



VĚSTNÍK

ÚŘADU PRO OCHRANU OSOBNÍCH ÚDAJŮ

2010

Částka 56

8. září 2010

Cena 168,- Kč

OBSAH

Úvod	3170
I. Registrace	
Přehled zrušených registrací za období od 22. 4. 2010 do 24. 8. 2010	3171
II. Sdělení Úřadu	
a) Úřad pro ochranu osobních údajů k problémům z praxe – č. 3/2010: K použití fotografie, obrazového a zvukového záznamu fyzické osoby	3172
b) Úřad pro ochranu osobních údajů k problémům z praxe – č. 4/2010: Zveřejňování osobních údajů na internetu	3174
c) Z rozhodovací činnosti Úřadu:	
1. Povinnost mlčenlivosti zaměstnanců orgánů sociálně-právní ochrany dětí	3176
2. Subsidiarita trestněprávní represe	3176
3. Zveřejňování rozsudku	3176
4. Povinnost zabezpečit osobní údaje, zproštění odpovědnosti	3178
5. Zveřejňování osobních údajů žadatelů o informace	3179
6. Zveřejňování citlivých údajů v médiích	3179
7. Zpracování osobních údajů v Národní databázi DNA	3181
8. Zveřejňování osobních údajů studentů	3183
d) Závěry jednání Konference evropských komisařů ochrany dat a soukromí v Praze (29. – 30. dubna 2010):	3184
1. Rezoluce k používání tělesných skenerů (body scanners) pro účely bezpečnosti na letištích	3184
2. Rezoluce k chystané dohodě mezi Evropskou unií a Spojenými státy americkými o standardech ochrany osobních údajů v oblasti policie a soudní spolupráce v trestních věcech	3185
3. Rezoluce k problematice dalšího vývoje v oblasti ochrany osobních údajů a soukromí	3185
4. Rezoluce o přípravě společných kroků zaměřených na informovanost a vzdělávání mladých lidí na evropské a mezinárodní úrovni	3186
e) Stanovisko č. 8/2009 Pracovní skupiny pro ochranu údajů podle článku 29 směrnice 95/46/ES (WP29) k problematice ochrany údajů o cestujících shromažďovaných a zpracovávaných bezcelními prodejnami na letištích a v přístavech (WP 167, 02318/09/CS); (Překlad pořízený Evropskou komisí, přetisk v původní podobě)	3188
f) Stanovisko č. 1/2010 Pracovní skupiny pro ochranu údajů podle článku 29 směrnice 95/46/ES (WP29) k pojmům „správce“ a „zpracovatel“ (WP 169, 00264/10/CS); (Překlad pořízený Evropskou komisí, přetisk v původní podobě)	3195

ÚVOD

Padesátá šestá částka Věstníku Úřadu pro ochranu osobních údajů obsahuje přehled zrušených registrací v období od 22. 4. 2010 do 24. 8. 2010.

Rubrika Sdělení Úřadu přináší v oddíle K problémům z praxe dva materiály. Prvním je dokument „K použití fotografie, obrazového a zvukového záznamu fyzické osoby“, který řeší otázku, jak přistupovat k použití a šíření fotografií, případně audiovizuálních záznamů fyzických osob z hlediska zpracování citlivých údajů. Druhý dokument nazvaný „Zveřejňování osobních údajů na internetu“ se zabývá problematikou ochrany práv uživatelů internetu, zejména práv spojených s ochranou osobnosti a soukromí. Je nepochybné, že osobní informace zveřejněné prostřednictvím internetu (bez ohledu na jejich pravdivost) mají obrovský potenciál zasáhnout dotčenou osobu v mnoha sférách jejího života. Proto je důležité si klást otázku, zda a jakými prostředky lze ochranu soukromí v prostředí internetu chránit.

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

Součástí Sdělení je také informace o Konferenci evropských komisařů ochrany dat a soukromí, která se konala v Praze ve dnech 29. – 30. dubna 2010. V příspěvku jsou publikovány čtyři rezoluce prezentující závěry a výsledky spolupráce delegátů konference.

Rubriku Sdělení Úřadu uzavírají dva dokumenty Pracovní skupiny pro ochranu dat podle článku 29 (WP29) směrnice 95/46/ES. Jsou jimi „Stanovisko 8/2009 k problematice ochrany údajů o cestujících shromažďovaných a zpracovávaných bezcelními prodejny na letištích a v přístavech“ a „Stanovisko 1/2010 k pojmům správce a zpracovatel“. Úřad přejímá oficiální překlady právně nezávazných dokumentů WP29 v jejich původní podobě.

Přehled zrušených registrací

Číslo registrace	Subjekt	Datum zrušení
00000485/001	BENEŠOVÁ ZOJA	11.05.2010
00001417/001	VODOVODY A KANALIZACE JIŽNÍ ČECHY, A.S.	25.06.2010
00001417/002	VODOVODY A KANALIZACE JIŽNÍ ČECHY, A.S.	25.06.2010
00001417/003	VODOVODY A KANALIZACE JIŽNÍ ČECHY, A.S.	25.06.2010
00002986/002	HSBC BANK PLC - POBOČKA PRAHA	07.05.2010
00002986/006	HSBC BANK PLC - POBOČKA PRAHA	07.05.2010
00004771/004	MĚSTO ČESKÁ TŘEBOVÁ	10.07.2010
00004840/005	PIVOVARY STAROPRAMEN A.S.	04.06.2010
00004840/009	PIVOVARY STAROPRAMEN A.S.	04.06.2010
00004840/011	PIVOVARY STAROPRAMEN A.S.	01.06.2010
00023155/001	ACTELION PHARMACEUTICALS LTD.ORGANIZAČNÍ SLOŽKA	02.07.2010
00025217/012	CZECH COAL SERVICES A.S.	21.08.2010
00025217/013	CZECH COAL SERVICES A.S.	21.08.2010
00025217/014	CZECH COAL SERVICES A.S.	21.08.2010
00025217/015	CZECH COAL SERVICES A.S.	21.08.2010
00025217/016	CZECH COAL SERVICES A.S.	21.08.2010
00026451/008	SCHENKER SPOL.S R.O.	24.08.2010
00030484/001	ČESKÁ NÁRODNÍ ZDRAVOTNÍ POJIŠŤOVNA	03.06.2010
00030484/002	ČESKÁ NÁRODNÍ ZDRAVOTNÍ POJIŠŤOVNA	03.06.2010
00030484/003	ČESKÁ NÁRODNÍ ZDRAVOTNÍ POJIŠŤOVNA	03.06.2010
00031690/003	ČD - TELEMATIKA A.S.	20.05.2010
00033034/001	DRINKS UNION A. S.	08.07.2010
00033034/002	DRINKS UNION A. S.	08.07.2010
00033034/003	DRINKS UNION A. S.	08.07.2010
00033034/004	DRINKS UNION A. S.	08.07.2010
00033034/005	DRINKS UNION A. S.	08.07.2010
00034889/001	SITRONICS TELECOM SOLUTIONS, CZECH REPUBLIC A.S.	09.07.2010
00035620/001	TOP WOOD WINDOWS A.S.	06.05.2010
00035851/001	O' NEILL LENKA ISABELLA	19.05.2010

II. SDĚLENÍ ÚŘADU

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ K PROBLÉMŮM Z PRAXE

č. 3/2010

červen 2010

K použití fotografie, obrazového a zvukového záznamu fyzické osoby

K častým dotazům adresovaným Úřadu pro ochranu osobních údajů patří otázka, jak přistupovat k používání a šíření fotografií případně audiovizuálních záznamů fyzických osob z hlediska zpracování citlivých údajů, pro které zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, stanoví přísnější režim.

Je zřejmé, že portrétní fotografie vypovídá o rasovém nebo etnickém původu zobrazené osoby, oblečení nebo pokrývka hlavy může vypovídat o náboženství apod. Fotografie nebo jiný obrazový záznam fyzické osoby je dokumentem osobní povahy, který mimo jiné obsahuje biometrické i jiné charakteristiky subjektu údajů, které vypovídají o skutečnostech definovaných v § 4 písm. b) zákona o ochraně osobních údajů jako citlivý údaj, a může být proto jako nosič informací zdrojem pro zpracování citlivých údajů.

Jestliže jsou však informace z fotografie subjektu údajů používány pro pouhé rozlišení jeho podoby ve srovnání s jinými osobami a tyto informace nejsou dále zpracovávány, nelze takové používání fotografií posuzovat jako zpracování citlivých osobních údajů.

Obdobné stanovisko zastává i Pracovní skupina pro ochranu údajů zřízená podle článku 29 směrnice Evropského parlamentu a Rady 95/46/ES, která ve svém stanovisku č. 5/2009 k internetovým sociálním sítím, v bodě 3.4 citlivé údaje, konstatuje, že „pracovní skupina obecně nepovažuje snímky na internetu za citlivé údaje, nejsou-li snímky jednoznačně použity k odhalení citlivých údajů o fyzických osobách“. (Věstník Úřadu pro ochranu osobních údajů, částka 54, str. 3124.)

K pořizování, používání, šíření či zveřejňování fotografií či jiných záznamů fyzických osob nebo skupin osob může docházet bez prvku systematickosti – v režimu zákona č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů,¹ nebo tyto dokumenty jako nosiče informací vstupují do systematicky prováděných operací s osobními údaji, které podléhají režimu zákona o ochraně osobních údajů jako zpracování osobních údajů. V obou případech je klíčové, zda fyzická osoba (subjekt údajů) sama ze své vůle používá (šíří, zveřejňuje) svou vlastní fotografii nebo záznam, nebo se jedná i o fotografie či záznamy jiných

osob. Při používání a šíření fotografií a audiovizuálních záznamů fyzických osob je zejména třeba brát v úvahu, zda dochází k jejich zveřejňování na internetu, kde je zvýšené nebezpečí jejich zneužití.

Pro pořízení a použití fotografie a rovněž obrazového nebo zvukového záznamu fyzické osoby je tedy třeba rozlišovat trojí zákonem stanovený režim:

1. Pořízení a následné použití jednotlivých fotografií nebo časově omezeného obrazového nebo zvukového záznamu projevu fyzické osoby (skupiny osob) – jednání, schůze, jiné akce:

- a) Svolení fyzické osoby podle § 12 odst. 1 občanského zákoníku;
- b) Bez svolení fyzické osoby podle § 12 odst. 2 občanského zákoníku k účelům úředním na základě zákona;
- c) Bez svolení fyzické osoby podle § 12 odst. 3 občanského zákoníku pro vědecké a umělecké účely a pro tiskové, filmové, rozhlasové a televizní zpravodajství.

2. Systematicky prováděné operace s fotografiemi nebo obrazovými a zvukovými záznamy projevů fyzických osob v datových souborech nebo systematické monitorování prostoru kamerovým systémem se shromažďováním údajů o osobách do tohoto prostoru vstupujících, za účelem rozlišení podoby fyzické osoby od ostatních subjektů údajů, aniž by byl stanoven účel zpracovávat rovněž údaje citlivé:

- a) Souhlas subjektu údajů podle § 5 odst. 2 zákona o ochraně osobních údajů;
- b) Zpracování bez souhlasu subjektu údajů podle § 5 odst. 2 písm. a) zákona o ochraně osobních údajů stanovené zvláštním zákonem;
- c) Zpracování bez souhlasu subjektu údajů podle § 5 odst. 2 písm. e) zákona o ochraně osobních údajů, pokud je to nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby.

3. Systematicky prováděné operace s fotografiemi nebo jinými záznamy projevů fyzických osob v datových souborech nebo systematické monitorování prostoru kamerovým systémem se shromažďováním údajů o osobách do tohoto prostoru vstupujících za účelem

zpracování citlivých údajů na základě informací na fotografii nebo záznamu uložených:

- a) Výslovný souhlas subjektu údajů podle § 9 písm. a) zákona o ochraně osobních údajů;
- b) Zpracování bez výslovného souhlasu podle § 9 písm. b) zákona o ochraně osobních údajů, je-li to nezbytné v zájmu zachování života nebo zdraví subjektu údajů nebo jiné osoby nebo odvrácení bezprostředního závažného nebezpečí hrozícího jejich majetku, pokud není možno jeho souhlas získat zejména z důvodů fyzické, duševní či právní nezpůsobilosti, v případě, že je nezvěstný nebo z jiných podobných důvodů. Správce musí ukončit zpracování údajů, jakmile pominou uvedené důvody, a údaje musí zlikvidovat, ledaže by subjekt údajů dal k dalšímu zpracování souhlas;
- c) Zpracování bez výslovného souhlasu subjektu údajů podle § 9 písm. i) zákona o ochraně osobních údajů a podle zvláštních zákonů při předcházení, vyhledávání, odhalování trestné činnosti, stíhání trestných činů a pátrání po osobách.

Závěr

Pořizování a používání fotografií a záznamů podle bodu 1. není zpracováním osobních údajů ve smyslu § 4 písm. e) zákona o ochraně osobních údajů, proto nepodléhá oznamovací povinnosti podle § 16 tohoto zákona. Této povinnosti, s výjimkou zpracování pro osobní potřebu podle § 3 odst. 3 zákona o ochraně osobních údajů, zpravidla podléhá zpra-

cování osobních údajů podle bodu 2. a), 3 b) a v případě monitorování prostoru kamerovým systémem se záznamem i podle bodu 2. c). V případě zpracování podle bodu 3 a) vzniká otázka legitimacy účelu takového zpracování a při splnění oznamovací povinnosti i případného nepovolení takového zpracování podle § 17 odst. 2 zákona o ochraně osobních údajů. Zákonem stanovené zpracování osobních údajů podle bodu 2. b) a 3. c) oznamovací povinnosti nepodléhá ve smyslu § 18 odst. 1 písm. b) zákona o ochraně osobních údajů.

