotlivé položky[9].

3. Důsledky pro ochranu údajů a soukromí

I když některé typy použití RFID nemusejí vzbuzovat žádné obavy ohledně ochrany údajů, jak je doloženo níže, mnohé tyto obavy vzbuzují. Cílem tohoto oddílu je poskytnout přehled hlavních důsledků pro ochranu údajů, které vyplývají z různých možností využití technologie RFID.

3.1. Technologie RFID využívaná ke shromažďování informací souvisejících s osobními údaji

První obavy o ochranu údajů vznikají, když se technologie RFID používá ke shromažďování informací, které přímo, či nepřímo souvisejí s osobními údaji. Vezměme si třeba případ, kdy je číslo výrobku ze štítku RFID propojeno se záznamem o zákazníkovi, který tento výrobek koupil. Například sklad spotřební elektroniky může označovat své výrobky štítky s jedinečnými kódy produktů, které maloobchodník systematicky kombinuje se jmény zákazníků získanými při platbě kreditní kartou a později propojenými s databází zákazníků maloobchodníka. To lze činit mj. pro záruční účely. Jako další příklad si můžeme vzít případ, kdy supermarket opatřuje štítky věrnostní karty nebo podobná zařízení, která identifikují osoby podle jména, aby zjistil a zaznamenal návyky spotřebitelů, když jsou v prodejně, včetně doby strávené v určité části supermarketu, kolikrát spotřebitel supermarket navštíví, aniž by si něco koupil atd.

Ve výše uvedených případech, pokud se informace shromažďované prostřednictvím technologie RFID spojí s osobními údaji, jsou důsledky pro soukromí zjevné. Kromě toho, že technologie RFID zlepšuje stávající schopnost dozvědět se o návycích spotřebitelů a vytvářet individuální profily, což umožňují věrnostní karty, zvyšuje tato technologie potenciál pro přímý marketing používáním štítků s rozlišením na úrovni položek (item-level tagging), jelikož lze poznat fyzické osoby, jakmile vejdou do prodejny, a lze zde sledovat jejich chování. Široké využívání této technologie navíc způsobí prudký nárůst údajů (jejich typu i počtu), které bude zpracovávat velké množství správců, a to je důvod k obavám.

3.2. Technologie RFID používaná k uchovávání osobních údajů na každém štítku

Druhý typ důsledků pro soukromí představují případy, kdy jsou osobní údaje uchovávány na štítcích RFID. Jedním příkladem tohoto využití může být systém jízdenek. Vezměme v úvahu hypotetický případ, kdy se nějaká organizace rozhodne zavést bezdotykový systém jízdenek založený na technologii RFID u měsíčních jízdenek, kde budou jméno a kon-

---

[5] *Radiofrequency Identification Feasibility Studies and Pilot Programs for Drugs; Guidance for FDA Staff and Industry; Compliance Policy Guide (Studie proveditelnosti a pilotní programy radiofrekvenční identifikace léků; Pokyny pro zaměstnance FDA a pro výrobní odvětví; Pokyny k dodržování předpisů); oddíl 400.210; Radiofrequency Identification Feasibility Studies and Pilot Programs for Drugs; listopad 2004.*

[6] *Odbor zdravotních a lidských služeb; Úřad pro potraviny a léčiva; 21 CFR část 880; spis č. 2004N-0477]; zveřejněno ve Federálním rejstříku/svazek 69, č. 237/pátek, 10. prosince 2004/Rules and Regulations (Pravidla a předpisy).*

[7] *Mezinárodní organizace pro civilní letectví.*

[8] *V roce 2003 organizace ICAO specifikovala technické požadavky na technologii RFID používanou v elektronických pasech. Tyto specifikace byly zveřejněny v dokumentu ICAO Doc 9303.*

[9] *Pro další informace o EPC Global viz oddíl 5.2.*

taktní údaje držitele jízdenky vloženy do štítku. V důsledku toho by organizace stále věděla, kudy identifikovaná osoba cestuje. To má očividně dopad na soukromí osob. Kromě toho, že by tyto informace měla organizace, mohly by tytéž informace podloudně získat také třetí strany, protože přítomnost konkrétních štítků RFID může zachytit kdokoliv se standardní čtečkou. Nutno poznamenat, že systémy RFID velmi snadno podléhají napadení. Jelikož pracují mimo osu přímé viditelnosti a bezdotykově, může útočník pracovat na dálku a pasivní čtení nebude zaznamenáno.

3.3. Využití RFID ke sledování bez „tradičních" identifikátorů

Třetí typ důsledků pro ochranu údajů vyplývá z používání technologie RFID, které s sebou nese sledování fyzických osob a získávání přístupu k osobním údajům. Několik následujících příkladů ukazuje, jaký může mít technologie RFID dopad na soukromí fyzických osob.

Například existuje možnost, že řetězec prodejen s potravinami dá zákazníkům zařízení vybavená štítkem (např. žetony), která umožňují manipulaci s nákupními vozíky a která zákazníci používají při každé návštěvě. Tento mechanismus by obchodu umožnil vytvořit si soubor dat vztahujících se k identifikačnímu číslu uloženému v zařízení se štítkem a tak sledovat, které výrobky osoba (identifikovaná podle žetonu) kupuje, jak často se tyto výrobky používají a ve které prodejně tohoto řetězce je tento spotřebitel kupuje. Obchod by z toho mohl vyvodit příjem dané osoby, její zdravotní stav, životní styl, nákupní zvyky atd. Tyto informace by bylo možno využít k různému rozhodování, například pro marketingové účely, nebo dokonce pro dynamické stanovení cen. Jelikož zařízení by fyzickou osobu identifikovalo pokaždé, kdy by vešla do prodejny, mohly by být spotřebiteli nabízeny výrobky na základě zpracování zaznamenaných spotřebních návyků. Kromě toho, že by výše uvedené informace mohl shromažďovat obchod, mohla by je potenciálně získat také třetí strana. Takto by o uvedené identifikované osobě mohla být přijímána různá rozhodnutí bez jejího informovaného souhlasu. Podobně jako při využívání cookies v on-line prostředí, i když člověk není bezprostředně a přímo identifikován na úrovni informací o položce, lze jej identifikovat na asociativní úrovni díky možnosti bezproblémové identifikace prostřednictvím velkého množství informací, které se k němu vztahují nebo které jsou o něm uchovávány. Navíc údaje, které jsou o uvedené osobě shromážděny, mohou ovlivnit způsob, jak se s ní zachází nebo jak se hodnotí. Toto využívání RFID s sebou také nese závažné důsledky pro ochranu údajů.

Dalším příkladem by mohl být případ, kdy používání štítků RFID může vést ke zpracování osobních údajů, i když technologie RFID nevyužije další jednoznačné identifikátory. Vezměme v úvahu hypotézu, kdy osoba Z vejde do obchodu C s taškou s výrobky označenými štítky z obchodů A a B. Obchod C oskenuje její tašku a ukážou se výrobky v ní (spíše změť čísel). Obchod C si záznam s čísly ponechá. Když se osoba Z vrátí do obchodu druhý den, je opět oskenována. Dnes se ukáže výrobek Y, který byl naskenován včera – číslo patří hodinkám, které tato osoba stále nosí. Obchod C založí datový soubor s číslem výrobku Y jakožto s „klíčovou" informací. Tak lze sledovat, kdy osoba Z přichází do tohoto obchodu, pomocí čísla RFID na jejích hodinkách jakožto jejího referenčního čísla. To obchodu C umožňuje vytvořit profil osoby Z (jejíž jméno nezná) a sledovat, co má v nákupní tašce při dalších návštěvách obchodu C. Takto obchod C zpracovává osobní údaje a použije se zákon o ochraně osobních údajů.

Nakonec si vezměme příklad používání štítků na některých předmětech, které obsahují informace o povaze předmětu. Osobní věci jsou velmi intimní a obsahují informace, jejichž znalost třetími stranami by představovala vniknutí do soukromí osoby, která předmět vlastní. Tuto hypotézu dokládají následující příklady. Vezměme případ, kdy kdokoliv, kdo vlastní čtečku, může zachytit bankovky, knihy, léky nebo cennosti kolemjdoucích. Třetí strany, které tyto informace znají, takto vnikají do soukromí osoby, která předmět vlastní. Bylo by na váženou, kdyby teroristé dokázali v davu odhalit osoby určité národnosti. K ještě dramatičtějšímu vniknutí do soukromí by došlo, kdyby jak je popsáno výše, samotné zařízení obsahovalo důležité osobní informace, jako například informace týkající se pasu nebo informace, které jsou vysoce citlivé.

Tyto příklady vysvětlují některé hlavní obavy o ochranu údajů a o soukromí, které vznikají v souvislosti s používáním technologie RFID, vyplývají z tajného a nevyžádaného sledování fyzických osob v důsledku neoprávněného přístupu k informacím sdělovaným štítkem nebo k obsahu paměti na štítku.

Jak se uvádí v dalších oddílech, je důležité stanovit pokyny k používání základních zásad uvedených ve směrnicích ES, zejména ve směrnici o ochraně údajů, v souvislosti s výše uvedenými operacemi zpracování údajů.

4. Použití právních předpisů EU o ochraně dat na informace shromážděné prostřednictvím technologie RFID

4.1. Pokyny k používání směrnice o ochraně dat na shromažďování a další zpracování údajů prostřednictvím technologie RFID

Pokud jde o rozsah působnosti, platí směrnice o ochraně údajů pro zpracování všech osobních údajů. Podle směrnice jsou „osobní údaje" velmi široce vymezeny a zahrnují „*veškeré informace o identifikované nebo identifikovatelné osobě*". Lze se pak ptát, zda to znamená, že směrnice o ochraně údajů nutně platí pro shromažďování údajů prostřednictvím technologie RFID. Odpověď bude obecně záviset na konkrétním použití technologie RFID, zejména na tom, zda konkrétní použití RFID s sebou nese zpracování osobních údajů, jak je vymezeno obecnou směrnicí o ochraně údajů.

Při posuzování, zda se na shromažďování osobních údajů prostřednictvím konkrétního použití RFID vztahuje směrnice o ochraně údajů, musíme určit, a) v jakém rozsahu se zpracovávané údaje *týkají* fyzické osoby a b) zda se tyto údaje týkají fyzické osoby, která je *identifikovatelná*, nebo *identifikovaná*. Údaje se týkají osoby, jestliže odkazují na totožnost, vlastnosti nebo chování osoby nebo jestliže jsou tyto informace použity k určení nebo ovlivnění způsobu, jak se s uvedenou osobou zachází nebo jak se hodnotí. Při posuzování, zda se informace týkají identifikovatelné osoby, se musí použít 26.

bod odůvodnění směrnice o ochraně údajů, který stanoví, že „je třeba přihlédnout ke všem prostředkům, které mohou být rozumně použity jak správcem, tak jakoukoli jinou osobou pro identifikaci dané osoby".

I když je zřejmé, že ne každé shromažďování údajů prostřednictvím technologie RFID bude spadat do rozsahu působnosti směrnice o ochraně údajů, je také ve světle výše uvedeného zjevné, že bude existovat mnoho scénářů, kdy budou prostřednictvím technologie RFID shromažďovány osobní informace, na jejichž zpracování se vztahuje směrnice o ochraně údajů.

Subjekty, které uvažují o využívání informací shromážděných prostřednictvím technologie RFID, předtím budou muset provést hodnocení, aby určily, zda se tyto informace považují za „osobní údaje" v souladu se směrnicí o ochraně údajů. Jestliže informace RFID neobsahují osobní informace ani nejsou sdružovány s osobními údaji, jak je vymezeno výše, pak by se ustanovení směrnice o ochraně údajů nepoužila. Jestliže informace na štítku skutečně nejsou sdružovány s jiným identifikačním materiálem, například s něčí fotografií nebo jménem a adresou či se stálým referenčním číslem, pak se směrnice o ochraně údajů nepoužije.

Ve třech scénářích popsaných v oddíle 3 by se ustanovení směrnice o ochraně údajů použila. V prvním případě tomu tak je proto, že informace na úrovni položek shromážděné prostřednictvím technologie RFID jsou přímo spojovány s osobními údaji obsaženými na kreditní kartě nebo věrnostních kartách. Ve druhém scénáři se směrnice o ochraně údajů použije, jakmile jsou osobní informace jako například jméno vloženy na štítek RFID. A konečně využívání technologie RFID ke sledování pohybu osob, které jsou vzhledem k masivnímu shromažďování údajů, paměťové kapacitě a kapacitě zpracování počítačů ne-li identifikované, tak identifikovatelné, má také za následek použití směrnice o ochraně údajů.

4.2. Pokyny k dodržování požadavků na ochranu údajů

Správci údajů shromážděných prostřednictvím technologie RFID budou povinni dodržovat povinnosti směrnice o ochraně údajů (v tomto dokumentu se na ně často odkazuje jako na „uživatele technologie"). I když není možné stanovit, jak tyto požadavky platí v každém scénáři RFID, lze poskytnout určité obecné pokyny, které mohou správci údajů využít a přizpůsobit podle okolností zpracování údajů. Jak je dále popsáno v oddíle 5 níže, jsou výrobci přímo zodpovědní za zavedení takové technologie, která respektuje soukromí, která správcům údajů pomůže vykonávat jejich povinnosti v souladu se směrnicí o ochraně údajů a usnadní uplatňování práv jednotlivců.

Zásady:

Pracovní skupina by ráda zdůraznila, že rámec, který se použije na využívání technologie RFID i jakékoliv jiné technologie, je stanoven v 2. bodě odůvodnění směrnice o ochraně údajů, který říká, že „*systémy zpracování údajů slouží lidem; (…) musí bez ohledu na státní občanství nebo bydliště fyzických osob dodržovat základní svobody a práva těchto osob, zejména právo na soukromí, a přispívat k hospodářskému a sociálnímu pokroku, k rozvoji obchodu, jakož i dobrých životních podmínek jednotlivců*".

Zásady související s kvalitou údajů: Správci údajů, kteří shromažďují údaje v rámci využívání RFID, musejí dodržovat několik **zásad ochrany údajů**, včetně těchto:

Používat zásadu omezení účelu: Tato zásada, která je částečně obsažena v čl. 6 odst. 1 písm. b) směrnice o ochraně údajů, mj. zakazuje další zpracování, které je neslučitelné s účely shromažďování.

Zásada kvality údajů: Tato zásada ve směrnici vyžaduje, aby osobní údaje byly podstatné a v množství úměrném účelům, pro které jsou shromažďovány. Proto se nesmějí shromažďovat žádné nepodstatné údaje, a jestliže již byly shromážděny, musejí být vymazány (čl. 6 odst. 1 písm. c)). Vyžaduje také, aby údaje byly přesné a aktuální.

Zásada uchovávání: Tato zásada vyžaduje, aby osobní údaje nebyly uchovávány déle, než je nezbytné pro účel, pro který byly údaje shromážděny nebo dále zpracovány.

Zákonné důvody zpracování: Podle článku 7 směrnice o ochraně údajů mohou být osobní údaje zpracovány, pouze když toto zpracování vychází z jednoho z důvodů pro legitimní zpracování údajů[10].

Ve většině scénářů, kde se používá technologie RFID, bude jediným zákonným důvodem, jejž budou mít správci údajů k dispozici pro legitimní shromažďování informací prostřednictvím RFID, souhlas jednotlivých osob. Například supermarket, který opatřuje věrnostní karty štítky, bude potřebovat buď výslovná smluvní ustanovení nebo souhlas jednotlivce, aby mohl osobní informace získané v souvislosti se získáním věrnostní karty propojit s informacemi shromážděnými prostřednictvím technologie RFID. Avšak souhlas není vždy odpovídajícím zákonným důvodem pro legitimní zpracování osobních údajů shromážděných v kontextu systémů RFID. Například nemocnice, která používá RFID v chirurgických nástrojích, aby odstranila riziko ponechání nástroje v pacientovi při ukončení operace, nemusí potřebovat souhlas pacienta, pokud by toto zpracování mohlo být legitimní pro zachování životně důležitých zájmů subjektu údajů, což je další zákonný důvod uvedený v článku 7 směrnice o ochraně údajů[11].

Je-li použit souhlas, podle článku 2 a čl. 7 písm. a) směrnice musí splňovat určité požadavky. (i) Musí být udělen svobodně, tj. musí být udělen bez „uvádění v omyl a bez nátlaku". (ii) Musí být výslovný, jinými slovy, musí se týkat kon-

[10] *Článek 7 uvádí tyto zákonné důvody pro legitimní zpracování údajů: (i) subjekt údajů nezpochybnitelně udělil souhlas; (ii) zpracování je nezbytné pro splnění smlouvy, kde je subjekt údajů jednou ze stran, (iii) zpracování je nezbytné pro splnění právní povinnosti, které podléhá správce, (iv) zpracování je nezbytné pro zachování životně důležitých zájmů subjektu údajů, (v) zpracování je nezbytné pro vykonání úkolu ve veřejném zájmu, (vi) zpracování je nezbytné pro uskutečnění oprávněných zájmů odpovědné osoby za podmínky, že nepřevyšují zájem nebo základní práva a svobody subjektu údajů, zejména právo na ochranu soukromí jednotlivce.*

[11] *Pracovní skupina 29 upozorňuje, že vhodný zákonný důvod uvedený v článku 7 směrnice o ochraně údajů pro legitimní zpracování údajů bude v konečném důsledku záviset na konkrétních okolnostech tohoto zpracování.*

krétního účelu. (iii) Souhlas musí být vědomým projevem vůle. (iv) Souhlas musí být informovaný. A konečně, souhlas musí být „nezpochybnitelný“, což znamená, že souhlas, který může mít více než jeden význam, by se za souhlas nepovažoval.

Informační požadavky: Podle článku 10 směrnice o ochraně údajů musejí správci údajů, kteří zpracovávají informace prostřednictvím technologie RFID, poskytnout subjektům údajů tyto informace: totožnost správce, účely zpracování a mj. také informace o příjemcích údajů a o existenci práva na přístup[12]. V souladu s touto povinností v souvislosti se scénářem popsaným v oddíle 4 bude muset maloobchodní prodejna poskytnout subjektům údajů alespoň zřetelné oznámení o těchto skutečnostech:

(i) přítomnost štítků RFID na výrobcích nebo jejich obalech a přítomnost čteček;

(ii) důsledky této přítomnosti v souvislosti se shromažďováním informací; správci údajů by měli zejména velmi zřetelně informovat, že přítomnost těchto zařízení umožňuje štítkům vysílat informace, aniž by se na tom dotyčná osoba musela aktivně podílet;

(iii) účely, pro které mají být informace využity, včetně (a) typu údajů, s nimiž budou informace RFID propojeny, a (b) zda budou informace dostupné třetím stranám, a

(iv) totožnost správce.

Kromě toho v závislosti na konkrétním využití RFID bude správce údajů muset informovat také o tom: (v) jak vyřadit z provozu, deaktivovat nebo odstranit štítky z výrobků a zabránit tak tomu, aby sdělovaly další informace, a (vi) jak uplatňovat právo na přístup k informacím. Tyto informace budou například nutné ve scénářích popsaných v oddíle 3.1. I když oznámení jako ta, která EPC Global navrhuje umísťovat na spotřební výrobky, slouží k účelu poskytování informací popsaných výše v bodě (i), měla by být doplněna další dokumentací s informacemi uvedenými výše[13].

Zásada řádného zpracování uvedená v čl. 6 písm. a) směrnice o ochraně údajů vyžaduje, aby subjektu údajů byly informace poskytnuty zřetelně a srozumitelně.

A konečně, při poskytování výše uvedených informací považuje pracovní skupina za důležité zdůraznit, že by subjekt údajů měl být schopen pochopit důsledky použití RFID.

Právo subjektu údajů na přístup: Článek 12 směrnice o ochraně údajů subjektům údajů umožňuje ověřit přesnost údajů a zajistit, že jsou údaje aktualizovány. Tato práva se v plném rozsahu použijí na shromažďování osobních údajů prostřednictvím technologie RFID. Vrátíme-li se k příkladu supermarketu, který vybavuje štítky věrnostní karty, v rámci zajištění práva na přístup musejí být dotyčné osobě sděleny všechny informace, které se jí týkají, což může zahrnovat, kolikrát tato osoba vstoupila do obchodu, zakoupené položky atd.

Jestliže štítky RFID obsahují osobní informace popsané v oddíle 3.2, měli by lidé mít nárok znát informace obsažené na štítku a opravovat je pomocí snadno dostupných prostředků.

Povinnosti, které se týkají bezpečnosti zpracování: Článek 17 směrnice o ochraně údajů ukládá správcům údajů povinnost přijmout vhodná technická a organizační opatření na ochranu osobních údajů proti náhodnému nebo nedovolenému zničení nebo neoprávněnému sdělování. Opatření mohou být organizační nebo technická. Tento požadavek je rozpracován v oddíle 5 v rámci pojednání o RFID a nezbytném používání technologie, která zvyšuje ochranu soukromí.

5. Technické a organizační požadavky na zajištění přiměřeného provádění zásad ochrany údajů

Subjekty, které používají aplikace RFID, musejí nezbytně dodržovat výše uvedené zásady i zásadu minimalizace údajů uvedenou v čl. 6 odst. 1 směrnice o ochraně údajů.

Pracovní skupina se domnívá, že technologie může hrát klíčovou úlohu při zajištění dodržování zásad ochrany údajů v souvislosti se zpracováním osobních údajů shromážděných prostřednictvím technologie RFID. Například konstrukce štítků RFID, čteček RFID i aplikací RFID vedená normalizačními iniciativami může mít velký dopad na minimalizaci shromažďování a využívání osobních údajů i na předcházení nezákonným formám zpracování, bude-li přístup k osobním údajům pro neoprávněné osoby technicky nemožný.

V této souvislosti chce pracovní skupina zdůraznit, že i když jsou za osobní údaje shromážděné prostřednictvím dotyčné aplikace v konečném důsledku zodpovědní uživatelé aplikací RFID, jsou výrobci technologie RFID a normalizační orgány zodpovědné za zajištění toho, aby ti, kdo tuto technologii používají, měli k dispozici technologii RFID, jež dodržuje zásady ochrany údajů/soukromí. Měly by být vypracovány mechanismy, které zajistí, aby se tyto normy obecně dodržovaly v praktických aplikacích. Zejména musejí být dostupné normy pro dodržování soukromí technologiemi RFID, jež zajistí, že správci údajů, kteří zpracovávají osobní údaje prostřednictvím technologie RFID, mají potřebné nástroje pro provádění požadavků obsažených ve směrnici o ochraně údajů. Pracovní skupina proto naléhá na výrobce štítků, čteček a aplikací RFID i na normalizační orgány, aby následující doporučení vzali v úvahu.

5.1. Dopady normalizace a interoperability na provádění zásad ochrany údajů

Ať již uvažujeme o jakékoliv technologii, proces normalizace obvykle představuje hlavní hnací sílu pro interoperabilitu, která je důležitá pro úspěšné přijetí a zavedení nových technologií. Normalizace může také usnadnit přijetí požadavků na ochranu údajů a soukromí.

Všechny složky systému RFID podléhají nebo budou podléhat normě, například konstrukce štítku a čtečky, údaje uchovávané na štítku, komunikační protokol (rádiové rozhraní)

---

[11] *Informace o příjemcích údajů, zda jsou odpovědi na otázky povinné, o existenci práva na přístup k údajům a o právu na jejich opravu musí být poskytnuty v míře, v jaké jsou tyto doplňující informace nezbytné, s ohledem na zvláštní okolnosti, za jakých jsou údaje shromažďovány, aby tak bylo zajištěno řádné zpracování údajů vůči subjekt údajů.*

[12] *Pro přehled činností EPC Global viz oddíl 5.1.*

mezi čtečkou a štítkem, zpracování údajů shromážděných čtečkou atd. Normalizační orgány a jiné skupiny již vykonaly určitou práci v oblasti RFID. Nutno poznamenat, že normalizace RFID bude mít vliv na značný počet trhů, což ovlivní zejména obchod se zbožím.

Původně v reakci na krizi šílených krav vypracovala Mezinárodní organizace pro normalizaci (ISO) odvětvové normy (nákladní kontejnery, dopravní jednotky, zvířata atd…) pro štítky RFID a obecnější pro rádiové rozhraní (řada ISO 18000) a pro správu jednotlivých položek (ISO/IEC 15963:2004).

EPCglobal Inc[14], společný podnik organizací EAN International a Uniform Code Council (UCC), řídí rada guvernérů EPCglobal, která je složena z předních společností. Organizace pracuje na tvorbě „elektronických kódů produktů" (Electronic Product Codes – „EPC"), které identifikují jednotlivé položky. Každý výrobek bude vybaven štítkem s číslem výrobku. Předchůdcem tohoto systému je „univerzální kód výrobku" (Universal Product Code – „UPC") neboli systém čárových kódů, který hodlá EPC nahradit. Rozdíl mezi těmito dvěma systémy je, že UPC identifikuje typ výrobku, aniž by byla očíslovaná každá jednotlivá položka. Síť EPC Global navíc vytváří normy pro propojení serverů, které obsahují informace, jež souvisejí s položkami identifikovanými pomocí čísel EPC. Servery s názvem EPC Information Services neboli EPCIS jsou dostupné přes internet a propojené, autorizované a přístupné prostřednictvím souboru síťových služeb[15].

Ve většině normalizačních iniciativ RFID lze zahrnout do technických specifikací parametry na ochranu údajů. Nedávno bylo například navrženo[16] upravit normu pro protokol čtečka-štítek vypracovanou ISO tak, aby zahrnovala Zásady čestného zacházení s informacemi vypracované OECD[17].

Evropský institut pro normalizaci v telekomunikacích (ETSI) nedávno schválil novou evropskou normu pro používání systémů RFID, když zvýšil povolený výkon čteček a počty dostupných frekvencí v pásmu UKV, které je v maloobchodním odvětví pro identifikaci na úrovni položek nejslibnější. Tento vývoj zvýší zejména čtecí vzdálenost mezi čtečkou a štítkem[18].

Interoperabilita systémů RFID (hardware, programové vybavení a vyprodukovaná data) logicky vyplývá z procesu normalizace. Z podnikatelského hlediska je interoperabilita systémů RFID příznivá. U udržitelného podnikatelského modelu by maloobchodník opravdu neměl být nucen zavádět několik různých čteček štítků, aby mohl skenovat štítky vyrobené různými výrobci. Z hlediska ochrany údajů, i když interoperabilita může zvýšit technickou kvalitu údajů a přispět k dodržování čl. 6 odst. 1 písm. d) směrnice, může mít interoperabilita RFID zároveň určité nežádoucí vedlejší účinky pro ochranu údajů, pokud nebudou přijata vhodná opatření. Například může být obtížnější používat a kontrolovat zásadu omezení účelu. Navíc by mohla být kritičtější také správa přístupových práv s ohledem na soukromí, jelikož se zvýší počet aktérů, kteří budou s údaji manipulovat.