Poznámka:

¹ Zákon č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů

§ 12

(1) Písemnosti osobní povahy, podobizny, obrazové snímky a obrazové a zvukové záznamy týkající se fyzické osoby nebo jejích projevů osobní povahy smějí být pořízeny nebo použity jen s jejím svolením.

(2) Svolení není třeba, použijí-li se písemnosti osobní povahy, podobizny, obrazové snímky nebo obrazové a zvukové záznamy k účelům úředním na základě zákona.

(3) Podobizny, obrazové snímky a obrazové a zvukové záznamy se mohou bez svolení fyzické osoby poříditi nebo použít přiměřeným způsobem též pro vědecké a umělecké účely a pro tiskové, filmové, rozhlasové a televizní zpravodajství. Ani takové použití však nesmí být v rozporu s oprávněnými zájmy fyzické osoby.

² Materiál je také k dispozici na internetové adrese Úřadu www.uoou.cz v sekci Názory Úřadu/K problémům z praxe.

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ K PROBLÉMŮM Z PRAXE

č. 4/2010

červenec 2010

Zveřejňování osobních údajů na internetu

Úvod

V souvislosti s tím, jak se internet stále více stává neodmyslitelnou součástí naší společnosti jako významný komunikační prostředek, vyvstávají také otázky spojené s ochranou práv jeho uživatelů, zejména práv spojených s ochranou osobnosti a soukromí. Je nepochybné, že osobní informace zveřejněné prostřednictvím internetu (bez ohledu na jejich pravdivost) mají obrovský potenciál zasáhnout dotčenou osobu v mnoha sférách jejího života, tedy jak v rodinném, tak i v pracovním či veřejném životě. Je proto na místě klást si otázku, zda a jakými prostředky lze ochranu soukromí v prostředí internetu chránit.

Ochrana osobnosti a soukromí je v České republice ústavně zakotvenou hodnotou (viz čl. 10 Listiny základních práv a svobod). Historicky spadá především do soukromoprávní kategorie práv, tedy do oblasti, kde jsou práva osob chráněna soudy v občanském soudním řízení v návaznosti na konkrétní žalobu. Nicméně pro určité oblasti, v nichž by zásah do práv představoval zvýšené riziko pro celospolečenské hodnoty, zákonodárce (obvykle pod vlivem společenského vývoje a mezinárodních dokumentů) rozhodl, že je důvodné poskytovat ochranu veřejnoprávní cestou, tj. formou státního zásahu. Zákonem provedení zmíněného čl. 10 Listiny základních práv a svobod tak lze nalézt jak v Občanském zákoníku (ochrana osobnosti podle § 11 až § 16), tak v Trestním zákoně (trestný čin neoprávněného nakládání s osobními údaji podle § 180) a v neposlední řadě i v zákoně č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.¹

Žádný z uvedených právních předpisů *a priori* nevylučuje ze své působnosti oblast internetu – je tedy nutno vycházet z toho, že i přes svobodu a volnost, které jsou základními atributy tohoto media, ani zde není právní vakuum umožňující zcela libovolné jednání.

Působnost zákona č. 101/2000 Sb.

V případě zákona č. 101/2000 Sb. je zmíněná veřejnoprávní regulace – realizovaná prostřednictvím Úřadu pro

ochranu osobních údajů (dále jen „Úřad“) – opodstatněna zájmem na ochraně osob před riziky spojenými se zneužitím shromážděných osobních údajů.² Hranice působnosti zákona č. 101/2000 Sb. jsou vymezeny v jeho § 3, dle kterého je státní zásah opodstatněný v situaci, kdy dochází k určitému systematickému (cílenému) využívání osobních údajů, které neslouží výhradně pro osobní potřeby fyzických osob.

Při aplikaci zákona č. 101/2000 Sb. je dále třeba přihlížet k předpisům komunitárního práva, konkrétně směrnici Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně jednotlivců v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen „směrnice“), kterou zákon č. 101/2000 Sb. provádí, a také k související judikatuře Evropského soudního dvora. Směrnice, s ohledem na dobu vzniku, neupravuje výslovně otázku zpracování (zveřejňování) osobních údajů na internetu, nicméně konstatuje, že do působnosti Směrnice spadá především automatizované zpracování dat – tj. zpracování s pomocí výpočetní techniky. Tento fakt je třeba vnímat jako základní východisko k závěru, že ani oblast internetu není *a priori* z působnosti směrnice (a tedy i zákona č. 101/2000 Sb.) vyloučena. Další vodítko poskytuje judikatura Evropského soudního dvora, ze které lze především zmínit rozhodnutí zn. C-101/01 ze dne 6. listopadu 2003 (tzv. případ Lindqvist). Podle tohoto rozhodnutí se Směrnice, a tedy pravidla v ní stanovená pro zpracování osobních údajů, uplatní v případech, kdy jsou prostřednictvím webových stránek zveřejňovány informace týkající se určité skupiny osob.³

Dalším vodítkem při aplikaci zákona č. 101/2000 Sb. je judikatura Ústavního soudu České republiky týkající se principu tzv. *ultima ratio* trestní represe⁴, kterou je nutno zohlednit nejen v oblasti trestního práva, ale i při správním trestání (tedy při trestání za správní delikty definované v zákoně č. 101/2000 Sb.). Ústavní soud ve svých nálezech opakovaně zdůrazňuje, že prostředky trestního práva (a analogicky tedy i správního trestání) lze využít pouze tehdy, pokud užití

¹ Otázka zveřejňování osobních údajů na internetu může v některých případech podléhat i dalším právním předpisům, např. zákonu č. 45/1995 Sb., o regulaci reklamy, zákonu č. 231/2001 Sb., o provozování rozhlasového a televizního vysílání, nebo zákonu č. 480/2004 Sb., o některých službách informační společnosti.

² Osobním údajem je ve smyslu § 4 písm. a) zákona č. 101/2000 Sb. každá informace vztahující se ke konkrétní fyzické osobě.

³ V uvedeném případě byly zveřejněny informace o osobách působících na farnosti, včetně jejich jména (úplného či jen křestního), popisu jejich funkce a zálib. V několika případech byl zmíněn i rodinný stav těchto osob, telefonní číslo a další informace (rozsudek viz <http://curia.europa.eu>).

⁴ Viz např. nálezy Ústavního soudu sp. zn. IV. ÚS 469/02, I. ÚS 4/04 nebo I ÚS 541/10.

jiných (soukromoprávních) prostředků ochrany nepřichází v úvahu nebo by bylo jejich využití zjevně neúčelné. Dle názoru Ústavního soudu lze trestněprávní kvalifikaci určitého jednání považovat až za krajní právní prostředek, který má své opodstatnění pouze v případě ochrany základních společenských hodnot.

Z uvedených východisek je zřejmé, že aplikace zákona č. 101/2000 Sb. na prostředí internetu, které slouží obvykle k realizaci soukromoprávních aktivit, je omezená, nikoli však vyloučená. Při naplnění podmínek uvedených v § 3 tohoto zákona a zachování uvedeného principu *ultima ratio*, je i zveřejňování osobních údajů na internetu postižitelné prostřednictvím zákona č. 101/2000 Sb. Jinými slovy pro zpracování (tedy zejména zveřejňování) osobních údajů na internetu neplatí a priori žádná výjimka a Úřad je kompetentní posoudit každý případ a rozhodnout, zda došlo k jednání, které zákon č. 101/2000 Sb. reguluje či nikoli. Skutečnost, že se ne vždy bude jednat o zpracování osobních údajů podléhající uvedenému zákonu, anebo že nebude vždy možné dohledat odpovědnou osobu (tj. z hlediska zákona č. 101/2000 Sb. správce či zpracovatele osobních údajů), neznamená, že zde není dána působnost Úřadu, anebo že lze rezignovat na aplikaci zákona č. 101/2000 Sb. v této oblasti.

Příklady z praxe

Co se týče zpracování osobních údajů na internetu, Úřad se ve své dosavadní praxi zabýval zejména případy, kdy došlo např. ke zveřejnění seznamu dlužníků (tzv. černé listiny neboli black listu) na webových stránkách obchodních

společností, podnikajících osob či obcí. Dále Úřad posuzoval případy zveřejnění osobních údajů zaměstnanců, ať již v souvislosti s pracovněprávním sporem nebo vyhlášením konkurzního řízení. Úřad se velmi často zabývá také zveřejněním osobních údajů v rámci dokumentů pocházejících z činnosti obcí či měst (blíže viz stanovisko Úřadu č. 2/2004 a text K problémům z praxe č. 1/2010).

Ve všech výše uvedených případech dospěl Úřad k závěru, že podmínky pro aplikaci zákona č. 101/2000 Sb. jsou naplněny a posuzoval tedy zjištěný stav z hlediska plnění povinností tímto zákonem stanovených, zejména povinnosti zpracovávat osobní údaje pouze na základě zákonem předvidaného právního titulu dle § 5 odst. 2 zákona č. 101/2000 Sb. a základních povinností vyjádřených v § 5 odst. 1 tohoto zákona (např. povinnosti zpracovávat osobní údaje pouze v souladu s původním účelem).

Naopak mimo působnost zákona č. 101/2000 Sb. budou obvykle jednotlivé informace publikované v rámci blogů, zájmových webových stránek, nejrůznějších diskuzí anebo sociálních sítí. Uvedené neznamená, že by zveřejněním nějaké osobní informace touto cestou nemohlo dojít k zásahu do osobnostních práv, nicméně s ohledem na výše uvedená východiska nebude ve většině takových případů opodstatněný veřejnoprávní zásah ze strany Úřadu. Dotčené osoby se nicméně mohou svých práv domoci cestou občanského soudního řízení.

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

Z rozhodovací činnosti Úřadu

Sdělení úvodem:

Úřad pro ochranu osobních údajů se prostřednictvím následující stručné charakteristiky vyjadřuje k některým problematickým okruhům případů porušování povinností při zpracování osobních údajů projednávaných Úřadem v rámci své rozhodovací činnosti.

1. Povinnost mlčenlivosti zaměstnanců orgánů sociálně-právní ochrany dětí

Podle § 52 odst. 1 zákona č. 359/1999 Sb., o sociálně-právní ochraně dětí, jsou zaměstnanci orgánu sociálně-právní ochrany a zaměstnanci obce s rozšířenou působností zařazení do obecního úřadu oprávněni v souvislosti s plněním úkolů podle tohoto zákona navštěvovat dítě a rodinu, ve které žije, v obydlí a zjišťovat v místě bydliště dítěte, ve škole a ve školském zařízení, ve zdravotnickém zařízení, v zaměstnání nebo v jiném prostředí, kde se dítě zdržuje, jak rodiče nebo jiné osoby odpovědné za výchovu dítěte o dítě pečují, v jakých sociálních podmínkách dítě žije a jaké má dítě chování. Sociálně-právní ochranou se poté dle § 1 odst. 1 zákona č. 359/1999 Sb. rozumí také ochrana práva dítěte na příznivý vývoj. Podle § 57 odst. 1 jsou poté zaměstnanci orgánu sociálně-právní ochrany, zaměstnanci obce s rozšířenou působností zařazení do obecního úřadu povinni zachovávat mlčenlivost o skutečnostech, se kterými se při provádění sociálně-právní ochrany nebo v přímé souvislosti s tím seznámili.

Je tedy zřejmé, že zákon č. 359/1999 Sb. ukládá zaměstnancům povinnost mlčenlivosti (ta ostatně vyplývá také z § 15 odst. 1 zákona č. 101/2000 Sb.). Současně je ale třeba konstatovat, že sdělení takových údajů, které jsou nezbytné při provádění a plnění úkolů sociálně-právní ochrany dle zákona č. 359/1999 Sb., tedy např. při šetření v rodině, u lékaře atd. nelze a priori považovat za porušení povinnosti mlčenlivosti. Je nepochybné, že bez využití určitého množství údajů při vlastním šetření by nebylo možné dosáhnout cílů zákona č. 359/1999 Sb., tedy ochrany práv dítěte. Jinými slovy lze tedy shrnout, že při provádění úkonů dle zákona č. 359/1999 Sb. se zaměstnanec orgánu sociálně-právní ochrany nebo obecního úřadu nemůže dopustit porušení povinnosti mlčenlivosti, pokud pracuje s údaji, které se týkají jím prověřované věci. (čj. VER-6219/08-7)

2. Subsidiarita trestněprávní represe

Ze shromážděné dokumentace vyplývá, že jednání popsané v podání oznamovatele není důvodem pro zahájení řízení o přestupku, protože dle názoru správního orgánu se pan XY dopustil jednání, které má výhradně soukromoprávní základ. V daném případě nedošlo k žádnému zveřejnění záznamů a kamery snímaly pouze konkrétní osoby a jejich soukromé

pozemky, záznamy byly přístupné pouze osobě XY. Jak vyplývá z nálezu Ústavního soudu zn. I. ÚS 4/04 ze dne 23. března 2004 „trestní právo a trestněprávní kvalifikace určitého jednání, které má soukromoprávní základ, jako trestného činu je třeba považovat za ultima ratio, tedy za krajní právní prostředek, který má význam především celospolečenský, tj. z hlediska ochrany základních společenských hodnot. V zásadě však nemůže sloužit jako prostředek nahrazující ochranu práv a právních zájmů jednotlivce v oblasti soukromoprávních vztahů, kde závisí především na individuální aktivitě jednotlivce, aby střežil svá práva, jimž má soudní moc poskytnout ochranu. Je však nepřijatelné, aby tuto ochranu aktivně přebíraly orgány činné v trestním řízení, jejichž úkolem je ochrana převážně celospolečenských hodnot, nikoliv přímo konkrétních subjektivních práv jednotlivce, jež svou povahou spočívají v soukromoprávní sféře“.