5.2. Technická a organizační opatření k informování o přítomnosti technologie RFID, rozpoznatelnosti a aktivovatelnosti

Jak upozorňuje oddíl 4, musejí uživatelé technologie RFID poskytnout subjektům údajů informace nejen o účelech zpracování údajů, ale *také* o přítomnosti zařízení RFID a rovněž musejí dodržovat tyto zásady:

Zaprvé, osoby musejí být informovány o přítomnosti čteček typu RFID nebo aktivovaných čteček RFID. K tomu jsou zjevně zapotřebí piktogramy (symbolické značky), které se stanou celosvětovou normou, i jiné informační prostředky pro tento účel. Poskytování tohoto typu informací je nezbytné, aby se předešlo neoprávněnému a tajnému shromažďování osobních údajů prostřednictvím technologie RFID. Má-li například prodejna nebo nemocnice aktivované čtečky, měli by o tom být lidé informováni.

Zadruhé ze stejných důvodů, jaké jsou uvedeny výše (předejít tajnému shromažďování osobních údajů), je dalším požadavkem identifikace *existence technologií RFID,* které jedince obklopují (například v oděvech a předmětech) vzhledem k jejich velikosti, díky níž mohou být téměř neviditelné. Metody splnění tohoto požadavku mohou mít různou podobu: Může se jednat o standardní upozornění, nebo upozornění pomocí technických prostředků.

Zatřetí, pouhé informování o přítomnosti RFID v praxi nebude stačit, informací, která musí být jednotlivým osobám poskytnuta a která vyplývá ze směrnice o ochraně údajů, je také aktivovatelnost nebo *aktivace RFID v reálném čase*. Jsou tedy také zapotřebí jednoduché techniky, které umožní vizuální označení stavu aktivace nebo aktivovatelnosti. Součástí snadno dostupných informací by měly být informace o přítomnosti a způsobu použití technologií PET (Privacy Enhancing Technologies, technologie na podoporu soukromí, např. dočasný deaktivátor, možnost štítek fyzicky odstranit atd.) a informace o organizačních opatřeních v daném prostředí.

Pracovní skupina zdůrazňuje, že je nezbytné, aby všechny strany prováděly další výzkum a vývoj těchto tří informačních témat.

5.3. Technická a organizační opatření pro uplatnění práv na přístup, opravu a výmaz

Jak bude ještě popsáno níže, konstrukčně-technologické řešení systému RFID může mít velký dopad na zajištění účin-

---

[14] *http://www.epcglobalinc.org/*

[15] *Dosud se obavy EU v těchto normalizačních iniciativách, jejichž účastníky jsou hlavně zainteresované strany z výrobních odvětví USA, vyskytovaly nedostatečně. Stále také není jisté, zda čínský trh přijme jednu z citovaných norem a nevypracuje normy vlastní.*

[16] *Christian Floerkemeier, Roland Schneider, Marc Langheinrich: Scanning with a Purpose - Supporting the Fair Information Principles in RFID protocols (Účelné skenování – podpora Zásad čestného zacházení s informacemi v protokolech RFID). 2. mezinárodní sympózium o všudypřítomných výpočetních systémech (ubiquitous computing systems – UCS 2004), 8. - 9. listopadu 2004, Tokio, Japonsko.*

[17] *ISO 18000 část 6 typ A*

[18] *Vzdálenost čtečky a její výkon může ovlivnit, do jaké míry daná aplikace RFID vniká do soukromí.*

ného provádění práv na přístup, opravu a výmaz uvedených v článku 12 směrnice o ochraně údajů.

a) Přístup k obsahu štítku [čl. 12 písm. a) směrnice o ochraně údajů]

Přístup k obsahu štítku RFID je technicky možný jen s použitím čtečky, která pracuje s protokolem štítku, a pomocí displeje pro jednotlivce. Ale u mnohých aplikací štítek obsahuje pouze identifikační číslo, k jehož sémantice lze přistupovat jen v prostředí úplné informační aplikace. Pokud víme, pouze malý počet štítků RFID nese sémantické informace (které popisují předmět, identifikátor správce údajů, účel shromažďování údajů atd.), což také představuje problém přístupu jednotlivce k obsahu.

Jednou možností, jak by tyto informace mohly být dostupné, je vymezit sémantické normy například pomocí XML. Ať už však tyto sémantické popisy budou mít jakoukoliv podobu, stále představují problém přístupu neoprávněnými třetími stranami (viz oddíl 3 výše).

b) Oprava obsahu [čl. 12 písm. b) směrnice o ochraně údajů]

Narozdíl od přístupu k obsahu oprava vyžaduje čtečku, která pracuje s protokolem štítku, a interaktivní informační systém, který jednotlivci umožní sledovat čtení i úpravy obsahu.

Jednou z navrhovaných možností je zabudovat do štítku prvek, který vymaže nebo zakóduje sériové číslo položky a ponechá úplně nebo částečně dostupný pouze popis typu zařazení položky (je to možné též naopak, ale s jinými důsledky pro soukromí).

c) Výmaz obsahu [čl. 12 písm. b) směrnice o ochraně údajů]

Zda by měly být zavedeny deaktivátory štítků, aby lidé mohli zastavit zpracování svých osobních údajů, když se štítek dostane do oblasti akčního rádiusu čtečky, záleží na zákonných důvodech pro legitimní zpracování osobních údajů. Toto zavedení by například nebylo přiměřené v případě štítků RFID zabudovaných v pasech, ale z pohledu ochrany údajů by bylo nutné u štítků RFID, kterými jsou opatřeny spotřební výrobky. Tato otázka byla zvažována na konferenci komisařů pro ochranu údajů a soukromí v Sydney, jak je doloženo v prohlášení o RFID ze Sydney[19].

V posledních několika letech byla zveřejněna různá navržená řešení. Jedním z přístupů bylo zavedení příkazu „vymazat". To znamená, že štítek může být trvale nebo dočasně deaktivován posláním příkazu „vymazat". Trvalou deaktivaci lze provést spálením tavné pojistky metodou „fuse effect", zakódováním paměti nebo odstraněním štítku. Dočasnou deaktivaci lze provést mechanicky nebo použitím softwarového zámku. Problémem u tohoto přístupu je, že dochází ke ztrátě výhody možnosti opětovného využití RFID mimo prodejnu. Proto byly navrženy jiné přístupy.

Variantní řešení spočívá v přepsání údajů uložených na štítku RFID nulami. Štítek stále zůstává aktivní, ale je-li dotázán, vrátí místo čísla pouze nuly. Tento systém RFID ve skutečnosti „nedeaktivuje". Štítek stále reaguje a předává informaci, že dotyčná osoba má věc opatřenou štítkem, což může mít tyto důsledky: Zaprvé, jelikož štítky RFID, které vracejí pouze nuly, nejsou příliš běžné, je pouhá existence tohoto štítku cennou informací. Ukazuje, že dotyčná osoba si koupila něco v prodejně, která položky opatřuje štítky. Dobře informovaná společnost může provést kvalifikovaný odhad. Zadruhé, zdá se, že nejdříve budou štítky RFID používány u cenných položek. Po několik let bude pouhá přítomnost štítku RFID (i když bude vracet nuly nebo nesrozumitelné údaje) pomáhat zlodějům vyhledávat věci ke krádeži ze šaten nebo garáží. A konečně, až bude štítků RFID více, nebudou asi obchody nadšeny ze štítků, které reagují načtečky, ale vracejí nepoužitelné údaje.

Dalším přístupem je fyzické odstínění štítku, které může uživatel vědomě použít. Například lze používat peněženky se stíněním, takže nebude možné zachytit bankovky opatřené štítkem. Také hliníková fólie zabudovaná do obalu pasu s RFID by mohla postačovat k ochraně jeho obsahu, pokud není pas otevřen. Stínění však není vhodné pro všechny aplikace. Například oděvy s připevněnými štítky nelze při nošení zabalit do stínicího materiálu. Navíc se zdá, že tento přístup klade nepřiměřenou zátěž na jednotlivce, na které se v konečném důsledku přenáší výhradní zodpovědnost za zabránění tomu, aby štítek sděloval informace.

Při vymezení toho, jak by deaktivátory štítků měly fungovat, by normalizační orgány, výrobci a uživatelé technologie RFID měli kromě výše uvedeného vzít v úvahu, že jednotlivci, kteří se rozhodnou pro odstranění štítku, by neměli být žádným způsobem vystaveni možnosti postihu.

Také zde pracovní skupina zdůrazňuje, že je neustále nutné, aby všechny strany prováděly další výzkum a vývoj těchto témat.

5.4. Zákonné důvody zpracování

Deaktivátory štítků: Kromě potřeby deaktivátorů štítků v kontextu oddílu 5.3 i jiná ustanovení směrnice o ochraně údajů vyžadují přítomnost této funkce (deaktivace štítku). Jestliže je podle směrnice o ochraně údajů jediným zákonným důvodem pro legitimní shromažďování osobních údajů prostřednictvím technologie RFID (viz oddíl 4.2) souhlas, mohou lidé svůj souhlas se zpracováním osobních údajů ve skutečnosti vždy odvolat (čl. 7 písm. a)). Nebude-li k dispozici žádné zařízení, které jedinci umožní štítek deaktivovat, osoba, která si již nepřeje, aby štítek o ní poskytoval informace, nebude moci toto právo uplatnit. Jestliže byly osobní údaje obsažené na štítcích RFID shromážděny na základě jiných zákonných důvodů, než je souhlas, není vždy nutné, aby tyto štítky měly deaktivační zařízení. Například osobní informace obsažené na štítcích používaných v souvislosti s prací pro účely sledování přístupu do práce nemusejí vyžadovat dostupné deaktivátory štítků, pokud má zpracování údajů základ v pracovněprávních vztazích.

[19] *Usnesení o radiofrekvenční identifikaci, 25. konference komisařů pro ochranu údajů a soukromí, Sydney 2003, http://www.privacyconference 2003. org, uvádí: „…jsou-li štítky RFID ve vlastnictví jednotlivců, měli by mít tito jednotlivci možnost vymazat údaje a štítky deaktivovat nebo zničit."*

U některých aplikací RFID, například když má jedinec právo odvolat svůj souhlas nebo vznést námitku proti zpracování (čl. 14 písm. a)) a následné právo štítek deaktivovat, by měli výrobci i uživatelé technologie RFID zajistit, aby tato operace deaktivování štítku byla snadno proveditelná. Jinými slovy, deaktivace štítku by pro subjekt údajů měla být snadná.

5.5. Zabezpečení údajů

Používání kódování na štítcích a aplikacích: Jestliže štítky RFID obsahují osobní údaje, musejí být podle článku 17 směrnice o ochraně údajů přijata technická opatření, která zabrání neoprávněnému přístupu k údajům. Pokud tato opatření nebudou provedena, mohl by kdokoliv s čtečkou štítek „probudit" a získat informace, které jsou na něm uložené. Tato opatření jsou podle čl. 6 odst. 1 písm. d) směrnice o ochraně údajů nutná také proto, aby se zajistila neporušenost údajů uchovávaných na štítku a zabránilo se tak neoprávněným změnám.

Typ technických prostředků bude záviset na povaze údajů. Jak je vysvětleno dále, tyto štítky by většinou mohly vystačit s *kódováním* údajů a ověřením čtečky, aby se zabránilo třetím stranám vybaveným čtečkou číst informace. Vezmeme-li si scénář, kdy štítky RFID obsahují totožnost pacienta, odpovědného lékaře a proceduru, kterou má nemocniční personál vykonat, je snadno pochopitelná povinnost nemocnice zajistit, aby tyto informace nebyly čitelné čtečkami třetích stran, což s sebou přináší nutnost použití technických opatření, jako je kódování, aby se tomu zabránilo.

Nejobecnějším a nejbezpečnějším přístupem je používání standardních ověřovacích protokolů (např. ISO/IEC 9798). Jejich používání je již rozšířené v sítích nebo u čipových karet. V těchto normalizovaných protokolech se používají šifrovací prvky. U symetrických ověřovacích metod, což znamená, že vysílač i příjemce mají stejný klíč, se používají autentizační kódy zpráv MAC nebo symetrické šifrovací algoritmy (např. DES, AES). U asymetrických metod, kde má každá strana soukromý a veřejný klíč, se využívají asymetrické šifrovací algoritmy (např. RSA, ECC) nebo podpisová schémata.

Některé šifrovací ověřovací metody se již provádějí u imobilizérů automobilů nebo u systémů kontroly přístupu, ale často využívají patentované algoritmy, protože většinou se snadněji zavádějí a jsou levnější než algoritmy standardní. Nicméně za účelem lepší bezpečnosti, která může být zapotřebí k ochraně citlivých údajů, by se měly zavést standardní algoritmy a protokoly. Výhodou těchto protokolů a algoritmů je, že se již široce používají. Byly tedy testovány a jsou vyzkoušeny v provozu mnoha různými stranami. Proto jsou nyní vesměs přijímány jako bezpečné.

Již existují publikace, které naznačují, že pro štítky RFID jsou vhodné symetrické algoritmy (jako AES)[20]. Problémem používání symetrických ověřovacích algoritmů je, že generování klíčů a správa klíčů je složitá věc. Asymetrické metody se tomuto problému vyhýbají, ale jsou dražší než metody symetrické.

6. Závěr

Vzhledem k rostoucímu používání technologie RFID pro různé účely a aplikace, z nichž některé s sebou nesou obrovské důsledky pro ochranu údajů, měla pracovní skupina za to, že je v této fázi nezbytné zveřejnit tento pracovní dokument a přispět k probíhající diskusi o otázkách RFID. Pracovní skupina doufá, že obsah tohoto dokumentu představuje užitečný příspěvek k debatě o RFID a vyzývá zainteresované strany k dodržování zásad uvedených v tomto dokumentu.

Tento pracovní dokument byl zpracován na základě dostupných informací s ohledem na stav vývoje technologie a zejména na její současné používání v různých odvětvích. Pracovní skupina si je však vědoma, že používání RFID se neustále vyvíjí: stále dochází k vývoji v této oblasti a čím více zkušeností získáváme, tím máme více znalostí o palčivých otázkách. Z tohoto důvodu je pracovní skupina odhodlána nadále sledovat technologický vývoj v této oblasti ve spolupráci se zainteresovanými stranami. Ve světle získaných zkušeností možná bude zapotřebí vrátit se k několika otázkám uvedeným v tomto pracovním dokumentu. Navíc v závislosti na vývoji technologie RFID a jejích aplikací se pracovní skupina v pozdější fázi možná rozhodne podrobně se zaměřit na konkrétní oblasti/aplikace a vydá další pokyny pro konkrétní použití.

PŘÍLOHA

TECHNOLOGIE RFID

Bezdrátová komunikace je nově vznikající technologie, která se nyní týká řady aplikací. Patří k nim sestavy bezdrátových místních sítí (WLAN) nebo bezdrátová připojení s malou šířkou pásma spojující různé přístroje, jako jsou laptopy, PDA, mobilní telefony atd. (Bluetooth).

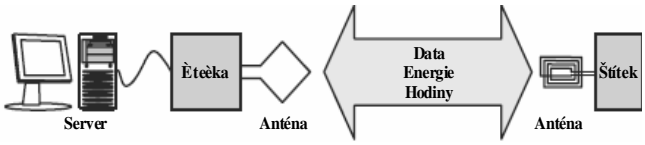
V průběhu několika posledních let roste obliba nové technologie. Říká se jí RFID, což znamená radiofrekvenční identifikace. Hlavní myšlenkou stojící za touto technologií bylo dát každému předmětu, který je opatřen štítkem RFID, jedinečnou identitu, kterou lze sdělit čtečce na rádiové frekvenci. To umožňuje různé způsoby použití v dodavatelském řetězci i jiná průmyslová použití. Na počátku se štítky RFID měly používat jako náhrada čárových kódů. Výhody jejich používání byly zjevné: Nevyžadují přímou viditelnost, a proto lze evidenci provádět automaticky. Nyní, jak technologie pokročila, můžeme přemýšlet o jiných důmyslnějších typech použití. Než se začneme zabývat možným použitím, uvádíme přehled o této technologii.

Nejjednodušší systém RFID se skládá ze dvou složek: ze štítku, který se připevní na předmět, a z čtečky, která dokáže získávat údaje ze štítku. Tyto složky spolu komunikují rádiovým spojením. Štítek i čtečka mají anténu a demodulátor (analogová předřazená část). Tato předřazená část „převádí" příchozí analogové informace z rádiového spojení na digitální data. Tato data může dále zpracovávat digitální část čtečky nebo štítku.

---

[20] *Feldhofer M., Dominikus S., Wolkerstorfer J., Strong Authentication for RFID Systems using the AES Algorithm (Odolné ověřování pro systémy RFID s využitím algoritmu AES), in Sborník ze semináře o šifrovacím hardwaru a vložených systémech (CHES 2004, 11. - 13. srpna 2004, Boston, USA), Lecture Notes in Computer Science (LNCS – Poznámky k přednáškám informatiky) svazek 3156, Springer Verlag, 2004, ISBN*

Na straně štítku může digitální zpracování provádět hardware na zakázku nebo mikroprocesor. Ke zpracování údajů získaných ze štítků lze použít hostitelský počítač (server) připojený ke čtečce. Tento server musí implementovat zvláštní aplikace s využitím údajů ze štítků. Obrázek znázorňuje běžný systém RFID.



Obrázek: Struktura systému RFID

Pro popis konkrétního systému RFID lze použít různé parametry této technologie. V závislosti na těchto parametrech mají systémy RFID různé možnosti použití:

– *aktivní/pasivní štítky RFID*. Základní štítky, které pracují pasivně, přijímají energii a synchronizační impulzy pro zpracování a přenos dat prostřednictvím elektromagnetického pole čtečky. Intenzita tohoto pole je omezena vnitrostátními a mezinárodními předpisy. Spotřeba energie štítku musí být proto omezena, aby se zajistilo správné fungování. Intenzita pole se zmenšuje se vzdáleností od čtečky, proto menší spotřeba energie štítku vede k většímu akčnímu rádiusu čtečky, tj. čtečka a štítek mohou komunikovat na delší vzdálenost. Aktivní štítky vysílají data, i když není přítomna nebo zaznamenána žádná čtečka. K tomu účelu jsou vybaveny baterií. Aby byl popis úplný, mohou některé štítky obsahovat kontrolní nebo měřicí zařízení, které zaznamenává hodnoty, jako např. teploměr, aby se zachytila přerušení chlazení v systému dopravy a skladování zmrazených potravin. V tomto případě je zapotřebí také baterie, ale bez přímých důsledků pro aktivní/pasivní povahu štítku;

– *provozní frekvence*. Systémy RFID mohou operovat s různými frekvencemi, akčními rádiusy a typy vazeb. Tyto parametry jsou často provázány silnými vzájemnými vazbami. Frekvence sahají od 135 kHz do 5,8 GHz. Zde je nutné mít na zřeteli mezinárodní omezení a fyzikální požadavky. Vazba může být elektrická, magnetická nebo elektromagnetická. Typ vazby ovlivňuje pracovní rozsah, který může činit od několika milimetrů po více než 15 m. Konkrétně lze rozlišit:

  - Systémy pro těsné spojení, které používají štítky s krátkým akčním rádiusem do jednoho centimetru. Pracovní frekvence jsou v rozsahu od oblasti nízkých frekvencí až po 30 MHz. Tyto štítky musejí být umístěny ve nebo na čtečce, aby mohly komunikovat. U těchto systémů je vysoká spotřeba energie a je možná vysoká přenosová rychlost dat.
  - Systémy pro dálkové spojení s akčním rádiusem přibližně jeden metr. Většina systémů RFID používá dálkové spojení na frekvencích mezi 135 kHz a 13,56 MHz.
  - Systémy s dalekým dosahem s akčním rádiusem přes jeden metr. Fungují na frekvencích mezi 868 MHz a 5,8 GHz.

Systémy RFID mohou rušit jiná rádiová zařízení. Proto je důležité, aby používaly jiné frekvence než audio-rozhlasové, televizní nebo mobilní rádiové služby. Nejvýznamnějšími frekvencemi využívanými pro systémy RFID jsou 0 až 135 kHz a frekvence pro průmyslové, vědecké a lékařské aplikace (Industrial-Scientific-Medical - ISM) 6,78 MHz, 13,56 MHz, 27,125 MHz, 40,68 MHz, 869,0 MHz, 2,45 GHz, 5,8 GHz a 24,125 GHz.

– schopnost číst/zapisovat. Složitost systémů RFID se liší. Často je omezena schopnostmi štítku.

  - U systémů nižší třídy („Low-End-Systeme“) jsou štítky pouze pro čtení. Čtečka může pouze číst obsah štítku, což je obvykle sériové číslo o několika bajtech. Tyto jednoduché štítky se často používají kvůli své nízké ceně a malé ploše čipu. Mohou se používat jako náhrada systémů čárových kódů tam, kde musejí být předměty identifikovány, obvykle pro účely skladového řízení nebo směrování zboží výrobním procesem. S tímto druhem štítků lze také provádět sledování zvířat.
  - Ve střední třídě systémů RFID mohou štítky obsahovat zapisovatelnou paměť. Kapacita paměti v současnosti sahá od několika bajtů po několik desítek nebo stovek kilobajtů EEPROM[21] u pasivních štítků a SRAM[22] u aktivních. V této řadě lze do štítků integrovat také čidla (teplotní, tlaková…), která například zachytí ekologické havárie, jež lze na štítek zaznamenat. Tyto štítky se mohou dále používat ke kontrole přístupu. Dalším způsobem použití, který již byl zaveden a vyzkoušen, je sledování zavazadel na letištích. Místo určení zavazadla lze zapsat do paměti štítku a směrování lze provést automaticky. Další uplatnění je ve zdravotnictví. Tyto štítky lze používat v nemocnicích k zaznamenání údajů o léčbě pacientů nebo ke sledování několika parametrů stavu pacienta.
  - Bezdotykové čipové karty s mikroprocesorem a operačním systémem jsou systémy vyšší třídy („High-End-Systeme“). Ty také obsahují určité množství paměti, které je obvykle větší než u štítků RFID střední třídy. Na kartě lze provádět složité funkce. Do paměti štítku lze ukládat programy, které lze pak spouštět mikroprocesorem. Vzhledem k vysoké spotřebě energie u těchto karet je akční rádius těchto systémů v současné době omezený na několik centimetrů. Tyto karty lze využít ke složitějším úkonům. Používají se u typických aplikací čipových karet, jako je kontrola přístupu. Lze je také používat jako průkaz totožnosti nebo průkaz zdravotního pojištění. Příklady, kdy se o těchto systémech RFID vyšší třídy diskutuje, představují cestovní doklady s ICC[23], jak je definuje ICAO, nebo víza a povolení k pobytu s ICC.

V Bruselu dne 19. ledna 2005

Za pracovní skupinu
Peter SCHAAR
Předseda

---

[21] *Electrically Erasable Programmable Read Only Memory (elektricky mazatelná programovatelná paměť pouze pro čtení)*

[22] *Static Random Acces Memory (statická paměť s náhodným přístupem)*

[23] *Integrated Circuit Chip (čip s integrovaným obvodem)*

PRACOVNÍ SKUPINA PRO OCHRANU DAT PODLE ČLÁNKU 29

654/06/EN
WP 119

Stanovisko č. 3/2006 ke směrnici Evropského parlamentu a Rady 2006/24/ES o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES

Přijato dne 25. března 2006

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

Její sekretariát je na Ředitelství C (Občanská spravedlnost, práva a státní občanství) Evropské komise, Generální ředitelství pro spravedlnost, svobodu a bezpečnost, B 1049 Brusel, Belgie, kancelář č. LX-46 01/43.
Internetová adresa:

http://europa.eu.int/comm/justice_home/fsj/privacy/index_en.htm

PRACOVNÍ SKUPINA PRO OCHRANU FYZICKÝCH OSOB

V SOUVISLOSTI SE ZPRACOVÁNÍM

OSOBNÍCH ÚDAJŮ

zřízená směrnicí Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995[1],

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

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

12. července 2002, s ohledem na svůj jednací řád, a zejména na články 12 a 14 uvedeného jednacího řádu,

PŘIJALA TOTO STANOVISKO:

Dne 21. února 2006 přijala Rada směrnici 2006/24/ES o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES[2]. Evropský parlament schválil návrh Komise (KOM (2005) 0438)[3] ve znění přijatém při vyjednávání s Radou a dne 14. prosince 2005 přijal příslušné legislativní usnesení (C6-0293/2005 – 2005/0182(COD)).

Pracovní skupina zřízená podle článku 29 vyjádřila své výhrady ve svém posledním stanovisku č. WP 113 ze dne 21. října 2005 k tehdejší předloze směrnice, poněvadž ustanovení směrnice s sebou přináší dalekosáhlé důsledky pro všechny evropské občany a hluboko zasahují do jejich soukromí. Rozhodnutí uchovávat elektronické údaje pro účely potírání závažné trestné činnosti je zatím bezprecedentní a má historický význam. Zasahuje do každodenního života každého občana a může ohrozit základní hodnoty a svobody, které požívají a ctí všichni evropští občané. Pracovní skupina připomíná své úvahy a obavy vyjádřené ve výše uvedeném stanovisku, které jsou stále aktuální. Z tohoto důvodu je nesmírně důležité, aby se provádění směrnice v každém členském státě opíralo o opatření, jež zredukují její dopad na soukromí.

Pracovní skupina zřízená podle článku 29 konstatuje, že ve směrnici postrádá přiměřená a konkrétní ochranná opatření zaměřená na nakládání s elektronickými údaji a že směrnice v tomto ohledu ponechává prostor pro odlišný výklad členskými státy a následně i pro různé provádění členskými státy. Přiměřená a konkrétní ochranná opatření jsou však nezbytná při ochraně základních zájmů fyzických osob, jak se uvádí ve směrnici 2002/58/ES, především práva na zachování důvěrnosti při využívání veřejně dostupných služeb elektronických komunikací. Pracovní skupina považuje rovněž za zásadní, aby byla ustanovení směrnice vykládána a prováděna harmonizovaně proto, aby se evropští občané mohli v celé Evropské unii těšit stejnému stupni ochrany.

Pracovní skupina zřízená podle článku 29 proto navrhuje jednotné celoevropské provádění směrnice. Tímto přístupem by mělo být zajištěno harmonizované uplatňování směrnice za současného dodržování nejvyššího možného stupně ochrany osobních údajů. Mělo by se tak postupovat i proto, aby se snížily značné náklady vynaložené poskytovateli služeb při plnění ustanovení směrnice.