Úřad pro ochranu osobních údajů proto dospěl k závěru, že je zde namísto aplikace občanskoprávní ochrany osobnosti dle zákona č. 40/1964 Sb., občanského zákoníku, který v § 12 upravuje problematiku pořizování obrazových záznamů týkajících se fyzické osoby, před správním postihem. Pasivita jednotlivce při ochraně jeho práv, či nedostatečná účinnost zákonných nástrojů sloužících k ochraně subjektivních práv osob, nemůže vést k tomu, aby byla tato opatření nahrazována či doplňována prostředky práva trestního resp. správního. (čj. SPR-6381/08-2)

3. Zveřejňování rozsudku

Informace uvedené v rozsudku Obvodního soudu Z, stejně tak jako v protokole o jednání před Obvodním soudem Z, jsou osobními údaji ve smyslu § 4 písm. a) zákona č. 101/2000 Sb., neboť se dají vztáhnout k určitelným osobám. Správní orgán v této souvislosti podotýká, že osobními údaji nejsou jenom identifikační údaje uvedené v označení účastníků v rozsudku, resp. protokolu o jednání, ale také výrok rozsudku a informace v těch částech odůvodnění rozsudku, které popisují skutková zjištění, resp. všechny další informace zjištěné např. z listinných důkazů (pracovní smlouvy paní XY). Operace prováděné s těmito osobními údaji (tzn. jejich uchování, použití, zpřístupnění) poté dle správního orgánu naplňují pojmové znaky zpracování dle § 4 písm. e) zákona č. 101/2000 Sb., neboť jsou přímo spojeny s pracovněprávním vztahem (případně jiným právním vztahem) mezi účastníkem řízení a paní XY v rámci kterých (a v souladu s takto vymezeným účelem) účastník řízení již dříve zpracovával jejich osobní údaje; předmětné zpřístupnění osobních údajů uvedených v rozsudku (protokole) je tedy pouze další, navazující fází tohoto zpracování.

V souladu se shora uvedeným lze dále konstatovat, že zaslání dokumentu obsahující osobní údaje elektronickou

poštou, resp. její vystavení na interním webu, je operací s osobními údaji ve smyslu § 4 písm. e) zákona č. 101/2000 Sb. Z tohoto ustanovení přitom nijak nevyplývá, že by se zpracování omezovalo pouze na operace činěné správcem osobních údajů navenek, ale vztahuje se na všechny operace správce (ve většině případů naopak převažující množství operací s osobními údaji probíhá uvnitř sféry správce), tedy i na informování vlastních členů.

Každý správce je v souladu s § 5 odst. 1 písm. f) zákona č. 101/2000 Sb. povinen zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny. K jinému účelu lze osobní údaje zpracovávat pouze se souhlasem subjektu údajů, resp. tehdy, je-li naplněna některá z výjimek dle § 5 odst. 2 písm. a) až g) zákona č. 101/2000 Sb. Účelem zpracování v předmětné věci je plnění práv a povinností z pracovněprávního vztahu mezi účastníkem řízení a paní XY (byť existence tohoto pracovněprávního vztahu je zde předmětem soudního řízení). Současně (a to především) je účelem zpracování osobních údajů vystupování účastníka řízení jako žalovaného v obou soudních sporech, s tím související řádné uplatňování jeho práv a ochrana jeho majetku a zájmů. Správní orgán konstatuje, že k těmto účelům lze celkem snadno vymezit okruh osob, které lze považovat za oprávněné v daných věcech jménem účastníka řízení vystupovat a rozhodovat a které jsou tedy oprávněny se s osobními údaji seznamovat a zpracovávat je.

Správní orgán se proto dále zabýval otázkou, zda lze jednání účastníka řízení podřadit pod ustanovení § 5 odst. 2 zákona č. 101/2000 Sb. Z obsahu stížností je nepochybné, že souhlasem paní XY účastník řízení nedisponoval. Účastník řízení ve svém vyjádření uvádí tři důvody, pro které byl dle jeho názoru postup v souladu se zákonem. Za prvé konstatuje, že osobní údaje paní XY byly zpřístupněny soudem v rámci vyhlášení rozsudku a je tedy je nutné považovat za údaje zveřejněné dle § 4 písm. l) zákona č. 101/2000 Sb. [srov. také § 5 odst. 2 písm. d) zákona č. 101/2000 Sb.]. Dále jsou osobní údaje paní XY zveřejněny ve veřejně přístupném seznamu, a to v obchodním rejstříku. Za třetí poté byly osobní údaje oznámeny výlučně osobám, jejichž informovanost je nezbytná pro řádné rozhodování orgánu (jehož jsou členy). K poslednímu správní orgán odkazuje na předchozí odstavec, kde je rozebráno, které orgány lze považovat za oprávněné se seznámit s osobními údaji a které již nikoliv. K druhé námitce účastníka řízení správní orgán uvádí, že obsahem rozsudku nejsou pouze osobní údaje, které jsou současně předmětem zveřejnění v obchodním rejstříku, ale i řada dalších osobních údajů (o pracovněprávním vztahu atd.), které v žádném veřejném seznamu uvedeny nejsou. Správní orgán se dále zabýval otázkou možné aplikace § 5 odst. 2 písm. d) zákona č. 101/2000 Sb. na danou věc.

Správní orgán považuje na prvním místě za potřebné zdůraznit, že zveřejněný osobní údaj [§ 4 písm. l) zákona č. 101/2000 Sb.] nelze považovat současně za oprávněně zve-

řejněný osobní údaj v souladu se zvláštním právním předpisem [§ 5 odst. 2 písm. d) zákona č. 101/2000 Sb.]. Prvně uvedený pojem je nepochybně pojmem širším než druhý z nich (srov. Kučerová, A., Bartík, V., Peca, J., Neuwirt, K., Nejedlý, J.: Zákon o ochraně osobních údajů. Komentář. 1. vydání. Praha: C. H. Beck, 2003, str. 91 a násl.). Přesto správní orgán dospěl k závěru, že osobní údaje uvedené v soudním rozsudku lze považovat za oprávněně zveřejněné osobní údaje v souladu se zvláštním předpisem. Současně je ale třeba v dané věci posoudit také větu druhou § 5 odst. 2 písm. d) zákona č. 101/2000 Sb., tedy to, zda nebylo zasaženo do práva na ochranu soukromého a osobního života. Správní orgán v této věci považuje za významný rozsah a charakter zveřejněných osobních údajů; lze především poukázat na příklady uvedené ve shora citovaném komentáři, který uvádí jako oprávněně zveřejněné osobní údaje uvedené v řadě veřejných rejstříků a seznamů (obchodním, živnostenském rejstříku apod.). Společně všem těmto veřejným seznamům je to, že v naprosté většině obsahují osobní údaje toliko identifikační spojené např. s určitým právem, které je rejstříkem prokazováno. Naproti tomu v případě soudního řízení a jeho výsledku, tj. rozsudku, jsou zveřejňovány osobní údaje mnohdy velmi citlivého charakteru, které by daná osoba sama o sobě dobrovolně nikdy nezveřejnila (ale k uplatnění nebo ochraně svého práva před soudem je k tomu okolnostmi donucena) a dle správního orgánu je proto třeba přiznat těmto osobním údajům přísnější ochranu. Lze také poukázat na judikaturu Ústavního soudu, dle kterého cílem principu veřejnosti soudního řízení je především kontrola soudní činnosti ze strany veřejnosti skrze reálné poučení o tom, jak soudnictví funguje, a tím budování důvěry veřejnosti v nezávislost a kvalifikovanost výkonu soudní moci (srov. nálezy Ústavního soudu sp. zn. II. ÚS 2672/07). Lze tedy uzavřít, že účelem veřejnosti soudního řízení není primárně zveřejňovat osobní údaje účastníků tohoto soudního řízení (oproti shora zmíněným veřejným rejstříkům), ale kontrola výkonu soudní moci veřejností a zveřejňování osobních údajů je přitom neoddelitelnou součástí. Správní orgán proto dospěl k závěru, že pravděpodobnost zásahu do soukromí dotčeného subjektu údajů v případě zpracování osobních údajů ze soudního řízení, resp. rozsudku soudu, je velmi vysoká. Současně správní orgán vychází z toho, že zveřejnění osobních údajů, stejně jako jejich zpřístupnění většímu počtu osob (v daném případě navíc neoprávněných), vnímá subjekt údajů jako zásah do svého soukromí. Účastník soudního řízení (subjekt údajů) totiž legitimně očekává, s ohledem na primárně omezené zpřístupnění jeho osobních údajů pouze těm, kteří se jednání soudu fyzicky zúčastňují, že tyto údaje již nebudou dále zpracovávány, zpřístupňovány nebo zveřejňovány bez jeho souhlasu (s výjimkou žurnalistické činnosti, která ovšem v daném případě nepřipadá v úvahu; srov. také čl. 9 směrnice Evropského parlamentu a Rady 95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů). Na základě

shora uvedených východisek dospěl správní orgán k závěru, že umístění rozsudku na interní web účastníka řízení, kde měli k osobním údajům paní XY přístup všichni členové účastníka řízení, nelze považovat za zpracování podřaditelné pod § 5 odst. 2 písm. d) zákona č. 101/2000 Sb., neboť není slučitelné s právem na ochranu jejího soukromého a osobního života. (čj. SPR-5860/08-13)

4. Povinnost zabezpečit osobní údaje, zproštění odpovědnosti

Účastník řízení, jako správce osobních údajů ve smyslu § 4 písm. j) zákona č. 101/2000 Sb., je povinen dodržovat při zpracování osobních údajů povinnosti stanovené zákonem č. 101/2000 Sb., včetně povinnosti vyjádřené v § 13 odst. 1 tohoto zákona. Podle tohoto ustanovení je správce osobních údajů povinen přijmout taková opatření, aby nemohlo dojít k neoprávněnému přístupu k osobním údajům, resp. k jejich neoprávněnému zpracování.

Povinnost dle § 13 odst. 1 zákona č. 101/2000 Sb. a této povinnosti odpovídající skutková podstata správního deliktu je formulovaná jako odpovědnost za následek. Dojde-li tedy k následku předvídanému v § 13 odst. 1 zákona č. 101/2000 Sb. (neoprávněnému přístupu k osobním údajům apod.), což je v této věci nepochybné, znamená to, že se správce osobních údajů dopustil také správního deliktu. Odpovědnost za správní delikt je přitom postavena na objektivní odpovědnosti (tedy bez ohledu na zavinění), přičemž zákon č. 101/2000 Sb. upravuje v § 46 odst. 1 liberační důvod, jehož naplněním se pachatel správního deliktu může odpovědnosti zprostit.

Za případnou poté považuje správní orgán argumentaci Nejvyššího správního soudu k problematice objektivní odpovědnosti za správní delikt v rozsudku čj. 9 As 36/2007-59 (byť v jiné oblasti veřejného práva a bez výslovného zakotvení liberačního ustanovení). Správní orgán proto považuje za vhodné se v souvislosti s citovaným rozsudkem podrobněji vyjádřit k naplnění skutkové podstaty správního deliktu dle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb. Dle názoru správního orgánu je pojem „přijmout taková opatření“ v normě ukládající primární povinnosti (tj. v § 13 odst. 1 zákona č. 101/2000 Sb.) nutno považovat za synonymum pojmu zajistit. Oba tyto pojmy je poté třeba dle názoru správního orgánu interpretovat jako garanci správce osobních údajů za bezpečnost zpracování osobních údajů, tedy za to, že se s osobními údaji např. neseznámí žádná nepovolaná osoba. Jedině tento výklad je schopen zajistit efektivní fungování právní normy a naplnění jejího elementárního smyslu a účelu, kterým je naplnění práva každého na ochranu před neoprávněným zasahováním do soukromí (viz opět rozsudek Nejvyššího správního soudu čj. 9 As 36/2007-59, www.nssoud.cz).

Skutková podstata správního deliktu dle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb. hovoří o nepřijetí nebo neprovede-

ní opatření pro zajištění bezpečnosti zpracování. S ohledem na shora uvedený výklad § 13 odst. 1 zákona č. 101/2000 Sb. je poté správní orgán toho názoru, že použití pojmů „nepřijme nebo neprovede“ nic nemění na charakteru odpovědnosti správce za nesplnění povinnosti dle § 13 zákona č. 101/2000 Sb.; uvedení bezpečnostních opatření v život, tak aby plnila svůj smysl a účel, nelze jiným způsobem, než jejich přijetím a provedením, přičemž tyto dva pojmy dle názoru správního orgánu současně plně pokrývají a vystihují všechny možné způsoby naplnění účelu bezpečnostních opatření; jinými slovy, s bezpečnostními opatřeními nelze dělat nic jiného, než je přijmout a provést. Správní orgán je proto toho názoru, že dikce § 45 odst. 1 písm. h) zákona č. 101/2000 Sb. nedává účastníkovi řízení prostor k tomu, aby prokazováním svého preventivního jednání popřel, že k naplnění skutkové podstaty deliktu došlo, byl-li přístup neoprávněné osoby k osobním údajům nepochybně prokázán.