Členské státy by měly zavést přiměřená a konkrétní ochranná opatření proto, aby jednotně transponovaly ustanovení směrnice do svých právních řádů a splnily požadavky stanovené v článku 8 Evropské úmluvy o lidských právech. Je třeba zohlednit alespoň tato ochranná opatření:

1) **Přesné vymezení účelu:** Údaje je třeba uchovávat pouze pro přesně vymezené účely. Z tohoto důvodu je třeba jasně definovat pojem „závažný trestný čin". Jakékoliv další zpracování údajů je třeba vyloučit nebo přísně omezit na základě konkrétních ochranných opatření.

2) **Omezení přístupu:** Údaje by měly být zpřístupněny pouze konkrétně pověřeným donucovacím orgánům při vyšetřování, odhalování a stíhání trestných činů uvedených ve směrnici. Je třeba zveřejnit seznam těchto pověřených donucovacích orgánů. Je třeba vést záznam o každém vyhledávání údajů a záznamy zpřístupnit orgánu dozoru, resp. orgánům dozoru, s cílem zajistit účinný výkon dozoru.

---

[1] *Úř. věst. L 281, 23.11.1995, s. 31, http://europa.eu.int/comm/justice_home/fsj/privacy/law/index_en.htm .*
[2] *Úř. věst. L 105, 13.4.2006, s. 54.*
[3] *Úř. věst. C 49, 28.2.2006, s. 42.*

3) **Minimalizace údajů:** Množství uchovávaných údajů je třeba omezit na minimum, přičemž musí být podle přísných měřítek prověřeno, zda je jakákoliv změna provedená v daném seznamu nezbytná.

4) **Zákaz vytěžování údajů:** Vyšetřování, odhalování a stíhání trestných činů uvedených ve směrnici nemůže být příčinou rozsáhlého vytěžování uchovávaných údajů ohledně způsobu cestování a komunikace osob, které nejsou podle donucovacích orgánů podezřelé ze spáchání trestného činu.

5) **Soudní / nezávislý přezkum oprávněného přístupu:** Je třeba respektovat zásadu, že soudní orgány v jednotlivých případech udělí řádné oprávnění k přístupu k údajům, aniž jsou dotčeny země, kde je konkrétní možnost přístupu k údajům, podléhající nezávislému dozoru, zakotvena v právním řádu. V oprávnění se případně uvedou přesně konkrétní údaje vyžadované v konkrétním případě.

6) **Účel uchovávání dat poskytovateli:** Poskytovatelům veřejných služeb elektronických komunikací nebo poskytovatelům sítí není dovoleno zpracovávat údaje, uchovávané pouze k účelu udržení veřejného pořádku podle směrnice o uchovávání údajů, pro jiné účely, zejména pro své vlastní.

7) **Oddělení systémů:** Logicky je především třeba oddělit systém ukládání údajů pro účely udržení veřejného pořádku od systémů používaných k obchodním účelům.

8) **Bezpečnostní opatření:** V souvislosti s technickými a organizačními bezpečnostními opatřeními, které jsou poskytovatelé povinni přijmout, je třeba definovat minimální standardy, ve kterých budou podrobně rozpracovány obecné požadavky směrnice o uchovávání údajů.

Pracovní skupina zřízená podle článku 29 vyzývá členské státy, aby koordinovaly provádění směrnice o uchování údajů do svých právních řádů s cílem zaručit harmonizovaný přístup v celé Evropské unii a zachovat vysoký stupeň ochrany údajů stanovený ve směrnicích 1995/46/ES a 2002/58/ES.

V Bruselu dne 25. března 2006

Za Pracovní skupinu
Peter SCHAAR
předseda

Pracovní skupina pro ochranu dat podle článku 29	

2067/05/CS
WP 116

Stanovisko 6/2005 k návrhům nařízení Evropského parlamentu a Rady (KOM (2005) 236 v konečném znění) a rozhodnutí Rady (KOM (2005) 230 v konečném znění) o zřízení, provozu a využívání Schengenského informačního systému druhé generace (SIS II) a k návrhu nařízení Evropského parlamentu a Rady o přístupu subjektů odpovědných za vydávání osvědčení o registraci vozidel v členských státech k Schengenskému informačnímu systému druhé generace (SIS II) (KOM (2005) 237 v konečném znění)

přijaté pracovní skupinou dne 25. listopadu 2005

OBSAH

Pracovní skupina pro ochranu fyzických osob

PŘI ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

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

s ohledem na čl. 29 a čl. 30 odst. 1 písm. a) a odst. 3 uvedené směrnice a na čl. 15 odst. 3 směrnice 2002/58/ES Evropského parlamentu a Rady ze dne 12. července 2002,

s ohledem na svůj jednací řád a zejména na články 12 a 14 tohoto jednacího řádu,

přijala toto stanovisko:

1. Úvod a základní informace

Schengenská spolupráce: stručný přehled

a) Schengenská úmluva a následně přijatá ustanovení představují formu mezivládní spolupráce značného významu s cílem zrušit kontroly na vnitřních hranicích zúčastněných členských států EU. Za tímto účelem byla v úmluvě stanovena zvláštní pravidla, zejména společná pravidla o vstupu a pobytu cizinců a o soudní a policejní spolupráci – cílem bylo uznat platnost činností a ustanovení každého zúčastněného členského státu (hledané osoby, záznamy za účelem odepření vstupu).

Za nezbytné k dosažení uvedených cílů bylo považováno vytvoření informačního systému SIS.

Účel SIS je jasně vymezen v čl. 92 odst. 1 úmluvy: umožnit orgánům určeným členskými státy získat pomocí automatizovaného vyhledávacího postupu přístup k záznamům o osobách a věcech při provádění hraničních kontrol a jiných policejních a celních kontrol.

Každá smluvní strana je povinna vyhodnotit, zda je v souvislosti s některými fyzickými osobami a se zvláštními typy chování kromě vnitrostátních opatření zapotřebí schengenská spolupráce, podle níž se do SIS vkládá záznam, který se týká např. fyzické osoby podléhající příkazu k vyhoštění nebo zákazu vstupu nejen na území země, která příkaz k vyhoštění vydala, ale také na celém schengenském území, což vyžaduje zásah všech smluvních stran.

Pokud jde o zpracování osobních údajů v systému, jsou smluvní strany společnými správci zpracování údajů v C-SIS vzhledem k tomu, že C-SIS je kumulativním výsledkem jednotlivých vnitrostátních archivů (N-SIS). C-SIS, který je jednotkou technické podpory, má sídlo ve Štrasburku a technickou zodpovědnost za něj má jedna z účastnických zemí, tj. Francie (viz články 115 a 92 úmluvy).

Vnitrostátní kontrolní orgány pro ochranu údajů vykonávají dozor a kontrolu nad vnitrostátní databází a společně, v rámci schengenského společného dozorového orgánu (Schengen JSA), nad C-SIS.

Schengenským informačním systémem se ve skutečnosti zabývá celá hlava úmluvy (hlava VI – články 92 až 119), která stanoví jeho provozní mechanismy specifikací kategorií údajů, které mají být vkládány, mechanismů pro provoz systému, pravidel o ochraně údajů – včetně práv subjektů údajů na informace a přístup – a přidělením povinností, které se týkají řízení systému na centrální (C-SIS) i vnitrostátní (N-SIS) úrovni;

b) Po začlenění do Smlouvy podléhá Schengenská úmluva právním předpisům EU, pokud jde o jakékoliv změny jejích ustanovení.

Po mnoha letech, kdy docházelo pouze k omezeným změnám ustanovení úmluvy, bylo v tomto posledním roce zaznamenáno značné zvýšení počtu iniciativ – například kodex Společenství neboli „hraniční kodex“, který upravuje překračování hranic, změny Společných konzulárních instrukcí, zřízení Vízového informačního systému jakožto nástroje pro společnou vízovou politiku[1] a ustanovení, která se použijí na vstup a vyhoštění a na policejní spolupráci atd.,[2], jimiž se brzy nahradí celé oddíly úmluvy.

Již několik let se diskutuje o vývoji nového Schengenského informačního systému (SIS) i o záměru zavést pro SIS nové funkce, které by integrovaly činnost vnitrostátních kanceláří SIRENE vytvořených proto, aby umožnily výměnu doplňujících informací k záznamům.

[1] Stanovisko vydané pracovní skupinou dne 23. června 2005 (WP110.Ref.1022/05).

[2] Odkazuje se na návrhy nařízení a nástrojů (kodex Společenství, VIS, návrh směrnice o vyhoštění), z nichž některé již byly předloženy k projednání, zatímco jiné ještě ne. Celkově je cílem těchto nástrojů nahradit první dvě hlavy Schengenské úmluvy, tj. základní pravidla provozu SIS, pokud jde o část, která má být regulována návrhem nařízení (záznamy o cizincích, jimž má být zamítnut vstup). Existují také iniciativy, které předpokládají změny jiných ustanovení Schengenské úmluvy, jež se týkají policejní spolupráce.

Navrhovaný nový právní základ pro SIS II bude velmi důležitý, jelikož umožní novým členským státům EU využívat systém a jejich občanům volně se pohybovat v prostoru bez vnitřních hranic a zároveň zachovat vysokou úroveň bezpečnosti.

c) Dne 31. května 2005 Komise Evropských společenství předložila tři různé návrhy právních aktů.

Dva návrhy (návrhy nařízení Evropského parlamentu a Rady a rozhodnutí Rady o zřízení, provozu a využívání Schengenského informačního systému druhé generace (SIS II)) mají nahradit celou hlavu VI úmluvy a obsahují ustanovení závazná pro členské státy.

Třetí návrh nařízení Evropského parlamentu a Rady se týká přístupu subjektů odpovědných za vydávání osvědčení o registraci vozidel v členských státech k SIS II[3].

Nařízení a rozhodnutí o zřízení, provozu a využívání SIS II mají podobnou strukturu, nejdříve vymezují cíle, a poté specifikují povinnosti členských států a Komise.

Po těchto ustanoveních následují pravidla, kterými se upravuje zpracování a jeho zákonnost: důvody pro pořizování záznamů, kategorie údajů, doba uchovávání, pravidla přístupu, práva subjektů údajů: právo na informace, právo na přístup, opravu a výmaz, opravné prostředky, úloha orgánů pro ochranu údajů.

Navzdory tomu, že bude SIS II regulován dvěma rozdílnými právními akty, které mají rozdílný právní základ, bude jednotným systémem.

Pracovní skupina byla požádána o stanovisko ke znění dotyčných návrhů. Za tímto účelem se stanovisko pracovní skupiny zaměří na společné otázky, kterými se tyto dva návrhy zabývají, a na ustanovení obsažená v návrhu nařízení. Na návrh rozhodnutí Komise se bude výslovně odkazovat vždy, když bude zapotřebí řešit konkrétní prvky, které se v nařízení nevyskytují.

Především je zapotřebí zdůraznit velmi složitou povahu návrhů, změny, které budou obsahovat, pokud jde o architekturu systému i o počet a kvalitu kategorií údajů, jež má systém podle předpokladů obsahovat, a významný dopad na základní lidská práva a ochranu údajů, jaký tento informační systém při použití napříč EU bude mít. V současnosti databáze SIS obsahuje přes 13 miliónů záznamů, z nichž se 1/10 týká „hledaných osob“.

Je třeba mít na paměti, že se SIS souvisí také mnoho připravovaných právních nástrojů: kromě výše uvedených návrhů, které se týkají VIS, lze odkázat přinejmenším na navrhovanou interoperabilitu SIS, VIS a systému EURODAC a na návrhy, jejichž cílem je umožnit orgánům pověřeným zajišťováním vnitrostátní bezpečnosti přístup k VIS a SIS.

Proto pracovní skupina velmi lituje toho, že Komise neposkytla podrobný vysvětlující komentář k důvodům, které jsou základem navrhovaných změn, a neprovedla hloubkové posouzení dopadu, včetně vyhodnocení jejich dopadu na ochranu údajů a základní lidská práva.

2. Právní základ a obecné připomínky

Nový právní základ pro SIS II se nachází ve Smlouvě o Evropské unii (pokud jde o rozhodnutí) a ve Smlouvě o založení Evropského společenství (pokud jde o nařízení), ačkoliv SIS II by měl být považován za jednotný informační systém.

Nutno uznat, že nařízení i rozhodnutí byly pečlivě zpracovány a obsahují několik prvků, které jsou vítány.

Velké obavy však vzbuzuje volba právních nástrojů provedená Komisí za účelem vytvoření SIS II.

Důvodová zpráva Komise ve skutečnosti zdůrazňuje, že volba nařízení (a rozhodnutí) „má náležité opodstatnění s ohledem na potřebu používat plně harmonizovaná pravidla, a to zejména v souvislosti se zpracováním údajů v systému“, takže „ustanovení…jsou přímo a jednotně použitelná jako závazná a svou samotnou podstatou nevyžadují, aby členské státy činily jakákoli opatření k jejich transpozici do vnitrostátního práva.“

Zde je potřeba připsat zvláštní význam dvěma bodům. Zaprvé se jedná o analýzu důsledků souvisejících s tímto druhem používání nařízení (a ještě více rozhodnutí), čímž by ze zákonodárného procesu byli vyloučeni zákonodárci a veřejné mínění v dotčených zemích; to se ve skutečnosti týká velmi složitých záležitostí, které mají velký vliv na základní práva a na právo na ochranu osobních údajů. Zadruhé se jedná o otázku jak přijmout jednotný právní rámec pro zpracování údajů v SIS II jakožto jednotném informačním systému, zatímco se předpokládají různé soubory pravidel pro různé účely zpracování.

[3] Návrh nařízení Evropského parlamentu a Rady o přístupu subjektů odpovědných za vydávání osvědčení o registraci vozidel v členských státech k Schengenskému informačnímu systému druhé generace (SIS II) (KOM(2005) 237 v konečném znění).

a) Obecný rámec

1 – V současnosti je zpracování osobních údajů v SIS regulováno v jednotné perspektivě ustanoveními Schengenské úmluvy.

Obecná pravidla ochrany údajů a zásady společného použití ve stávajícím znění úmluvy zaručuje kromě práva na respektování soukromého a rodinného života článek 8 Úmluvy Rady Evropy o ochraně lidských práv a základních svobod (EÚLP) (který představuje – částečně ve světle příslušné judikatury Evropského soudního dvora pro lidská práva – hlavní vodítko k objasnění omezení narušování soukromého života jednotlivců orgány veřejné moci, jež vykonávají pravomoci, které jim byly svěřeny), Úmluva Rady Evropy o ochraně osob s ohledem na automatizované zpracování osobních údajů (Úmluva 108) z r. 1981 a zvláštní doporučení 87 (15), které upravuje používání osobních údajů v policejní oblasti[4].

Schengenská úmluva tedy smluvní strany zavazuje přijmout nezbytná vnitrostátní ustanovení, aby se dosáhlo úrovně ochrany osobních údajů, která alespoň odpovídá úrovni vyplývající z Úmluvy 108 a je v souladu s výše uvedeným doporučením. Všechny země, které se v současnosti podílejí na Schengenském informačním systému, přijaly požadovaná vnitrostátní opatření – která se týkají například mechanismů k výkonu práv svěřených subjektům údajů, odpovědnosti za zpracování osobních údajů a přidělení dozorčích a kontrolních funkcí.

2 – Návrhy předložené Komisí obsahují důkladnou reorganizaci SIS zejména proto, že pro operace zpracování vykonávané v SIS nebo jeho prostřednictvím se používají různé právní základy. Návrhy tedy odlišují operace zpracování prováděné v SIS na základě nových kompetencí Společenství v oblasti přistěhovalectví a azylu, zatímco jiné kategorie údajů nebo operací by zůstaly v oblasti působnosti tzv. třetího pilíře. Jedná se o pokus provést plán – který v roce 1999 nebyl splněn – podle něhož by pravidla SIS, jež se vztahují k záznamům o státních příslušnících třetích zemí (tj. o cizincích), kterým má být zakázán vstup (článek 96), měla podléhat právním předpisům Společenství (viz body odůvodnění 10 a 11 návrhu nařízení).

3 – Komise také předpokládá jiný typ architektury SIS; na rozdíl od současného rámce založeného na vnitrostátních systémech (N-SIS) plus na jednotce centrální podpory, která se nachází ve Štrasburku a obsahuje stejné informace jako vnitrostátní systémy, by byla vytvořena centrální

[4] Doporučení č. R (87) 15 ze dne 17. září 1987

databáze, do které by informace – tj. záznamy a jiné další údaje podle návrhů – měly být vkládány přímo prostřednictvím vnitrostátních rozhraní, která neobsahují žádné údaje.

Přístup zvolený Komisí a výsledná změna architektury SIS tak mohou mít závažný vliv jen na mechanismy zpracování údajů a na související dozorčí a kontrolní činnosti svěřené nezávislým orgánům pro ochranu údajů.

Referenční legislativní rámec projde hloubkovými změnami a zejména pravidla ochrany údajů použitelná na zpracování – jak již bylo zdůrazněno – už nebudou stanovena jednotně.

To znamená, že je třeba posoudit, zda – a do jaké míry – jsou pravidla, která mají být zavedena s ohledem na část SIS zařazenou do oblasti práva Společenství, v souladu s obecnými zásadami ochrany údajů stanovenými ve směrnici 95/46/ES, jež by měla být vlastně považována za harmonizovaný regulační rámec, který by se měl používat jako měřítko[5].

Než se bude vyžadovat zpracování biometrických údajů v SIS (digitální podobizna a otisky prstů), umožní přístup pro jiné orgány a zavede možnost předávání údajů do zemí a orgánů mimo EU, je také nutné provést pečlivé vyhodnocení ve světle pravomocí, které Smlouva o EU svěřuje zákonodárci EU.

Pracovní skupina vítá okolnost, že přijetí návrhu nařízení na úrovni Společenství bude založeno na postupu spolurozhodování a že Evropský parlament si je plně vědom problémů vyplývajících v tomto i v jiných případech (přistěhovalecká a azylová politika). Pracovní skupina by však ráda zdůraznila nutnost obecné analýzy otázek, které se dříve řešily v rámci třetího pilíře (a byly regulovány pomocí nástrojů třetího pilíře) a nyní spadají do oblasti působnosti právních předpisů Společenství.

Kdykoliv se jako v těchto návrzích sestávají dotyčné otázky výlučně ze shromažďování, používání a výměny osobních údajů, musí být vždy zaručeno řádné a kompetentní vyhodnocení dopadu takovýchto návrhů na soukromý život jednotlivců. Pracovní skupina opakuje požadavek zajistit, aby probíhající proces za účelem schválení příslušného znění a jeho vstupu v platnost byl alespoň vyvážený a umožnil subjektům, jako jsou orgány pro ochranu údajů, využívat vhodné informační a odpovědní mechanismy, jako jsou mechanismy, které jsou obecně k dispozici v každé zemi v souvislosti s každým právním předpisem, jenž spadá do jejich pravomoci.

[5] V této souvislosti viz 14. bod odůvodnění návrhu nařízení Komise o SIS II.

b) Pravidla prvního pilíře pro ochranu údajů

Pokud jde o ustanovení ES o ochraně údajů, článek 7 Charty základních práv potvrzuje zásadu stanovenou v EÚLP, zatímco článek 8 zavádí nové základní právo pro každého jednotlivce, právo na ochranu údajů.

Obecné harmonizované zásady jsou stanoveny ve směrnici Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995[6] o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (směrnice 95/46). Bod odůvodnění 14 návrhu nařízení potvrzuje použití směrnice na zpracování údajů provedené podle nařízení.

Návrh nařízení však poskytuje členským státům příležitost – na základě pravomocí, které jim jsou svěřeny za účelem stanovení výjimek nebo omezení pro subjekty údajů podle článku 13 směrnice – provádět „doplnění nebo výklad“ uvedených zásad, bude-li to nutné.

Nutno zvážit, zda a do jaké míry mohou být rozvíjena v rámci prvního pilíře opatření, která jsou pro členské státy přísně závazná, a ačkoliv odkazují na zásady stanovené ve směrnici o ochraně údajů, regulují otázky ochrany údajů jiným způsobem.

V této souvislosti nutno upozornit, že dodatečná zvláštní ustanovení o zpracování osobních údajů byla dosud přijata pouze v odvětví elektronických komunikací prostřednictvím směrnice 2002/58/ES a že mnohé jiné nástroje Společenství obsahují zvláštní ochranná opatření, které se používají na osobní údaje – v tom smyslu, že neovlivňují pravidla stanovená ve směrnici 95/46/ES, která stanoví, jak již bylo uvedeno, harmonizovaný regulační rámec na úrovni EU.

Ačkoliv pracovní skupina vítá rozhodnutí Komise přesunout nařízení, která se týkají části SIS, jež obsahuje záznamy o cizincích pro účely odepření vstupu (článek 96 úmluvy) do prvního pilíře, ráda by zdůraznila, že je zároveň nutné zajistit, aby se směrnice používala úplně a bezvýhradně – aniž by bylo dotčeno případné použití ustanovení stanovených zejména v článku 13.

Je nepochybné, že posledně uvedená ustanovení mohou vstoupit do hry pouze v případech, kdy směrnice o ochraně údajů ponechává členským státům určité diskreční pravomoci. Jestliže však nástroj Společenství jako navrhované nařízení zavede opatření, která se přesně týkají případů, na něž se odkazuje výše, lze mít za to, že uvedený nástroj stanoví harmonizovaný přístup, a ruší tedy

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

tyto diskreční pravomoci. To znamená, že by členským státům nezbýval prostor na zavedení dodatečných vnitrostátních opatření v této oblasti s výjimkou případů, kdy to bude nezbytné pro účely konkrétního provádění dotyčného nástroje (nástrojů) Společenství. Podobně by se dalo ukázat, že odkaz na plně harmonizovaná pravidla obsažená v důvodové zprávě by mohl právě vést k tomu, že jedinými povolenými odchylkami by byly ty, na které odkazuje nařízení.

Návrhy uvedené v navrhovaném nařízení však nejsou v tomto ohledu plně v souladu se směrnicí 95/46/ES a vyvolávají určité obavy.

Co se týče směrnice 95/46/ES, neexistuje zde přímé použití obecných zásad, ale pouze „přepsání" obsahu některých ustanovení, která jsou někdy neúplná; tak vzniká jakási *lex specialis* neboli nové kategorie ustanovení o ochraně údajů v prvním pilíři. Odkazuje se zejména na práva subjektů údajů, dodržování zásady omezení účelu, definici správce a odpovědnosti za zpracování osobních údajů v systému a na dozor a kontrolu na centrální a vnitrostátní úrovni. Nesrovnalosti panují také v souvislosti se stávajícím zněním, kde důvod některých změn zůstává nejasný, jelikož neexistuje řádné posouzení.

3. Konkrétní otázky vyvolané návrhy

Stávající pravidla představují komplexní soubor ustanovení pro zpracování údajů SIS, včetně přísného režimu ochrany údajů pro používání osobních údajů. Je třeba zvážit, zda a do jaké míry zajistí navrhovaná nová pravidla vysokou úroveň ochrany, která by měla alespoň odpovídat stávající úrovni ochrany.

a) Cíl a rozsah působnosti SIS II

Směrnice 95/46 povoluje zpracování osobních údajů pro stanovené, výslovně vyjádřené a legitimní účely a požaduje, aby údaje nebyly dále zpracovány žádným způsobem, který je s těmito účely neslučitelný.

Ve světle této zásady se pracovní skupina domnívá, že navrhované nařízení, na rozdíl od navrhovaného rozhodnutí, omezuje zpracování údajů v SIS II na účel odmítnutí vstupu na území členských států (čl. 2 odst. 1). Je však třeba zdůraznit, že článek 1 obou návrhů nástrojů odkazuje na širší účel výměny informací pro kontrolu osob a předmětů. V posledním případě by se účel jevil svým rozsahem jako nepochybně širší než současný účel systému – jímž je umožnit přístup k záznamům o osobách a věcech při provádění hraničních kontrol a jiných policejních a celních

kontrol a u záznamů podle článku 96 pro účel vydávání víz a povolení k pobytu a správy právních předpisů o cizincích.

Tento restriktivní výklad účelů SIS, pokud jde o část, kterou se zabývá návrh nařízení, podporuje okolnost, že články 17 a 18 stanoví, které orgány mají právo na přístup do systému, a toto právo je omezeno na orgány zodpovědné za kontrolu osob na vnějších hranicích a na orgány, které se podílejí na provádění přistěhovaleckých zákonů. Orgány zodpovědné za policejní a celní kontroly prováděné v členských státech, které měly k těmto údajům přístup podle Schengenské úmluvy (článek 101), jsou nyní vyloučeny. Podle nařízení jim přístup není povolen.

Jelikož však navrhované znění jako takové nespecifikuje, které činnosti jsou pro dotyčné účely skutečně zahrnuty, vítá pracovní skupina objasnění účelů SIS podle návrhu nařízení. Pracovní skupina opakuje nutnost stanovit konzistentní pravidla týkající se orgánů, kterým má být povolen přístup k systému, aby se zajistilo dodržování zásad minimalizace údajů a proporcionality v souvislosti s přidáním nových funkcí k systému – zejména s ohledem na zahrnutí biometrických údajů a na propojení záznamů.

Vyvstávají také některé otázky, pokud jde o možnost nástroje třetího pilíře, který by umožnil obecnější přístup policejních orgánů, jak se předpokládá v souvislosti s přístupem k VIS. Opět je nutné dodržovat přísné používání zásady stanovení účelu, což nepřipouští systematický a rutinní přístup policejních orgánů k této části SIS.

b) Přístup k systému

Jak jsme již upozornili, nařízení o přístupu k údajům SIS II budou muset být přijata striktně pro požadované účely, jak obecně, tak s ohledem na předpokládané konkrétní úkoly.

Co se týče návrhů nástrojů, zdá se, že je zapotřebí hlouběji prozkoumat důvody a mechanismy, které povolují přístup k údajům úřadům a orgánům EU, jako jsou azylové orgány, orgány zodpovědné za osvědčení vozidel, Europol a Eurojust.

Výše uvedené orgány nejsou příslušné rozhodovat o jednání v souvislosti se záznamy SIS; proto by k jejich přístupu do databáze docházelo pouze v souvislosti s různými úlohami svěřenými uvedeným orgánům nástroji, které je zřídily – vyhodnocení žádostí o azyl, vyhodnocení za účelem registrace vozidla, splnění cílů stanovených ve vztahu k Europolu a Eurojustu příslušnými nástroji a úmluvami. V tomto případě je potřeba striktně a jasně stanovit pro tyto orgány nové dodatečné

úlohy, které musí být doplněny přísnými ochrannými opatřeními. Pokud jde o postupy, které se týkají přiznání postavení uprchlíka, měla by se vynaložit mimořádná péče, aby se předešlo nesprávnému používání opatření, které spočívá na humanitárních, nikoliv pouze na „byrokratických" základech – a to na právu, jež uznává a reguluje Ženevská úmluva z roku 1951.