Ustanovení § 46 odst. 1 zákona č. 101/2000 Sb. je formulováno tak, že právnícká osoba za správní delikt neodpovídá, jestliže prokáže, že vynaložila veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránila. Posuzování naplnění liberačního ustanovení je přitom závislé vždy na konkrétních okolnostech daného případu a nelze jej dle názoru správního orgánu jakkoliv předem zobecnit (při současném respektování limitu vyjádřeného v § 2 odst. 4 správního řádu).

Správní orgán přitom považuje za nezbytné konstatovat, že v případě ustanovení § 46 odst. 1 zákona č. 101/2000 Sb. (a ostatně všech liberačních ustanovení) se přenáší důkazní břemeno na účastníka řízení a je to on, kdo musí k prokázání liberace navrhnout důkazy (srov. Mates, P. a kolektiv: *Základy správního práva trestního*, 3. vydání, Praha: C.H. Beck, 2002, str. 12; dále také § 52 správního řádu).

Správní orgán proto na základě shora uvedeného posuzoval jednání účastníka řízení (tj. přijetí opatření formou vnitřních předpisů, způsob seznámení zaměstnanců s těmito předpisy atd.) toliko z hlediska ustanovení § 46 odst. 1 zákona č. 101/2000 Sb. Správní orgán v této souvislosti uvádí, že vynaložení veškerého úsilí, které bylo možno požadovat, neznamená jakékoliv úsilí, které správce vynaloží, ale musí se ve vztahu ke každému, konkrétně posuzovanému případu, jednat o úsilí maximálně možné, které je správce objektivně schopen vynaložit (zákon používá kritérium veškeré úsilí, které bylo možno požadovat, a nikoliv např. spravedlivě požadovat, požadovat s ohledem na poměry atp.). V případě účastníka řízení sice došlo ke zpracování interních předpisů, ale nedošlo prokazatelně k jejich dostatečnému provedení, které by zabránilo úniku osobních údajů. Jak vyplývá z výpovědi zaměstnankyně, nebyla si vědoma všech svých povinností vyplývajících z jejího funkčního zařazení a také se neseznámila s předpisy, byť i zveřejněnými na intranetu, účastníka řízení. Správní orgán má proto za prokázané, že účastník řízení nevynaložil veškeré úsilí, které bylo možné

požadovat, a že nepochybně existovaly další možnosti, jak mohl postupovat, aby odcizení osobních údajů zabránil; minimálně mohl zajistit skutečné proškolení své zaměstnankyně s následným ověřením jejích znalostí ve vztahu k bezpečnostním opatřením. Za vynaložení veškerého úsilí poté správní orgán v žádném případě nepovažuje odkaz na povinnost mlčenlivosti v pracovní smlouvě (zákonnou povinnost mlčenlivosti má každý zaměstnanec správce osobních údajů dle § 15 zákona č. 101/2000 Sb., přičemž tato povinnost nijak nezavazuje správce odpovědnosti za zabezpečení osobních údajů) stejně tak jako obecné stanovení místa výkonu práce.

Jak již bylo uvedeno, účelem povinnosti dle § 13 odst. 1 zákona č. 101/2000 Sb. není primárně to, aby správce osobních údajů přijal formálně bezpečnostní předpisy, ale zajištění toho, aby nedošlo k neoprávněnému přístupu k osobním údajům, a tím naplnění práva subjektu údajů na ochranu jeho soukromí. Z tohoto hlediska a tímto kritériem proto správní orgán také posuzoval vynaložené úsilí správce ve vztahu k možnému naplnění liberačního ustanovení. (čj. VER-6243/08-17)

5. Zveřejňování osobních údajů žadatelů o informace

Účastník řízení je správcem osobních údajů žadatelů o informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve smyslu § 4 písm. j) zákona č. 101/2000 Sb. a jako takový je povinen dodržet veškeré povinnosti stanovené tímto zákonem pro zpracování osobních údajů. Podle § 5 odst. 1 písm. f) zákona č. 101/2000 Sb. je povinen nakládat s osobními údaji pouze v souladu s účelem, pro který byly shromážděny a k jinému účelu jen v mezích ustanovení § 3 odst. 6 citovaného zákona, nebo pokud k tomu dal subjekt údajů předem souhlas. Podle § 5 odst. 3 zákona č. 106/1999 Sb. se zveřejňuje pouze vlastní poskytnutá informace, nikoliv údaje o žadateli ani o tom, komu byla poskytnuta. Zveřejnění osobních údajů v žádostech o informace a odpovědích na tyto žádosti na webových stránkách je třeba považovat za takový jiný účel, k němuž je třeba souhlasu subjektu údajů, což se však v daném případě nestalo. (čj. SPR-0097/09-8)

6. Zveřejňování citlivých údajů v médiích

Dle § 4 písm. e) zákona č. 101/2000 Sb. je zpracováním osobních údajů jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Výklad činností (operací), které spadají pod pojem zpracování dle zákona č. 101/2000 Sb. musí být přitom totožný s výkladem pojmu zpracování dle čl. 3 odst. 1 směrnice Evropského parlamentu a rady 95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Ze spisového materiálu přitom vyplývá, že předmětná zpráva je dostupná prostřed-

nictvím internetové stránky účastníka řízení. Dle Rozsudku Soudního dvora ze dne 6. listopadu 2003 ve věci C-101/01 (Úřední věstník C 7 ze dne 10. ledna 2004, str. 3) čin uvádění různých osob na internetové stránce a jejich identifikace jménem nebo jiným způsobem tvoří zpracování osobních údajů zcela nebo částečně automatizovanými způsoby ve smyslu čl. 3 odst. 1 směrnice 95/46/ES. Vzhledem ke skutečnosti, že výklad a aplikace vnitrostátního předpisu nesmí být v rozporu s výkladem směrnice, považuje správní orgán uvedení osobních údajů pana XY v předmětné zprávě, která je dostupná na internetových stránkách účastníka řízení, za zpracování osobních údajů ve smyslu § 4 písm. e) zákona č. 101/2000 Sb. Na účastníka řízení se tak vztahují veškeré povinnosti stanovené zákonem č. 101/2000 Sb. Bez ohledu na shora uvedené lze poté dle správního orgánu konstatovat, že žurnalistická činnost spadá pod pojem zpracování osobních údajů dle zákona č. 101/2000 Sb.; je totiž zjevné, že spočívá ve vyhledávání, shromažďování, třídění, používání a až následně ve zveřejňování informací, které jsou svojí povahou osobními údaji dle § 4 písm. a) zákona č. 101/2000 Sb., a že tyto operace jsou prováděny systematicky a s jednotčím cílem (vytvoření konkrétní „zpravodajské“ informace a její zveřejnění). Dle správního orgánu si lze pouze obtížně představit systematictější činnost s osobními údaji než je novinářská práce, která spočívá ve shromažďování informací k jednotlivým osobám a věcem, dávání těchto informací do souvislostí a jejich následné publikaci.

Dle § 9 písm. a) zákona č. 101/2000 Sb. lze citlivé údaje zpracovávat jen tehdy, pokud k tomu dal subjekt údajů výslovný a informovaný souhlas, který je správce schopen po celou dobu zpracování prokázat. Bez tohoto souhlasu lze citlivé údaje zpracovávat v případech uvedených v § 9 písm. b) až i) zákona č. 101/2000 Sb. Ze spisového materiálu a okolností zpracování vyplývá, že účastník řízení souhlasem subjektu údajů nedisponoval. Na zpracování poté dle názoru správního orgánu nelze vztáhnout ani žádné z dalších ustanovení § 9 zákona č. 101/2000 Sb. Správní orgán pouze na okraj konstatuje, že ustanovení § 9 písm. g) zákona č. 101/2000 Sb. se na předmětné zveřejnění nevztahuje, neboť jeho podmínkou je, aby citlivý údaj předem zveřejnil sám subjekt údajů (nikoliv tedy Policie České republiky). Dle správního orgánu nelze použít ani ustanovení § 9 písm. b) zákona č. 101/2000 Sb.; podmínkou tohoto ustanovení je, aby zpracování bylo nezbytné pro uvedené účely. Podmínku nezbytnosti v této věci správní orgán neshledal, neboť by při zobecnění tohoto případu bylo možné dojít k závěru, že každá osoba, která je nakažena virem HIV, nemá právo na ochranu této citlivé informace, neboť je jejím zveřejněním chráněno zdraví a život jiných osob. Tento výklad je dle správního orgánu v přímém rozporu s právem subjektu údajů na ochranu soukromí. Na tomto nemění dle správního orgánu nic ani údajné chování pana XY, neboť právě s ohledem na toto chování je na svobodné vůli každého, zda podstoupí riziko nákazy případnou nemocí či nikoliv. Pokud účastník

řízení argumentuje potřebou zahájit vlastní léčbu pana XY, tak za tímto účelem, tedy k jeho nalezení a předání do diagnostického ústavu, resp. k léčbě, nepochybně údaj o jeho zdravotním stavu nezbytný nebyl. Pokud se jedná o účastníkem řízení uváděný § 9 písm. c) zákona č. 101/2000 Sb., podmínkou zpracování citlivých údajů je zde kromě konkrétních činností (tj. zajišťování zdravotní péče atd.) také to, aby takovéto zpracování stanovil zvláštní zákon. Mimo to, že zveřejnění informace nesouvisí s takto vymezeným účelem zpracování, správnímu orgánu není znám žádný zvláštní zákon, který by médiím ukládal zveřejňovat údaje o zdravotním stavu občanů České republiky. Účastníkem řízení uváděný § 9 písm. i) zákona č. 101/2000 Sb. se opět s odkazem na nezbytnost zmocnění ve zvláštním zákoně vztahuje pouze na zpracování osobních údajů Policií České republiky, resp. orgány činnými v trestním řízení, a nikoliv na média.

Správní orgán dále k vyjádření účastníka řízení konstatuje, že i pokud by se pan XY dopouštěl trestného činu šíření nakažlivé choroby, přesto by bylo třeba chránit jeho soukromí a to s ohledem na jeho věk a tuto informaci dále nesdělovat [srov. § 52 a násl. zákona č. 218/2003 Sb., o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů (zákon o soudnictví ve věcech mládeže)]; i v tomto případě by český právní řád poskytoval panu XY jako nezletilé osobě ochranu jeho soukromí. Správní orgán dále uvádí, že samotná skutečnost, že citlivý údaj (navíc v jiné podobě, kdy umožňoval, jak uvedl i sám účastník řízení, závěr o nakažení i jinou nemocí, např. žloutenkou B nebo C) zveřejnila Policie České republiky, nezbavuje další osoby povinnosti nakládat s ním v souladu s příslušnými zákony; současně nelze ani presumovat, že postup Policie České republiky byl v souladu s příslušnými právními předpisy, kterými je povinna se řídit při zpracování osobních a citlivých údajů (zejména se zákonem č. 273/2008 Sb., o Policii České republiky, což ale není předmětem tohoto řízení).

Správní orgán považuje dále za nutné uvést další východiska, dle kterých posuzoval odpovědnosti účastníka řízení, a to především s ohledem na předmět jeho činnosti, kterým je žurnalistika. V této souvislosti je třeba především zmínit čl. 9 směrnice 95/46/ES, dle kterého členské státy stanoví pro zpracování osobních údajů prováděné výlučně pro účely žurnalistiky nebo uměleckého či literárního projevu, odchylky a výjimky z této kapitoly (tj. kapitoly II), a z kapitol IV a VI, pouze pokud se ukáží jako nezbytné pro uvedení práva na soukromí do souladu s předpisy upravujícími svobodu projevu (srov. také recitál č. 37 ke směrnici č. 95/46/ES). K tomuto je ovšem třeba konstatovat, že v českém právním řádu zákonodárce žádné výjimky přímo pro zpracování za účelem žurnalistiky nestanovil a zákonné povinnosti se proto na tato zpracování vztahují v plné míře. Přesto je třeba při posuzování odpovědnosti za jejich porušení vycházet z ústavního práva vyjádřeného v čl. 17 Listiny základních

práv a svobod. Jinými slovy, ne každé porušení povinnosti dle zákona č. 101/2000 Sb. v souvislosti se zpracováním osobních údajů pro účely žurnalistiky bude správním deliktem dle tohoto zákona, už z toho důvodu, že k tomuto porušování musí z povahy žurnalistické činnosti docházet velmi často a opakovaně.

Druhým východiskem je poté názor vyjádřený v již účastníkem řízení zmiňovaném nálezu Ústavního soudu sp. zn. I. ÚS 4/04 ze dne 23. března 2004, dle kterého „trestní právo a trestněprávní kvalifikace určitého jednání, které má soukromoprávní základ, jako trestného činu je třeba považovat za ultima ratio, tedy za krajní právní prostředek, který má význam především celospolečenský, tj. z hlediska ochrany základních společenských hodnot. V zásadě však nemůže sloužit jako prostředek nahrazující ochranu práv a právních zájmů jednotlivce v oblasti soukromoprávních vztahů, kde závisí především na individuální aktivitě jednotlivce, aby střežil svá práva, jimž má soudní moc poskytnout ochranu. Je však nepřijatelné, aby tuto ochranu aktivně přebíraly orgány činné v trestním řízení, jejichž úkolem je ochrana převážně celospolečenských hodnot, nikoliv přímo konkrétních subjektivních práv jednotlivce, jež svou povahou spočívají v soukromoprávní sféře“.