V této souvislosti zastává pracovní skupina názor – jak již upozornila ve svém stanovisku k VIS[7] *– že přístup uvedených orgánů k SIS II přesahuje kritérium omezení účelu, a proto by neměl být povolen.*

Dále je třeba upozornit, že články 18 a 19 navrhovaného nařízení se pokoušejí určit orgány na základě několika nástrojů Společenství, které ještě nebyly přijaty nebo vůbec ještě navrženy. Proto by se jevilo jako nutné vyčkat na přijetí dotyčných nástrojů Společenství, než se posoudí, zda jsou v souladu se zásadami ochrany údajů, zejména v souvislosti s omezením účelu.

Současné znění navrhovaného rozhodnutí, které umožňuje přístup k některým kategoriím záznamů Europolu a Eurojustu a předpokládá možnost předávání údajů třetím zemím a orgánům, pravděpodobně vyústí v širší důsledky vzhledem k návrhům spojit SIS II s Vízovým informačním systémem (VIS) a k postoupení třetím zemím.

Navrhované předávání údajů Europolu a Eurojustu rovněž tak postihne nepříznivě systém ve smyslu dodržování zásady stanovení účelu vzhledem k větším příležitostem přistupovat k údajům a používat je pro různé účely vyhledávané těmito organizacemi.

Pracovní skupina opakuje svou výzvu k Radě výslovně vymezit účel SIS II. Pouze po tomto objasnění bude možné posoudit, zda, a pokud ano, ve kterých situacích bude možné předávání údajů SIS II třetím stranám nebo orgánům. Je však třeba zdůraznit, že samotná možnost předávání informací třetím stranám – což by bylo rozhodnutí, které by v každém případě spadalo do rozsahu pravomoci jednotlivých členských států a používalo by se pouze na údaje, které vlastní, vzhledem ke konfiguraci systému – se nezdá být v souladu s účelem systému tak, jak je v současnosti konfigurován.

[7] Stanovisko WP110 k návrhu nařízení Evropského parlamentu a Rady o vízovém informačním systému (VIS) a výměně údajů o krátkodobých vízech mezi členskými státy (KOM (2004) 835 v konečném znění) ze dne 23. června 2005.

c) Nové kategorie údajů a záznamů – biometrie

V 10. bodě odůvodnění návrh nařízení vysvětluje, že je „nanejvýš žádoucí dále harmonizovat ustanovení o důvodech pořizování záznamů o státních příslušnících třetí země za účelem odepření vstupu“, a dále uvádí, že „by mělo být více sjednoceno, jaké mohou být důvody pořizování těchto záznamů, jejich účely a orgány s právem přístupu k záznamům“.

Není však jasné, jaké změny byly provedeny za účelem harmonizace důvodů pro vkládání záznamů, a stále se zdá, že orgánům odpovědným za rozhodnutí, zda je záznam odůvodněný, je dána velká míra volnosti v rozhodování.

Článek 15 návrhu nařízení nezahrnuje tento požadavek pro vnitrostátní záznamy, i když je třeba zvážit nové návrhy na vyhoštění.

Nařízení přidává nové kategorie údajů bez ohledu na nedávné přijetí a vstup v platnost dvou zvláštních nástrojů, které mají hlavně rozšířit kategorie údajů, jež lze do systému vkládat. Stanoví, jak již bylo řečeno, bez jakéhokoliv řádného posouzení nutnosti tohoto návrhu, zahrnutí fotografií (v podobě digitálních podobizen) a otisků prstů spolu se záznamem.

Pracovní skupina opakuje své obavy také vzhledem k tomu, že návrhy neobsahují žádné ustanovení, jak se otisky prstů a fotografie mají pořizovat a začleňovat do systému, v souvislosti s pravidly přístupu nebo se zvláštními bezpečnostními opatřeními, která musí být zavedena.

Nařízení by zejména mělo objasnit postup zápisu řečených biometrických údajů a skutečnost, zda do systému budou také zahrnuty údaje, které v současnosti mají příslušné orgány a které se týkají případů, jež mají být regulovány podle článku 25 návrhu (tj. nesprávná identifikace osob).

Vzhledem k vysoké citlivosti této kategorie údajů, která spadá do rozsahu působnosti kategorií, na něž odkazuje článek 6 Úmluvy 108, by zpracování těchto údajů mělo být zajištěno stanovením adekvátních norem na mezinárodní úrovni. V zásadě by měly být vyloučeny vyhledávací funkce založené na těchto údajích.

V této souvislosti by pracovní skupina upozornila na své předchozí dokumenty a stanoviska ke zpracování biometrických údajů – od Pracovního dokumentu o biometrii z roku 2003 po nedávné stanovisko WP110 k Vízovému informačnímu systému (VIS) a stanovisko WP112 k biometrii

v pasech a cestovních dokumentech – a odkázala by také na připomínky, které k tomuto bodu učinil Evropský inspektor ochrany údajů ve svém stanovisku k SIS II[8].

d) Propojení záznamů

Článek 26 nařízení umožňuje členskému státu vytvořit odkaz mezi pořizovanými záznamy v SIS „v souladu se svými vnitrostátními právními předpisy". Vzhledem k tomu, že se propojení záznamů považuje za novou kategorii údajů obsažených v záznamech (viz čl. 16 písm. j) nařízení), že údaje SIS musí být uchovávány odděleně od jiných údajů a zpracovávány v souvislosti s konkrétním účelem sběru a konečně že navrhovaný nový právní rámec nevyžaduje „transpozici" do vnitrostátního práva, je toto znění zdrojem obav.

Návrhy musí zajistit, aby měl každý odkaz zřetelný provozní požadavek, dodržoval zásadu proporcionality a byl založen na jasně vymezeném vztahu, jak vyžadují závěry Rady ze dne 14. června 2004[9] k funkčním požadavkům SIS II.

Zejména by mělo být výslovně vyloučeno propojení záznamů pocházejících z několika zemí, protože by změnilo pravidla, která se používají na odpovědnost za zpracování osobních údajů, a vyvolalo by to zkreslené účinky, pokud jde o dozor a kontrolu vnitrostátních a centrálních orgánů pro ochranu údajů.

Propojení dále nesmí vytvořit nová přístupová práva. V této souvislosti by pracovní skupina uvítala jasnější znění odstavce 2 uvedeného článku a sdílí obavy vyslovené schengenským společným dozorovým orgánem, který varoval, že propojení záznamů by mohlo uživatelům umožnit přístup k informacím, na které nemají nárok.

Vzhledem k obrovskému počtu záznamů, které v systému pravděpodobně budou, musí být návrh vytvořit „vztahy mezi dvěma nebo více záznamy" pečlivě posouzen ve světle zásady omezení účelu. Nařízení by mělo zavést prováděcí ochranná opatření pro používání těchto odkazů a omezit přístup na oprávněné členy příslušných orgánů za účelem plnění jejich úkolů.

[8] Stanovisko ze dne 19. října 2005 ke třem návrhům Schengenského informačního systému druhé generace (SIS II) (KOM (2005)230 v konečném znění, KOM (2005)236 v konečném znění a KOM (2005)237 v konečném znění).

[9] Závěry zasedání Rady ve složení pro obecné věci a vnější vztahy ze dne 14. června 2004.

e) Doba uchovávání

Nutno zdůraznit, že ve všech navrhovaných nástrojích je doba uchovávání údajů pro každý typ záznamu prodloužena – včetně kontrolních protokolů – i když Komise nevysvětlila důvod (y) tohoto požadavku.

Konkrétněji, čl. 20 odst. 5 nařízení zavádí ustanovení, podle kterého se záznam vymaže automaticky po uplynutí pěti let od data rozhodnutí uvedeného v čl. 15 odst. 1, jestliže členský stát nerozhodne o ponechání záznamů v systému, pokud jsou splněny podmínky článku 15. Zdá se, že tak byl nahrazen požadavek v čl. 112 odst. 1 Schengenské úmluvy přezkoumat potřebu uchovávání osobních údajů v SIS nejpozději tři roky po jejich zařazení.

Pracovní skupina opakuje, že osobní údaje nesmí být uchovávány déle, než je nezbytné, a ráda by věděla, na základě jakých zkušeností a požadavků se Komise rozhodla zavést tyto doby uchovávání. Jelikož neexistují adekvátní důvody, je pracovní skupina toho názoru, že doba uchovávání, které je v současnosti stanoveno v Schengenské úmluvě, by se nemělo měnit.

Pracovní skupina by si v každém případě přála, aby nařízení výslovně stanovilo kratší dobu pro přezkoumání, aby se zajistilo, že osobní údaje lze vymazat, když již nebudou zapotřebí.

f) Právo na informace, přístup, opravu a výmaz a opravné prostředky

1. Článek 28 nařízení dává jednotlivcům právo na informace podobné článku 10 směrnice, ale nejsou uvedeny žádné informace o úloze a adrese vnitrostátního dozorového orgánu za účelem poskytnutí účinných opravných prostředků.

Proto *by návrh Komise měl být doplněn o specifikaci, že informace musí výslovně odkazovat na možnost zpochybnit rozhodnutí o vložení záznamu do systému a musí zahrnovat adresu vnitrostátního dozorového orgánu pro ochranu údajů.*

2. Článek 29 stanoví právo osob na přístup k jejich osobním údajům v souladu s právem členského státu, v němž se osoba uvedeného práva domáhá, a dokonce stanoví 60denní lhůtu pro odpověď na tuto žádost o přístup. S ohledem na různé předpisy platné v členských státech by jistě bylo vhodné, *aby navrhované nařízení (a možná rozhodnutí) přímo stanovilo jasná, jednotná pravidla celého postupu – která by měla výslovně odkazovat na případy, kdy mohou být informace odepřeny, nebo by jinak vylučovala možnost použít omezení povolená článkem 13 směrnice.*

3. Čl. 15 odst. 3 nařízení dává jednotlivcům právo požadovat přezkoumání rozhodnutí pořídit záznam, které učinil správní orgán, nebo odvolat se, ale není zde řečeno nic o jakékoliv odpovídající povinnosti informovat uvedenou osobu, když je takovýto záznam pořízen, ani o postupu při výkonu uvedeného práva. *Pracovní skupina toto ustanovení vítá, ale zastává názor, že aby bylo účinné, měl by návrh nařízení výslovně stanovit, že informace musí být poskytnuty nejpozději když je přijato opatření vyplývající z vložení záznamu do SIS.*

4. Článek 30 musí být v souladu s článkem 22 směrnice vzhledem k možné úloze orgánů pro ochranu údajů při poskytování správního opravného prostředku. Je třeba mít na paměti, že pouze v omezeném počtu případů bude žadateli povoleno vstoupit na území členského státu a že výkon tohoto práva nemůže být omezen na fyzickou přítomnost na území dožádaného členského státu.

Podle toho by měl být také změněn článek 52 návrhu rozhodnutí; to by bylo ve skutečnosti v souladu se současným zněním Schengenské úmluvy[10]. *Proto by zeměpisný požadavek, který je v současnosti stanovený v tomto článku, neměl být brán v úvahu, aby subjekty údajů mohly podávat stížnosti – právě kvůli okolnostem uvedeným v předcházejícím odstavci.* V porovnání se současným rámcem, který umožňuje adresovat žádosti příslušným orgánům v členském státě také zasláním řádně doložené žádosti, podkopává navrhované znění postavení subjektu údajů.

Čl. 29 odst. 1 stanoví, že právo na přístup, opravu a výmaz „se vykonává v souladu s právem členského státu, v němž se osoba uvedeného práva domáhá“, ale vůbec neodkazuje na pravomoci svěřené v této konkrétní záležitosti vnitrostátním orgánům pro ochranu údajů směrnicí (čl. 28 odst. 4: pravomoc kontrolovat vnitrostátní soubory údajů a úloha zajistit, aby zpracování a používání neporušovalo práva subjektů). Článek 31 uvádí úkol sledovat zákonnost zpracování „na jeho území“, ale není nic řečeno o zpracování „vnitrostátních“ údajů v CS-SIS ani o tom jak zajistit řádné sledování zákonnosti tohoto zpracování.

g) Úloha Komise

V SIS II hrají významnou úlohu Komise i členské státy. Členské státy je třeba považovat za správce. „Provozně-řídící“ úloha CS-SIS-II bude přidělena Komisi. Tato úloha není zcela jasná a měla by být specifikována. Jelikož povinnosti Komise nepochybně zahrnují alespoň organizaci,

[10] Článek 111 Schengenské úmluvy nestanoví v této souvislosti žádné omezení. Mělo by se také zohlednit, že informační politika zahájená schengenským společným dozorovým orgánem stanoví, že konzuláty dožádané země by měly vysvětlit, jak mohou subjekty údajů uplatňovat svá práva podle úmluvy.

uchovávání a zpřístupňování osobních údajů, které budou do SIS II vkládány, měla by být úloha Komise popsána co nejpodrobněji[11]. Sdílení odpovědností nesmí ohrozit základní zásady ochrany osobních údajů.