Na druhé straně je třeba nepochybně zhodnotit samotnou skutečnost, že údaj o zdravotním stavu je citlivým údajem ve smyslu § 4 písm. b) zákona č. 101/2000 Sb. a jako takový proto požívá vyšší právní ochrany. Současně přitom údaj o zdravotním stavu, natož údaj o nakažení virem způsobujícím nevyléčitelnou nemoc, je společností vnímán jakožto údaj svým charakterem velmi citlivý (nikoliv ve smyslu právním) a informace o zdravotním stavu rozhodně nelze považovat za údaje běžně dostupné a bez vědomí a souhlasu subjektu údajů zveřejňované. Tomu také odpovídá právní úprava nahlížení do zdravotnické dokumentace v zákoně č. 20/1966 Sb., o péči o zdraví lidu. V daném případě došlo současně ke zveřejnění údaje týkajícího se nezletilé osoby, tedy osoby, jejíž schopnost hájit svá práva a svoje soukromí, je nižší, a zájem společnosti na její ochranu nezpochybnitelný. Správní orgán se v této věci neztotožňuje s názorem účastníka řízení, že samotná společnost informací o nákaze virem HIV nevnímá jako difamující.

Správní orgán po posouzení všech shora uvedených kritérií dospěl k závěru, že je na místě v daném případě posuzovat odpovědnost účastníka řízení za spáchání správního deliktu dle zákona č. 101/2000 Sb., neboť postih za zveřejnění informace o zdravotním stavu (nakažení virem HIV) nezletilého bez jeho vědomí a souhlasu má celospolečenský význam. Odpovědnost účastníka řízení poté dle správního orgánu nepředstavuje ani zásah do svobody projevu dle čl. 17 Listiny základních práv a svobod, neboť podle čl. 17 odst. 4 lze svobodu projevu omezit, je-li to nezbytné pro ochranu práv a svobod druhých; dle správního orgánu právo na ochranu soukromí upravené v čl. 10 Listiny základních práv

a svobod v daném konkrétním případě převažuje. (čj. SPR-1117/09-7)

7. Zpracování osobních údajů v Národní databázi DNA

Informace obsažené v profilu DNA, který je předmětem dalšího zpracování v Národní databázi DNA (dále jen „ND DNA“), jsou genetickou informací. Ve smyslu § 4 písm. b) zákona č. 101/2000 Sb. je citlivým údajem mimo jiné genetický údaj subjektu údajů. Zařazování, uchovávání, vyhledávání, resp. používání profilů DNA v ND DNA je nepochybně činností, kterou lze podřadit pod pojem zpracování osobních údajů ve smyslu § 4 písm. e) zákona č. 101/2000 Sb. Účastník řízení je přitom správcem těchto osobních, resp. citlivých, údajů podle § 4 písm. j) zákona č. 101/2000 Sb. a jako takový musí dodržovat veškeré povinnosti stanovené zákonem č. 101/2000 Sb.

Podle § 9 zákona č. 101/2000 Sb. může správce zpracovávat citlivé údaje jen tehdy, pokud k tomu dal subjekt údajů výslovný informovaný souhlas, nebo při naplnění některé z dalších, taxativně vymezených, podmínek dle § 9 písm. b) až i) zákona č. 101/2000 Sb. Podle § 9 písm. i) zákona č. 101/2000 Sb. lze zpracovávat citlivé údaje, pokud se jedná o zpracování podle zvláštních zákonů při předcházení, vyhledávání, odhalování trestné činnosti, stíhání trestných činů a pátrání po osobách. Zákon zde tedy umožňuje zpracovávat citlivé údaje bez souhlasu subjektu údajů za specifikovaným účelem, současně formulace „se jedná o zpracování podle zvláštních zákonů“ znamená, že takové zpracování může být prováděno pouze na základě zmocnění ve zvláštním zákoně a v rozsahu a za podmínek stanovených v tomto zvláštním zákoně.

Podle § 79 zákona č. 273/2008 Sb. může Policie zpracovávat osobní údaje včetně citlivých údajů bez souhlasu osoby, jíž se tyto údaje týkají, pokud je to nezbytné pro plnění jejich úkolů. Ustanovení § 85 a § 86 poté upravují práva a povinnosti Policie při zpracování osobních údajů při plnění jejich úkolů. Tato ustanovení tedy (velmi obecně) upravují oprávnění Policie zpracovávat osobní údaje, a to ve vztahu ke všem myslitelným účelům, které s činností Policie souvisejí od vlastního vyšetřování trestných činů a přestupků (zpracování osobních údajů v jednotlivých vyšetřovacích spisech) až po veškeré evidence a informační systémy Policie, které využívá při své činnosti, a to včetně ND DNA. Prvotní část zpracování osobních údajů v některých evidencích Policie (včetně ND DNA), tj. shromažďování osobních údajů ve smyslu § 4 písm. f) zákona č. 101/2000 Sb., upravuje § 65 zákona č. 273/2008 Sb., který opravňuje Policii u vymezeného okruhu osob snímat daktyloskopické otisky, zjišťovat tělesné znaky, provádět měření těla, pořizovat obrazové, zvukové a obdobné záznamy a odebírat biologické vzorky umožňující získání informací o genetickém vybavení, to vše při plnění úkolů Policie pro účely budoucí identifikace. Správní orgán je toho názoru, že uvedená ustanovení jsou

ve svém vzájemném vztahu s ohledem na použité, mnohdy neurčité, právní pojmy obtížně vyložitelná, což samo o sobě značně zpochybňuje jejich využití jakožto právního základu pro ND DNA.

Dle názoru správního orgánu je třeba vycházet při výkladu shora uvedených právních norem jak ze systematiky a účelu zákona č. 273/2008 Sb., tak především z obecné systematiky a účelu zákona č. 101/2000 Sb., resp. jeho práv a povinností pro zpracování osobních údajů. Z tohoto hlediska lze konstatovat, že ND DNA je evidencí osobních údajů ve smyslu § 86 písm. b) zákona č. 273/2008 Sb., jinými slovy, jedná se o zpracování osobních údajů dle § 4 písm. e) zákona č. 101/2000 Sb. Jako každé jiné zpracování, musí mít i ND DNA stanovený svůj účel [§ 86 písm. a) zákona č. 273/2008 Sb.]; tento účel je účastník řízení povinen vymezit co nejpresněji. V případě ND DNA je přitom třeba dovozovat tento účel nejenom z vnitřních předpisů deklarovaných účastníkem řízení (v Závazném pokynu policejního prezidenta č. 88 ze dne 29. května 2008 je sice čl. 1 označen jako účel, žádné vymezení účelu ovšem neobsahuje; ten lze najít jednak v preambuli tohoto pokynu jako odhalování trestné činnosti a zjišťování jejích pachatelů, a dále negativním vymezením v čl. 3 odst. 2 tohoto pokynu). Mnohem přesněji se k účelu obdobné databáze DNA vyjádřil Evropský soud pro lidská práva (dále jen „Soud“), který uvedl, že zatímco prvotní odběr (otisků prstů a genetických vzorků) je určen ke zjištění spojitosti mezi konkrétní osobou a jednotlivým trestným činem, z jehož spáchání je podezřelá, uchování sleduje širší cíl, a to identifikaci budoucích pachatelů (srov. rozhodnutí velkého senátu ve věci S. a Marper proti Spojenému království ze dne 4. prosince 2008, § 100; Přehled rozsudků Evropského soudu pro lidská práva č. 2/2009). Jinými slovy, prvotní odběr stop či vzorků slouží k usvědčení pachatele (nebo vyvrácení jeho viny), zatímco jejich uchování slouží pro případ spáchání dalšího trestného činu k odhalení pachatele na základě stop zanechaných na místě činu. Ve vztahu k takto vymezenému účelu správní orgán ve shodě se Soudem konstatuje, že se jedná o účel legitimní. Správní orgán si je vědom významné role ND DNA při odhalování pachatelů trestných činů, která vyplývá z moderních kriminalistických metod. Současně je ovšem mít na zřeteli, že veškerý postup veřejné moci, včetně orgánů činných v trestním řízení, musí odpovídat ústavním principům zákonnosti a přiměřenosti (viz čl. 2 odst. 2 a čl. 4 Listiny základních práv a svobod).

Každé zpracování osobních údajů musí být v souladu s povinnostmi stanovenými zákonem č. 101/2000 Sb., resp. zvláštním právním předpisem, který otázku zpracování osobních údajů v dané oblasti dále upřesňuje anebo zcela samostatně upravuje. V případě ND DNA se v souladu s § 3 odst. 6 zákona č. 101/2000 Sb. namísto povinností stanovených v § 5 odst. 1 zákona č. 101/2000 Sb. použijí ustanovení § 85 odst. 1 zákona č. 273/2008 Sb. Lze tedy konstatovat, že některé povinnosti správce osobních údajů dle zákona

č. 101/2000 Sb. se na zpracování prováděné účastníkem řízení nevztahují; mezi těmito povinnostmi ovšem není povinnost zpracovávat osobní údaje pouze na základě právního titulu dle § 5 odst. 2 zákona č. 101/2000 Sb. a v případě citlivých údajů dle § 9 zákona č. 101/2000 Sb., kterým může být souhlas subjektu údajů nebo jiná, zákonem stanovená podmínka [viz § 5 odst. 2 písm. a) až g), § 9 písm. b) až i) zákona č. 101/2000 Sb.].

Jak již bylo shora uvedeno, dle § 9 písm. i) zákona č. 101/2000 Sb. lze zpracovávat citlivé údaje podle zvláštních zákonů při předcházení, vyhledávání, odhalování trestné činnosti, stíhání trestných činů a pátrání po osobách. Ustanovení § 79 odst. 1 zákona č. 273/2008 Sb. je oním předvídaným ustanovením zvláštního zákona, které dále zužuje toto zákonné oprávnění Policie zpracovávat osobní údaje bez souhlasu na případy, kdy je to nezbytné pro plnění jejích úkolů výslovně definovaných zákonem č. 273/2008 Sb. Zákodárce zde přitom zvolil velmi obecné vymezení pro oprávnění Policie, která se uplatní na všechny případy zpracování osobních údajů Policií (jak již bylo výše zmíněno), přičemž aby se nejednalo o zmocnění neomezené, stanovil jako kritérium vedle souvislosti s úkoly Policie především nezbytnost takového zpracování. Správnímu orgánu, jakožto orgánu pověřenému dle § 29 odst. 1 písm. a) zákona č. 101/2000 Sb. nezávislým dozorem nad zákonností zpracování osobních údajů, tak nezbyvá, než tento neurčitý právní pojem „nezbytnost“ pro potřeby zpracování osobních údajů v ND DNA vyložit a na jeho základě posoudit, zda je zařazení a uchovávání osobních údajů pana XY v ND DNA skutečně nezbytné pro plnění úkolů Policie nebo nikoliv.

Správní orgán v první řadě konstatuje, že při posuzování nezbytnosti vyjádřené v § 79 odst. 1 zákona č. 273/2008 Sb. jakožto další podmínky vedle souvislosti s úkoly Policie (vymezené opět značně obecně v § 2 zákona č. 273/2008 Sb.), je třeba přihlídnout k účelu každého jednotlivého zpracování osobních údajů Policií, v daném případě ke shora nastíněnému účelu ND DNA. Ačkoliv ustanovení § 79 odst. 1 zákona č. 273/2008 Sb. již nepoužívá jakožto omezující kritérium pro zpracování citlivých údajů povahu trestného činu, tak jak činilo ustanovení § 42g odst. 3 zákona č. 283/1991 Sb., je toto kritérium dle správního orgánu stále nejvýznamnějším hlediskem, na základě kterého lze definovat okruh osob, jejichž profil bude do ND DNA zařazen, tak aby se nejednalo o zcela svévolný a náhodný postup. Jak se již správní orgán vyjádřil ve svém rozhodnutí zn. SPR-0836/08-14 ze dne 30. května 2008, na které sám účastník řízení ve svém vyjádření odkazuje, při hodnocení povahy trestného činu budou kritériem typový stupeň nebezpečnosti trestného činu pro společnost a faktická využitelnost ND DNA pro odhalení pachatele daného trestného činu (druhově vymezeného). Správní orgán v tomto rozhodnutí uvedl také další kritéria pro posouzení povahy trestného činu a nezbytnosti zařazení profilu odsouzené osoby do ND DNA, jako

je vysoký podíl recidivistů, způsob spáchání trestného činu a s tím související pravděpodobnost zanechání biologické stopy na místě nebo řada dílčích útoků. Všechna tato hlediska, případně i další vyplývající z okolností daného případu, je dle správního orgánu nutno posoudit předtím, než je rozhodnuto o vložení daného profilu DNA do ND DNA, tedy o tom, že v konkrétním případě je takové zpracování citlivého údaje nezbytné pro plnění úkolů Policie.

Správní orgán se v zásadě shoduje s účastníkem řízení, že v případě trestného činu krádeží daně, poplatku a jiné podobné dávky podle § 148 trestního zákona, jsou uvedená hlediska (až na jedno) naplněna. Z hlediska účelu ND DNA je ovšem správní orgán toho názoru, že faktická využitelnost ND DNA pro odhalení pachatele těchto trestných činů není dána. V daném případě se jedná o hospodářské trestné činy, jejichž pachatelem již z jejich povahy bude ve většině případů subjekt daně (tedy osoba orgánům činným v trestní řízení známá již od počátku trestního řízení nebo snadno zjistitelná na základě jiných stop a důkazů, než je profil DNA). Správní orgán považuje za značně hypotetickou situaci, pokud by v trestním řízení vedeném pro tento trestný čin nebylo možné vymezit relativně úzký okruh pachatelů. Ačkoliv lze obecně připustit, že se trestného činu dle § 148 trestního zákona může dopustit i jiná osoba, než subjekt daně, odborná literatura uvádí pouze jediný příklad, a to daňového poradce (srov. Šámal, P., Púry, F., Rizman, S. Trestní zákon. Komentář. II. díl. 6., doplněné a přepracované vydání. Praha: C. H. Beck, 2004, str. 919). Správní orgán v této souvislosti zdůrazňuje, že porovnávání profilu DNA obviněného, resp. podezřelého, získaného na základě § 114 odst. 2 trestního řádu, v konkrétním trestním řízení se stopami z místa činu nijak nesouvisí s dalším uchováváním získaných dat v ND DNA, resp. uchovávat pro tento účel profil DNA v této databázi není nezbytné.

Správní orgán si je vědom toho, že při posuzování kritéria nezbytnosti a v důsledku i povahy trestného činu vychází z předpokladu, že se pachatel trestného činu může dopustit v budoucnu stejného nebo obdobného trestného činu; z tohoto hlediska je potom posuzována povaha jednotlivých trestných činů jak v rovině jejich společenské nebezpečnosti, tak v rovině faktické využitelnosti a nezbytnosti ND DNA k odhalení pachatele (nikoliv k jeho usvědčení). Správní orgán proto vychází z přesvědčení, že nezbytnost uchování profilu DNA v ND DNA, tj. poměrně významného zásahu do práv pachatele (viz níže k zásahu do soukromí), který se tímto stane subjektem dlouhodobě evidovaným ve spojení s informací o předchozí trestné činnosti, lze nalézt pouze u těch závažných trestných činů, u nichž může být současně profil DNA hlavním či jedním z mála důkazů vedoucích k odhalení pachatele. Správní orgán je toho názoru, že se tento přístup (který ostatně zvolil ve svém vnitřním předpise také sám účastník řízení) jeví jako jediný rozumný, neboť vyvažuje jak práva na ochranu soukromí dle čl. 10 odst. 3 Listiny základ-

ních práv a svobod a čl. 8 Úmluvy o ochraně lidských práv a základních svobod (sdělení Federálního ministerstva zahraničí č. 209/1992 Sb.; dále jen „Úmluva“), tak legitimní cíl ND DNA. Uvedený přístup potvrzuje mimo jiné také Doporučení č. R (92) 1 Výboru ministrů členským státům (Rady Evropy) o využívání analýzy deoxyribonukleové kyseliny (DNA) v rámci systému trestní justice, které v čl. 8 uvádí, že výsledky analýzy DNA a informace z nich odvozené mohou být uchovávány, jestliže byl dotčený jednotlivec odsouzen pro závažné trestné činy ohrožující život, zdraví nebo bezpečnost osob. I toto doporučení tedy vychází z klasifikace jednotlivých trestných činů s ohledem na jejich povahu.

Správní orgán závěrem uvádí, že ke shora uvedeným závěrům dospěl na základě ústavně konformního výkladu příslušných ustanovení zákona č. 273/2008 Sb., především jeho §§ 64, 79, 85 a 86. Přitom vycházel z premisy, že uchováním profilů DNA dochází k zásahu do práva na soukromý život (srov. rozsudek Soudu ve věci S. a Marper proti Spojenému království ze dne 4. prosince 2008, § 70 až § 77). Správní orgán podotýká, že zákonné zmocnění státu, které by ospravedlňovalo a umožňovalo zásah do soukromí dotčených osob chráněného čl. 10 odst. 3 Listiny, jak jej předpokládá čl. 8 odst. 2 Úmluvy, musí být v souladu se zásadou právního státu, musí být dostatečně dostupné, předvídatelné, tedy vyjádřené s velkou mírou přesnosti (srov. rozsudek Soudu ve věci S. a Marper proti Spojenému království ze dne 4. prosince 2008, § 95 a násl.). Správní orgán je toho názoru, že tyto atributy ustanovením, ze kterých lze dovozovat oprávnění Policie vést ND DNA, scházejí, a pro potřeby tohoto řízení je musí tedy sám dovodit výkladem ad hoc. Přesto i při tomto postupu zůstává pochybnost, zda určitost citovaných norem je natolik dostatečná, aby sama o sobě mohla tvořit zákonný základ pro uplatnění státní moci formou vytvoření ND DNA ve smyslu čl. 2 odst. 2 Listiny základních práv a svobod, to především proto, že nespĺňuje ani minimální požadavky na stanovení rozsahu a použití profilů DNA (srov. obecný účel vymezený úkoly Policie), délku uložení (srov. vymezení doby uchování v § 86 odst. 1 a § 65 odst. 1 zákona č. 273/2008 Sb.), použití a přístup třetích osob, procedury vedoucí k ochraně celistvosti a důvěrnosti údajů a procedury jejich zničení (opět viz rozsudek Evropského soudu pro lidská práva ve věci S. a Marper proti Spojenému království ze dne 4. prosince 2008, § 99).

Správní orgán se s ohledem na změnu příslušného zákona o Policii České republiky musel vypořádat také s tím, zda zařazení profilu DNA pana XY do ND DNA neumožňovala předchozí právní úprava, tedy zákon č. 283/1991 Sb. Vzhledem k tomu, že většina relevantních ustanovení byla beze

změn, nebo pouze s drobnými změnami přejata do zákona č. 273/2008 Sb., dospěl správní orgán k závěru, že stejné argumenty, které platí pro posouzení dané věci dle zákona č. 273/2008 Sb., platí také pro příslušná ustanovení zákona č. 283/1991 Sb., a zařazení a uchování profilu DNA bylo proto v rozporu i se zákonem č. 283/1991 Sb. (viz znění § 42e odst. 1 zákona č. 283/1991 Sb. a § 65 zákona č. 273/2008 Sb.; znění § 42g odst. 1 a 3 zákona č. 283/1991 Sb. a § 79, § 85 a § 86 zákona č. 273/2008 Sb.). Pokud došlo ve formulaci jednotlivých ustanovení k nějakým změnám, tak pouze směrem k jejich ještě větší obecnosti. (čj. SPR-3309/09-18)

8. Zveřejňování osobních údajů studentů

Účastník řízení zpracovává osobní údaje svých studentů v souladu s povinností vyplývající mu ze zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů. Ale jelikož zákon č. 111/1998 Sb., ani žádný jiný právní předpis, neobsahuje podmínky zveřejňování osobních údajů studentů na internetových stránkách fakulty, je nutno dojít k závěru, že se na daný postup bude vztahovat obecná úprava nakládání s osobními údaji obsažená v zákoně č. 101/2000 Sb. Účastník řízení je jako správce osobních údajů ve smyslu § 4 písm. j) zákona č. 101/2000 Sb. povinen podle § 5 odst. 1 písm. f) zákona č. 101/2000 Sb. nakládat s osobními údaji pouze v souladu s účelem, pro který byly shromážděny, a k jinému účelu jen v mezích ustanovení § 3 odst. 6 tohoto zákona, nebo pokud k tomu dal subjekt údajů předem souhlas. Stanovený účel zpracování (vedení matriky studentů, resp. organizační zajištění studia) byl zveřejněním osobních údajů studentů překročen. Na jednání účastníka řízení není dále možné aplikovat žádnou z výjimek stanovených v § 3 odst. 6 zákona č. 101/2000 Sb. a účastník řízení nedisponoval ani souhlasem osob, jejichž osobní údaje byly zveřejněny. Účastník řízení navíc disponuje informačním systémem, prostřednictvím kterého informuje studenty o záležitostech týkajících se jejich studia, a do kterého mají přístup pouze studenti prostřednictvím přihlašovacího jména a hesla, a není tudíž přístupný veřejnosti, jak je tomu u veřejně přístupných internetových stránek účastníka řízení. (čj. SPR-6265/09-3)

Poznámka:

- ¹⁾ Za jednotlivými texty, které jsou rozděleny do tematických okruhů, jsou vždy kurzívou uvedena interní čj., pod kterými jsou jednotlivé případy v Úřadu evidovány.
- ²⁾ Materiál je také k dispozici na internetové adrese Úřadu www.uouu.cz v sekci Dozorová činnost v rubrice Správní delikty / Z rozhodovací činnosti.

Závěry jednání Konference evropských komisařů ochrany dat a soukromí

(Praha 29. – 30. dubna 2010)

Ve dnech 29. – 30. dubna 2010 se v Praze uskutečnila Konference evropských komisařů ochrany dat a soukromí. Konference, v odborných kruzích často nazývaná jen „jarní konference“, je pro ochránce osobních údajů z celé Evropy příležitostí diskutovat o aktuálních, a nejen evropsky významných, tématech oboru.

Programovým a organizačním zabezpečením byl pověřen český Úřad pro ochranu osobních údajů. Prestižního úkolu a výzvy se český Úřad ujal v duchu jednotící myšlenky, kterou pro pražskou konferenci zvolil – „Hodnotit minulost, myslet na budoucnost“.

K jednáním se na Pražském hradě, kde se konference konala, sešla více než stovka delegátů z většiny států Evropy. Program byl rozdělen do čtyř tematických bloků: „Internet věcí a všudypřítomné monitorování v prostoru a čase“, „Děti v pavučině sítí“, „Ochrana osobních údajů na rozcestí“ a „Veřejný sektor – respektovaný partner, nebo privilegiovaný zpracovatel dat?“. Výsledkem jednání a spolupráce bylo přijetí čtyř společných rezolucí.

1. Rezoluce k používání tělesných skenerů (body scanners) pro účely bezpečnosti na letištích

Po nevydařeném útoku na let Delta 253 z Amsterdamu do Detroitu dne 25. prosince 2009 začaly vlády a bezpečnostní orgány po celém světě diskutovat o tom, jak zvýšit bezpečnost na letištích a zda instalovat tělesné skenery k usnadnění prohlídek cestujících před nástupem do letadla. Nasazení takových skenerů a prohlídka celého lidského těla může vážně narušit právo cestujícího na soukromí a ochranu dat. Z tohoto důvodu by se mělo při úvahách o použití tělesných skenerů počítat s principy ochrany osobních údajů a s ochrannými opatřeními, stejně jako se zásadou „privacy by design“.

Jedním z principů ochrany dat, který je třeba vzít v úvahu, je potřebnost zpracování. Stále ještě není jasné, jestli tato zařízení skutečně zvýší bezpečnost na letištích. Před jejich nasazením by se také měla zvážit jejich účinnost a vliv na zdraví cestujících.

Vzhledem k současnému stavu diskuze má Konference evropských komisařů ochrany dat a soukromí obavu, že jsou zaváděna nová zařízení, která nesplňují standardy ochrany osobních údajů. Zdůrazňuje proto potřebu vědecky podložené a koordinované diskuze o tomto tématu.¹ Také posudkům všech zainteresovaných, jako jsou vědci, techničtí experti, odborníci z oblasti zdravotnictví a ochrany dat, by mělo být popráno sluchu. Před ukvapeným rozhodnutím o použití

tělesných skenerů je třeba probrat zejména tyto následující aspekty:

1. Je zavedení tělesných skenerů na letištích nezbytné pro leteckou bezpečnost, a pokud ano, do jaké míry? Je potřeba vypracovat podrobné studie opírající se o vědecké metody a užitečnost tělesných skenerů by měla být prokázána spolehlivými empirickými daty. Stále přetrvávají vážné pochyby, zda tělesné skenery skutečně dokážou lépe odhalovat výbušniny jako třeba malá množství kapalin nebo jiných látek nízké hustoty. Je tu přidaná hodnota ve srovnání s jinými metodami prověřování osob průchodem kovovými detektory, ručními skenery nebo osobní prohlídkou? Existují-li méně rušivé metody², kterými je možné dosáhnout stejného zvýšení úrovně bezpečnosti, potom by také měly být použity.
2. Existují přiměřené záruky zajišťující soukromí osob kontrolovaných tělesnými skenery? Technická opatření musejí zaručit, že osobní údaje cestujících nebudou ani uchovávány, ani předávány. Obrázky by měly být smazány hned, jak cestující úspěšně projde kontrolou.

Standardizovaný obrys lidského těla (mimic board picture) tolik nenarušuje soukromí a mohl by být preferovaným způsobem zobrazování těla na obrazovkách. Pokud by se objevily jakékoliv intimní detaily osob, např. zdravotně podpůrná zařízení nebo umělé části těla, měly by se zobrazit pouze obsluze skeneru. Pracovníci, kteří posuzují snímky zachycené tělesnými skenery, nesmějí být ti samí, kteří provádějí další kontroly. Svou činnost musejí vykonávat v prostorách, kde je vyloučena jakákoli komunikace s jinými kontrolory a nesmějí na cestující vidět. Kromě toho by tělesné skenery měly být instalovány až po provedení posouzení dopadů na soukromí (privacy impact assessment – PIA), jehož výsledkem by mělo být začlenění všech zde zmiňovaných principů do posuzovaného systému.