Zdá se, že znění předložených návrhů vylučuje možnost Komise zasahovat do operací zpracování údajů; veškerá zodpovědnost za vkládání údajů a zajištění kvality údajů spočívá výlučně na členských státech a práva subjektů údajů na přístup, opravu a výmaz údajů lze ze stejného důvodu vykonávat na vnitrostátní úrovni. Podobně je na členských státech, aby dotčené osoby informovaly o zpracování jejich údajů v SIS; pravidla dozoru a kontroly jsou pravidla stanovená vnitrostátními zákony.

h) Výkon dozoru

Jak již bylo zdůrazněno, současný schengenský systém kontroly ochrany údajů rozlišuje mezi vnitrostátním dozorem a dozorem nad centrální jednotkou SIS nezávislým společným dozorovým orgánem. Ve společném dozorovém orgánu jsou zastoupeny a hrají aktivní úlohu vnitrostátní dozorové orgány.

V novém právním základu pro SIS II zůstává dozor na vnitrostátní úrovni beze změn, zatímco na centrální úrovni nahradí společný dozorový orgán Evropský inspektor ochrany údajů.

Kontrola činností zpracování údajů Komise v technické architektuře SIS II, jak je definována v rozhodnutí i v nařízení, je svěřena Evropskému inspektorovi ochrany údajů.

Mechanismy pro dozor nad SIS II by měly být konzistentní s vývojem právních předpisů v oblasti ochrany údajů na úrovni EU.

Mělo by se velmi pečlivě provést porovnání dozorové činnosti společného dozorového orgánu s novými úkoly plánovanými pro Evropského inspektora ochrany údajů, aby případné nesrovnalosti neovlivnily současné úrovně dozoru a kontroly a aby se zaručila alespoň současná úroveň ochrany. Každý mechanismus by měl nejen zajistit účelný a účinný dohled, ale také úzkou spolupráci mezi všemi příslušnými zainteresovanými dozorovými orgány.

Návrhy předpokládají, že činnost schengenského společného dozorového orgánu bude postupně zastavena spolu se současnou odpovědností společného dozorového orgánu (zejména podle čl. 115

[11] Článek 2 směrnice 95/46/ES

odst. 3 Schengenské úmluvy) za „přezkoumávání obtíží při uplatňování nebo výkladu, které mohou vzniknout“, za „zkoumání obtíží, které mohou vzniknout při výkonu nezávislé kontroly prováděné vnitrostátními orgány pro ochranu údajů“, a za „vypracování harmonizovaných návrhů s cílem nacházet společná řešení stávajících obtíží“.

Pracovní skupina vítá ustanovení o úzké spolupráci mezi vnitrostátními dozorovými orgány a Evropským inspektorem ochrany údajů, ale domnívá se, že by tato spolupráce měla být alespoň lépe strukturovaná a vylepšená, aby se stala životaschopnou alternativou současného společného dozorového orgánu a vytvořila účinný systém společné kontroly.

Pokud jde o koordinaci kontrolních činností, mělo by být nadále možné, aby vnitrostátní dozorové orgány mohly provádět společné audity a vyměňovat si zjištění. V tomto kontextu by jako vzor mohl sloužit čl. 115 odst. 3 Schengenské úmluvy[12]. Navíc je nutná úzká spolupráce mezi Evropským inspektorem ochrany údajů a vnitrostátními orgány pro ochranu údajů.

V úvahu by také měla být vzata pracovní skupina navržená v nedávném návrhu rámcového rozhodnutí Komise o ochraně osobních údajů zpracovávaných v rámci policejní a soudní spolupráce v trestních věcech (KOM(2005) 475 v konečném znění).

Dále by se měl vzít v úvahu vývoj předpokládaný v Chartě základních práv EU i ve Smlouvě o Ústavě pro Evropu, který by měl nahradit rámec tří pilířů; tento rámec je považován za obzvlášť umělý, a tedy velmi obtížně srozumitelný, pokud jde o opatření, která se týkají základních práv jednotlivců, a o ochranná opatření, jež mají být vytvořena na ochranu těchto práv.

Měla by se věnovat pozornost úloze a úkolům přiděleným této pracovní skupině, jejímiž jsou vnitrostátní orgány pro ochranu údajů a Evropský inspektor ochrany údajů plnoprávnými členy.

Proto pracovní skupina navrhuje, že by se při této příležitosti měla potvrdit její úloha a kompetence s ohledem na dalekosáhlá rozhodnutí, která jsou v současnosti zdrojem sporných bodů.

i) Bezpečnostní opatření – vedení protokolů

[12] Čl. 115 odst. 3 Schengenské úmluvy: „Společný kontrolní orgán je rovněž příslušný pro přezkoumávání obtíží při uplatňování nebo výkladu v souvislosti s provozováním Schengenského informačního systému, pro zkoumání obtíží, které mohou vzniknout při výkonu nezávislého dozoru prováděného vnitrostátními dozorovými orgány smluvních stran nebo při výkonu práva na přístup do systému, jakož i pro vypracování harmonizovaných návrhů s cílem nacházet společná řešení stávajících obtíží.“

Je potřeba odkázat na úvahy obsažené ve stanovisku pracovní skupiny k VIS (potřeba uživatelských profilů, uživatelských identifikátorů, vlastní kontroly atd.).

j) Kopie údajů (čl. 4 odst. 3)

Je stanovena možnost zpracování všech záznamů SIS ve vnitrostátní kopii CS-SIS spíše než přímého přístupu k CS-SIS.

V současnosti postup kopírování neumožňuje oddělení záznamů pořízených podle nařízení za účelem odepření vstupu od jiných typů záznamů.

Pracovní skupina souhlasí s úvahami Evropského inspektora ochrany údajů v jeho stanovisku ve smyslu, že potřeba „vnitrostátních kopií" není adekvátně odůvodněna a ve skutečnosti vede k mnohonásobnému počtu přístupových bodů; oprávnění používat údaje, aniž by byla stanovena adekvátní ochranná opatření v souvislosti se způsoby a prostředky přístupu k nim, navíc ještě dále ztěžuje dozorčí a kontrolní úkoly, které mají být v této oblasti vykonávány.

k) Provádění ustanovení a sledování fungování SIS II

Oba návrhy předpokládají, že Komise může pro technické specifikace potřebné k provádění složitého rámce, který se navrhuje, využít postupy projednávání ve výborech.

Některé záležitosti, kterými se mají zabývat jednotlivé výbory, však mohou mít dopad na práva jednotlivců. Například lze poukázat na pravidla vkládání a zpracování biometrických údajů v systému.

Článek 36 návrhu rozhodnutí, který se zabývá výměnou osobních údajů, jež mohou mít k předmětům, o kterých je pořízen záznam, pouze nepřímý vztah (jako údaje o osobě, která koupila odcizenou věc v dobré víře), nechává navíc přípravu prováděcích pravidel pro výměnu těchto osobních údajů jakožto doplňujících informací na regulačním výboru.

Pracovní skupina opakuje svou žádost, jak již učinila ve stanovisku k VIS, aby se uvedený výbor zabýval pouze otázkami, které s sebou nenesou žádné důsledky pro jednotlivce v podobě dopadu na úroveň ochrany povolenou nařízením i rozhodnutím podle obecných zásad, na které se odkazuje v úvodu. Posledně uvedené aspekty by měly být nadále regulovány adekvátními legislativními

opatřeními a mělo by být zřetelně stanoveno, že v každém případě budou adekvátně zastoupeny a konzultovány dozorové orgány SIS II.

Pokud jde o sledování provádění různých ustanovení a jejich dopadu, což je úkol svěřený podle současných návrhů Komisi, pracovní skupina se domnívá, že je také nutné sledovat dopad nového regulačního rámce na základní lidská práva a na ochranu osobních údajů.

Tato část monitorovací zprávy by měla být zpracována ve shodě s orgány pro ochranu údajů na základě zkušeností s prováděním, které budou shromážděny.

ZÁVĚRY A KONEČNÁ DOPORUČENÍ

Pracovní skupina si uvědomuje, že návrhy předložené Komisí s sebou nesou důkladnou reorganizaci SIS zejména proto, že se pro operace zpracování vykonávané v SIS nebo jeho prostřednictvím předpokládají různé právní základy podle toho, zda spadají do rozsahu působnosti nových pravomocí Společenství (přistěhovalectví a azyl), v kterémžto případě by se referenčním měřítkem stala směrnice 95/46/ES, nebo budou nadále zahrnuty do jiných kategorií údajů či operací tzv. třetího pilíře. Komise dále předpokládá jiný typ architektury SIS, podle které by byla vytvořena centralizovaná databáze, do níž by informace – tj. záznamy a další údaje podle návrhů – měly být vkládány přímo přes vnitrostátní rozhraní neobsahující žádné údaje (na rozdíl od současných vnitrostátních rozhraní SIS, tj. N-SIS).

Pracovní skupina se zvlášť obává případného ohrožení práv dotčených jednotlivců zejména proto, že ustanovení o ochraně údajů uvedená v návrhu nařízení (a rozhodnutí) se nejeví plně v souladu s ustanoveními stanovenými v referenční směrnici.

Zejména:

ÚČEL SIS II A PŘÍSTUP K SIS II

Je nutné držet se přísného používání zásady stanovení účelu v nařízení, která policejním orgánům neumožňuje systematický přístup. Dále by měla být stanovena konzistentní pravidla týkající se dalších orgánů, kterým má být umožněn přístup k systému, a před přidáním nových funkcí k systému by se měly řádně zvážit zásady minimalizace údajů a proporcionality – zejména pokud jde o zahrnutí biometrických údajů a propojení záznamů. V každém případě je pracovní skupina

toho názoru, že předpokládaná možnost přenosu informací SIS II na třetí strany nebo orgány se nezdá být v souladu s účely systému tak, jak je v současnosti konfigurován.

NOVÉ KATEGORIE ÚDAJŮ: BIOMETRIE

Pracovní skupina by odkázala na stanoviska, která již k biometrii vydala, zejména na stanovisko 7/2004 o zařazení biometrických prvků do víz a povolení k pobytu a na nedávné stanovisko k VIS. Používání biometrie k identifikačním účelům musí být přísně omezeno na zvláštní případy, kde jsou tyto informace skutečně nezbytné, včetně případů, které jsou v zájmu subjektu údajů (tj. falešná totožnost, přezdívky). Pracovní skupina zdůrazňuje potřebu stanovit okolnosti a účely, které umožňují vyhledávání biometrických údajů, a poskytnout příslušné záruky ze zákona, aby se omezilo nebo snížilo riziko užívání údajů pro jiné účely, než bylo původně zamýšleno („function creep“).

PROPOJENÍ ZÁZNAMŮ

Možnost vytvářet „vztahy mezi dvěma nebo více záznamy“ musí být pečlivě posouzena podle zásady omezení účelu. Nařízení by mělo zavést prováděcí ochranná opatření pro používání těchto propojení a omezit přístup na oprávněné členy příslušných orgánů za účelem plnění jejich úkolů.

PRÁVO NA INFORMACE, PŘÍSTUP, OPRAVU A VÝMAZ

- návrh nařízení by měl výslovně stanovit, aby informace byly poskytnuty dříve než je přijato opatření, které vede k vložení záznamu do SIS.

- informace musí výslovně uvádět možnost zpochybnit rozhodnutí o vložení záznamu do systému a musí obsahovat adresu vnitrostátního dozorového orgánu pro ochranu údajů.

- v návrhu nařízení by měla být stanovena jasná jednotná pravidla, jak mohou subjekty údajů vykonávat práva na přístup, zejména by měla označovat případy, kdy může být přístup k informacím odepřen.

- subjektům údajů by také mělo být umožněno podávat stížnosti, když nejsou fyzicky přítomny na území příslušného členského státu. V textu by měl být zahrnut odkaz na pravomoci svěřené vnitrostátním orgánům pro ochranu údajů, pokud jde o uplatňování opravných prostředků.

Čl. 15 odst. 3 nařízení dává jednotlivcům právo požadovat přezkoumání rozhodnutí pořídit záznam učiněné správním orgánem nebo odvolat se, ale není zde řečeno nic o jakékoliv odpovídající povinnosti informovat uvedenou osobu, když je takovýto záznam pořízen, ani o postupu při výkonu uvedeného práva. Pracovní skupina toto ustanovení vítá, ale je toho stanoviska, že aby bylo účinné, měl by návrh nařízení výslovně stanovit, že informace musí být poskytnuty, nejpozději když je přijato opatření vyplývající z vložení záznamu do SIS.

UCHOVÁVÁNÍ ÚDAJŮ

Pracovní skupina by si přála, aby nařízení výslovně stanovilo kratší dobu pro přezkoumání záznamů, aby se zajistilo, že osobní údaje lze vymazat, když již nebudou zapotřebí. Delší doba uchovávání záznamů navrhovaná Komisí by navíc měla být lépe odůvodněna.

DOZOR

Aniž by byla dotčena rozhodnutí, která se v současnosti přijímají za účelem zajištění ochrany osobních údajů v záležitostech třetího pilíře, a ve světle předchozích úvah o této otázce je nutné mít jasné předpisy o úloze a povinnostech všech zainteresovaných dozorových orgánů.

Pracovní skupina by ráda upozornila na svou úlohu a úkoly a navrhuje, aby při této příležitosti byly její úloha a kompetence potvrzeny s ohledem na současná dalekosáhlá sporná rozhodnutí.

Pracovní skupina věří, že úvahy uvedené v jejím stanovisku budou řádně zohledněny.

V Bruselu dne 25. listopadu 2005

Za pracovní skupinu

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: info@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