Pouze při nastolení spravedlivé rovnováhy mezi účinností a nutností těchto nových technologických zařízení na straně jedné a dopadem na soukromí cestujících v letecké přepravě na straně druhé, bude možné z hlediska ochrany dat považovat tělesné skenery za vyvážený a vhodný prostředek bezpečnostních prohlídek.

Konference evropských komisařů ochrany dat a soukromí proto vyzývá evropské činitele odpovědné za rozhodování, aby důkladně zvážili dopad tělesných skenerů na základní práva cestujících ještě před rozhodnutím o jejich využití na letištích.

Používána by měla být pouze zařízení přátelská vůči ochraně osobních údajů tím, že uplatňují technologie zvyšující soukromí, a která navozují správnou rovnováhu mezi potřebou vyšší bezpečnosti a právem na soukromí a ochranu osobních údajů. Úřady pro ochranu dat by měly zůstat zapojeny do rozhodovacího procesu, obzvláště během zkoušek a testovacích fází, prostřednictvím předběžných kontrol skenerových systémů (pokud to umožňuje národní právo) a možnosti monitorovat řádné fungování zařízení po jejich instalaci na letištích.

Cestující by měli být před prohlídkou tělesným skenerem informováni odpovídajícím způsobem o tomto zařízení a o svém právu na ochranu osobních údajů. Letištní orgány by měly úzce spolupracovat s úřady pro ochranu dat, aby zajistily, že informace budou splňovat zákonem stanovené požadavky.

¹ Pracovní skupina podle článku 29 přijala 11. února 2009 dokument ohledně tělesných skenerů. Tento dokument a průvodní dopis Evropské komisi se nacházejí na následujících stránkách: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/others/2009_05_11_letter_chairman_art29wp_daniel_calleja_dgtren_en.pdf
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/others/2009_05_11_annex_consultation_letter_chairman_art29wp_daniel_calleja_dgtren_en.pdf

² Např. ruční detektory nebo cvičení psi.

2. Rezoluce k chystané dohodě mezi Evropskou unií a Spojenými státy americkými o standardech ochrany osobních údajů v oblasti policie a soudní spolupráce v trestních věcech

Na základě závěrečné zprávy tzv. Kontaktní skupiny na vysoké úrovni (High Level Contact Group) hodlají zástupci Evropské unie a Spojených států amerických začít dojednávat dohodu o standardech ochrany osobních údajů v oblasti policejní a soudní spolupráce v trestních věcech.

Evropští komisaři ochrany dat tento projekt velmi vítají. Chovají značnou naději, že touto dohodou se EU a USA zavážou k vysoké úrovni ochrany dat při výměně osobních údajů v trestních věcech, a tak vytvoří model pro další dohody o mezinárodní výměně osobních údajů v oblasti prosazování práva.

Evropští komisaři ochrany dat připisují této dohodě velkou důležitost, neboť vzhledem k mezinárodnímu terorismu i ke kriminalitě překračující hranice nároky na mezinárodní spolupráci orgánů prosazujících právo s největší pravděpodobností porostou, a tudíž se bude téma podmínek mezinárodní výměny osobních údajů mezi orgány prosazujícími právo stále častěji objevovat v politické agendě.

Konference evropských komisařů ochrany dat a soukromí vyzývá v tomto smyslu Evropskou unií k silné obhajobě

vysoké úrovně ochrany dat a – prostřednictvím této dohody – k účinnému zajištění neměnných principů – zejména přísného omezení účelu předávání údajů, vysoké úrovně bezpečnosti dat, existence nezávislých orgánů pro ochranu osobních údajů, práva přístupu a soudní náhrady pro všechny subjekty údajů bez ohledu na národnost nebo zemi pobytu – a to také při výměně osobních údajů s USA.

3. Rezoluce k problematice dalšího vývoje v oblasti ochrany osobních údajů a soukromí

Konference připomíná pozitivní výsledky v oblasti ochrany osobních údajů a zejména oceňuje, že Lisabonská smlouva výslovně uznává ochranu dat jako základní právo. Vývoj v této oblasti prohloubí důvěru v informační společnost.

Nad výše uvedené Konference bere v úvahu, že:

- ochrana osobních údajů čelí zásadním výzvám souvisejícím se zaváděním nových informačních technologií a s globalizací;
- roste poptávka, především v souvislosti s bojem proti závažné trestné činnosti a terorismu, po druhotném užívání osobních údajů, které původně byly shromážděny k jiným účelům.

Maje na zřeteli, že tyto skutečnosti opakovaně staví do popředí potřebu vhodného systému úpravy ochrany osobních údajů, který by zaručoval vysokou a odpovídající úroveň ochrany. Přihlížeje k riziku úprav právního systému v oblasti ochrany osobních údajů, které by snížily úroveň ochrany nebo dokonce opomíjely nebo obcházely etablované zásady:

- zásada zákonného a korektního shromažďování a zpracování dat,
- zásada přesnosti,
- zásada stanovení a omezení účelu,
- zásada proporcionality,
- zásada transparentnosti,
- zásada účasti, zejména záruka práva subjektu údajů na přístup k údajům a na informaci,
- zásada nediskriminace,
- zásada bezpečnosti dat,
- zásada odpovědnosti,
- zásada nezávislého dozoru a zákonných sankcí,
- zásada přiměřené úrovně ochrany pro mezinárodní přenosy osobních údajů.

Konference:

- prohlašuje, že ochrana osobních údajů a soukromí zůstává významným výdobytkem naší civilizace. Je nezbytné zachovávat ochranu základních práv také v budoucnu. Zásady ochrany osobních údajů proto musejí být účinné a důsledně dodržovány, aby se předešlo následkům pramenícím z neustálého sledování a neomezeného profilování občanů, což může mít nežádoucí dopady včetně nepatřičné kategorizace jednotlivců;

- dále prohlašuje, že základní principy ochrany osobních údajů by se měly nadále uplatňovat i přes výše uvedené výzvy;
- vybízí naléhavě zákonodárce a další zainteresované strany, aby nepřetržitě pracovali na vyváženém přístupu k aktuálním problémům a zajišťovali ochranu osobních údajů jako základní právo;
- připomíná znovu své prohlášení z krakovské Jarní konference v roce 2005, že takovým výzvám by se mělo čelit na míru šitými pravidly ochrany dat pro oblast prosazování práva;
- vítá a potvrzuje doporučení Pracovní skupiny pro ochranu dat podle článku 29 s ohledem na současné diskuse o budoucnosti ochrany soukromí směřující k dosažení vyšší efektivity v oblasti ochrany osobních údajů v globálním prostředí.

Zejména je nezbytné:

- trvat na úrovni národní i v EU na jasném stanovení, kdo nese odpovědnost za zpracování a ochranu osobních údajů. Dále trvat na tom, že souhlas subjektu údajů je jedním ze základních předpokladů zákonného zpracování dat, a dále trvat na přísných, zákonem stanovených ochranných opatřeních pro druhotné využívání osobních údajů. A také usilovat o to, aby rozsah veškerých byrokratických opatření souvisejících s ochranou osobních údajů zůstal omezený;
- vyžadovat, aby před přijetím nových zákonných opatření nebo nasazením nových informačních technologií byl vzat v úvahu koncept „privacy by design“ nebo, v případě nutnosti, bylo provedeno náležité a prokazatelné posouzení dopadů v takové míře, aby případné narušení soukromí nepřevážilo nad zamýšlenou účinností chystaného právního opatření nebo informační technologie;
- usilovat na národní i evropské úrovni o vytvoření úplné soustavy pravidel pro ochranu osobních údajů ve všech oblastech (včetně boje proti zločinu a terorismu);
- usilovat o přijetí celosvětových závazných standardů ochrany osobních údajů založených na mezinárodních standardech vypracovaných v roce 2009 na Konferenci o ochraně dat v Madridu a dále také podporovat úsilí Rady Evropy prosadit přistoupení zemí třetího světa k Úmluvě 108 a jejímu dodatkovému protokolu.

4. Rezoluce o přípravě společných kroků zaměřených na informovanost a vzdělávání mladých lidí na evropské a mezinárodní úrovni

Přestože Úmluva Spojených národů o právech dítěte z 20. listopadu 1989 právě oslavila dvacáté narozeniny, je třeba si přiznat, že výzva Spojených národů vytvářet „svět vhodný pro děti“ zůstává nenaplněna. To platí zejména v oblasti zabezpečení ochrany soukromí dětí v současné „digitální éře“.

V dnešní době mladí lidé v Evropě a všude po celém světě denně užívají internet a další komunikační prostředky, aby si vyměňovali zprávy, fotky, videa a jiné informace, což jsou údaje, které se mohou týkat přímo jich samotných nebo například jejich kamarádů, rodičů anebo učitelů. Tyto nové komunikační prostředky mohou přispívat k lepšímu šíření nápadů a znalostí. Mladí lidé (stejně jako dospělí) si ale většinou neuvědomují, že osobní údaje, které sdělují, zanechávají stopy odhalující jejich životní zvyky a chování. Takové osobní údaje mohou být využity ke komerčním účelům, k profilování a v některých případech dokonce k trestné činnosti.

Je důležité si také uvědomit, že i když některé sociální sítě vyžadují pro registraci minimální věk 13 let, je na těchto sítích zaregistrováno hodně mladých lidí pod touto věkovou hranicí.

Čelit těmto závažným problémům, které se objevily v souvislosti s novými vývojovými trendy, znamená pro naše úřady nutnost vykonávat dozor a dohled nad činností sociálních sítí a dalších hráčů ve světě informačních a sdělovacích technologií. Obvyklá praxe poskytovatelů sociálních sítí se příliš často zakládá na tzv. „svobodném a informovaném souhlasu“ zahrnujícím informace, které jsou především pro mládež složité a nesrozumitelné. Takový postup neposkytuje odpovídající úroveň ochrany dětských práv. Nadto by měla být přijata mnohem účinnější opatření, která zajistí, že mladým lidem v jejich běžném životě bude dostatečným způsobem zaručeno právo „být zapomenut“, a to zejména prostřednictvím práva na vymazání osobních údajů.

Zároveň naše úřady musejí orientovat svou činnost na mládež samotnou. Podpora povědomí mladých generací o nebezpečích ukrytých v nových technologiích a o využívání těchto technologií společensky odpovědným způsobem při respektování sebe i druhých, zejména jejich soukromí (a jejich osobních údajů), se pro naši evropskou civilizaci musí stát cílem nejvyšší důležitosti.

V tomto směru již byly na mezinárodních i na národních úrovních podniknuty různé aktivity.

Během třicáté Mezinárodní konference komisařů ochrany dat a soukromí, v říjnu 2008 ve Štrasburku, schválilo 60 zástupců dozorových orgánů ze všech světadílů dvě rezoluce, o službách sociálních sítí a o soukromí dětí na síti. V březnu 2008 přijala Mezinárodní pracovní skupina pro ochranu dat v telekomunikacích (tzv. Berlínská skupina) „Římské memorandum“ o službách sociálních sítí¹. Výbor ministrů Rady Evropy², složený ze 47 členských států a Pracovní skupina WP 29 Evropské unie³ jsou do této problematiky také zapojeny.

Kromě toho Evropská komise vedle uvedeného vytvořila program Bezpečnější internet⁴, který si klade za cíl financovat projekty k vytvoření ochranného rámce pro

komunikační služby, jako jsou “network sites“. Také vypracovala „Zásady pro bezpečnější sociální sítě v Evropské unii“⁵. Zavedení těchto principů na dobrovolné bázi a prostřednictvím prohlášení o souladu je pozitivní krok. Je třeba dál pokračovat tak, aby se tato pravidla stala obsahovým základem závazných pravidel platných pro všechny společenské sítě.

Mnohé země v Evropě, i mimo ni, již zavedly na národní úrovni novátorské, netradiční postupy v oblasti edukativních a osvětových aktivit zaměřených na děti. Takové iniciativy je nezbytné podporovat a učit se z nich a v rámci mezinárodní spolupráce tyto pro-aktivní postupy rozšiřovat. Proto Evropská konference komisařů ochrany dat a soukromí znovu potvrzuje své rozhodnutí učinit všechna potřebná opatření k zajištění skutečné a účinné ochrany soukromí dětí na internetu, především na jeho sociálních sítích. Evropská konference dále podporuje:

- evropské úřady pro ochranu osobních údajů k vyvinutí nástrojů, které zohlední specifika ochrany soukromí mladých lidí; především vyzývá správce dat k přijímání takových zásad ochrany soukromí, kterým budou mladí lidé při čtení skutečně rozumět;
- vládní iniciativy k vytvoření zvláštních předpisů, které výrazným způsobem posílí zabezpečení ochrany osobních údajů a soukromí mladých lidí;
- vládní iniciativy zavádějící propagaci základních principů ochrany osobních údajů jako povinnou součást školních vzdělávacích programů;
- vytvoření školicích modulů věnovaných ochraně osobních údajů ve vyšším vzdělávání, vyškolení kompetentních pracovníků pro vzdělávání mládeže a také vytvoření specifických struktur pro zvyšování povědomí mezi

mladými, které budou jasně identifikované a viditelné pro veřejnost;

- spolupráci a výměnu informací mezi úřady pro ochranu osobních údajů na evropské a globální úrovni za účelem rozvinout opatření ke vzdělávání mladých lidí a sestavit přehled nástrojů pro zvyšování povědomí, které byly v různých evropských zemích vytvořeny.

¹ Viz <http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdp/working-papers-and-common-positions-adopted-by-the-working-group> ;

² Viz Deklarace o ochraně důstojnosti, bezpečí a soukromí dětí na internetu ze dne 20. března 2008; [https://wcd.coe.int/ViewDoc.jsp?Ref=Decl\(20.02.2008\)&Language=lanEnglish&Ver=0001&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75](https://wcd.coe.int/ViewDoc.jsp?Ref=Decl(20.02.2008)&Language=lanEnglish&Ver=0001&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75) ;

³ Viz Stanovisko 2/2009 ze dne 11. března 2009 k ochraně osobních údajů dětí (http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp160_en.pdf) a Stanovisko 5/2009 ze dne 12. června 2009 k internetovým sociálním sítím (http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf);.

⁴ Rozhodnutí č. 854/2005/CE z 11. května 2005 a Rozhodnutí č. 1351/2008/EC Evropského parlamentu a Rady o vytvoření víceletého programu Společenství na ochranu dětí užívajících internet a jiné komunikační technologie;

⁵ http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=5565;

Poznámka:

Rezoluce jsou k dispozici také na webových stránkách Úřadu <http://www.uoou.cz> v rubrice Zahraničí/Mezinárodní aktivity Úřadu.

Pracovní skupina pro ochranu údajů zřízená podle článku 29.



**02318/09/CS
WP167**

**Stanovisko 8/2009
k problematice ochrany údajů o cestujících shromažďovaných
a zpracovávaných bezcelními prodejnami na letištích a v přístavech**

přijaté dne 1. prosince 2009

Tato pracovní skupina byla zřízena podle článku 29 směrnice 95/46/ES. Je to nezávislý evropský poradní orgán pro ochranu údajů a soukromí. Její úkoly jsou popsány v článku 30 směrnice 95/46/ES a článku 15 směrnice 2002/58/ES.

Sekretariát poskytuje ředitelství C (Civilní soudnictví, práva a občanství) Evropské komise, generální ředitelství pro spravedlnost, svobodu a bezpečnost, B-1049 Brusel, Belgie, kancelář č. LX-46 01/190.

Internetové stránky: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

Pracovní skupina pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů

zřízená směrnicí 95/46/ES Evropského parlamentu a Rady ze dne 24. října 1995, s ohledem na článek 29 a čl. 30 odst. 1 písm. a) a článek 3 uvedené směrnice a čl. 15 odst. 3 směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002, s ohledem na článek 255 Smlouvy o ES a nařízení Evropského Parlamentu a Rady (ES) č. 1049/2001 ze dne 30. května 2001 o přístupu veřejnosti k dokumentům Evropského parlamentu, Rady a Komise, s ohledem na vlastní jednací řád,

přijala toto

stanovisko č. 8/2009 k problematice ochrany údajů o cestujících shromažďovaných a zpracovávaných bezcelními prodejny na letištích a v přístavech

Úvod

Právo Společenství umožňuje osvobodit od spotřebních daní nákupy prováděné cestujícími v bezcelních prodejnách na letištích a v přístavech. Takové nákupy však podléhají určitým podmínkám.

Aby tyto podmínky splnila, při nákupu zboží většina prodejen v členských státech EU shromažďuje a zpracovává údaje včetně údajů o cestujících.

Praxe shromažďování a zpracování takových údajů o cestujících se však v jednotlivých bezcelních prodejnách v Evropě značně liší.

Cestující nejsou vůbec informováni o sběru údajů včetně jejich osobních údajů, o účelu tohoto sběru, o svých právech a o využívání těchto podrobností veřejnými orgány, pokud jim jsou takové údaje předávány.

V souladu s článkem 30 směrnice 95/46/ES požádala Evropská komise pracovní skupinu zřízenou podle článku 29, aby se touto problematikou zabývala a posoudila současnou praxi v členských státech EU v souvislosti s otázkami ochrany údajů, aby v případě potřeby vydala doporučení o jednotném uplatňování všeobecných zásad ochrany údajů, jež mají bezcelní prodejny na letištích a v přístavech dodržovat.

Toto stanovisko rozebírá právní a praktické otázky ohledně sběru a zpracování údajů o cestujících v bezcelních prodejnách a jeho cílem je poskytnout pokyny obchodníkům a celním orgánům, které mají dohlížet na provádění práva Společenství, za účelem harmonizovanějšího uplatňování stávajících ustanovení.

Právní rámec

Osvobození od spotřebních daní je založeno na těchto právních předpisech Společenství, které jsou provedeny do vnitrostátních právních řádů a členskými státy prováděny.

a) směrnice Rady 92/12/EHS ze dne 25. února 1992,

která má být nahrazena

b) směrnicí Rady 2008/118/ES ze dne 16. prosince 2008 o obecné úpravě spotřebních daní a o zrušení směrnice 92/12/EHS (směrnice o spotřebních daních). Směrnice vstoupí v platnost dne 1. dubna 2010.

Zatímco směrnice 92/12/EHS problematiku osvobození neupravuje, směrnice 2008/118/ES poskytuje jasný právní základ, podle kterého by mohlo být zboží osvobozeno v tzv. bezdaňových nebo bezcelních prodejnách v Evropské unii.

Článek 14 směrnice o spotřebních daních stanoví podmínky, za kterých lze zboží podléhající spotřební dani osvobodit od placení spotřební daně způsobilými cestujícími.

Toto nařízení se vztahuje na zboží prodávané bezdaňovými prodejny, které je převáženo v osobních zavazadlech cestujících do třetí země (nebo na třetí území) uskutečňujících let nebo námořní cestu.

Pro účely uvedené směrnice platí následující definice uvedená v čl. 14 odst. 4 písm. b): „*cestujícím na třetí území nebo do třetí země*“ se rozumí každý cestující, jenž je držitelem cestovního dokladu opravňujícího k letecké či námořní dopravě, v němž je jako konečné místo určení uvedeno letiště či přístav nacházející se na třetím území nebo ve třetí zemi.

V důsledku těchto ustanovení lze od spotřebních daní osvobodit dosti omezené množství zboží, pokud má cestující cestovní doklad jako například palubní vstupenku nebo lístek na trajekt a kromě toho musí z Evropské unie odjet do přístavu, který leží mimo území Společenství. Není však požadováno, aby cestující bydlel mimo EU.

Aby nedocházelo k zneužívání osvobození, směrnice v čl. 14 odst. 3 stanoví, že členské státy musí přijmout opatření nezbytná k zajištění toho, aby osvobození od daně byla používána tak, aby bylo zabráněno možným daňovým únikům, vyhýbání se daňovým povinnostem nebo zneužití daňového režimu.

Směrnice 92/12/EHS ani směrnice 2008/118/ES neobsahuje žádnou zmínku o ustanoveních o ochraně údajů. Z toho důvodu je nutno používat všeobecná ustanovení směrnice 95/46/ES.

Různé praktiky v Evropě

Na základě žádosti Evropské komise předložené v létě 2009 pracovní skupina zřízená podle článku 29 zahájila šetření způsobu shromažďování údajů o cestujících bezcelními prodejny a způsobu, jakým jsou tyto údaje zpracovávány samotnými prodejny a jinými subjekty. Výsledný obraz ukazuje, že se praxe v bezcelních prodejnách v různých zemích Evropy značně liší, což by mohlo být způsobeno rozdílnými výklady

práva Společenství nebo vnitrostátních právních předpisů nebo skutečností, že směrnice o spotřebních daních vstoupí v platnost až 1. dubna 2010.

Během svého šetření pracovní skupina zřízená podle článku 29 zjistila následující čtyři obecné vzorce, které mohou být v některých členských státech odlišné.

1 Nákup výrobků bez daně není možný bez uvedení čísla letu. Za účelem kontroly, zda cestující splňuje podmínky pro osvobození od spotřební daně, a aby nedocházelo k nedorozuměním nebo diskusím s cestujícími, musí cestující ukázat pokladní(mu) svou palubní vstupenku, která je elektronicky zkontrolována, aby byl zjištěn způsobilý let. Žádné jiné údaje jako například jméno nebo číslo pasu se neshromažďují a neukládají. Pokud let skutečně míří do cílového místa mimo EU, na pokladně se ukáže snížená částka, kterou má zákazník zaplatit.

Údaje o letu a zakoupených položkách, které si cestující vzal na palubu letadla, se ukládají na dobu 10 let, aby mohla být později provedena kontrola bezcelní prodejny příslušnými celními orgány.

2 V jiném členském státu bezcelní prodejny na letištích shromažďují velké množství údajů o cestujících. V případě nákupů zboží osvobozeného od spotřebních daní příslušné celní předpisy stanoví, že za účelem umožnění kontroly musí všichni prodejci uchovávat podrobnou stvrzenku, na které je kromě jiných informací uvedeno i prvních pět písmen z označení totožnosti kupujícího, prvních pět písmen nebo číslic z čísla letu, cílové místo letu a datum transakce.

Letištní prodejny shromažďují tyto údaje buď snímáním palubních vstupenek prostřednictvím optických čteček nebo ručním zapsáním údajů. Kromě toho shromažďují ještě další údaje, jako je například povaha, počet a hodnota zakoupených položek, totožnost kupujících (15 písmen), a všechny tyto podrobnosti uchovávají v elektronické podobě v ústřední databázi po dobu tří let. Neshromažďují se však žádné citlivé údaje. Díky tomuto postupu lze snadno identifikovat určité cestující a sestavovat databáze položek zakoupených bez daně jednotlivými cestujícími za určité období.

3 V jiných členských státech bezcelní prodejny shromažďují pouze informace o cílovém místě letu (číslo letu) za účelem kontroly, zda se jedná o let v rámci EU, nebo o let mimo území EU, aniž by číslo letu zaznamenávaly. Žádné další údaje se neshromažďují a neukládají.

Ve všech těchto případech pracovní skupina zřízená podle článku 29 zjistila, že žádná bezcelní prodejna neposkytovala cestujícím žádné informace o tom, proč jsou shromažďována čísla letů nebo jak jsou údaje ukládány.

4 V jednom členském státě nejsou bezcelní prodejny od cestujících shromažďovány vůbec žádné údaje bez ohledu na to, zda si kupují zboží osvobozené od spotřební daně, či nikoli, nebo zda se jedná o let v rámci území Evropy, nebo o let mimo území Evropy.

Zde uvedené příklady jasně ukazují, že současná praxe v Evropě není jednotná a že navzdory výslovným ustanovením směrnice o spotřebních daních si členské státy vypracovaly rozdílné metody řešení nákupů bez spotřební daně. I když v některých případech, jak je uvedeno výše, nejsou shromažďovány vůbec žádné údaje, v jiných

členských státech musí cestující poskytovat velké množství informací, které jsou pak ukládány. Také doba, po kterou jsou tyto informace uchovávány, vykazuje značné rozdíly.

Kromě otázek ochrany údajů nastolují tyto rozdílné praktiky otázku, zda jsou v souladu s ustanoveními směrnice o spotřebních daních, která členským státům jasně ukládá povinnost přijmout veškerá nezbytná opatření, aby nedocházelo k zneužívání a daňovým únikům.

Zásady ochrany údajů

Jak již bylo zmíněno výše, tyto směrnice neobsahují žádná ustanovení o ochraně údajů a z toho důvodu se musí používat všeobecné zásady směrnice 95/46/ES, jelikož osobní údaje by mohly být zpracovávány bezcelními prodejny a celními orgány, což je nutno považovat za činnost patřící do prvního pilíře.

Mezi tyto obecné zásady mimo jiné patří:

- zákonnost,
- omezení účelu,
- údaje nesmí být nadměrné a musí být přiměřené a přesné,
- údaje nesmí být dále zpracovávány k neslučitelným účelům,
- přiměřená doba uchování údajů,
- dostatečné informování subjektů údajů.

Kromě toho může být v určitých členských státech vyžadován postup předběžného oznámení.

Práva subjektů údajů

Práva subjektů údajů (osob, jichž se údaje týkají), která jsou stanovena v člancích 10, 11 a 13 a 14 směrnice, se musí uplatňovat také tehdy, když cestující kupují zboží v bezcelních prodejnách a přitom jsou shromažďovány a zpracovávány jejich osobní údaje. Na případy, kdy jsou shromažďovány citlivé údaje, se vztahuje článek 8 směrnice.

Použitelnost zásad ochrany údajů

Praxe uvedená pod číslem 3, kdy se shromažďují omezené informace o cílových místech letů, a pod číslem 4, kdy bezcelní prodejny v jednom členském státu vůbec neshromažďují osobní údaje, zajisté z hlediska ochrany údajů nejvíce respektuje soukromí a měla by být podporována, pokud umožňuje účinné uplatňování směrnice o spotřebních daních. Směrnice skutečně ukládá členským státům povinnost přijímat opatření nezbytná k zamezení zneužívání a daňových úniků a k boji proti těmto jevům. Jakákoli taková opatření by mohla zahrnovat sběr některých údajů jako vhodný a nezbytný prostředek plnění těchto úkolů.

V případě uvedeném pod číslem 2, kdy jeden členský stát shromažďuje velké množství osobních údajů, klade pracovní skupina zřízená podle článku 29 otázku, jak je tato praxe slučitelná se zásadami minimalizace a přiměřenosti údajů. Množství shromažďovaných údajů se zdá být nadměrné a zbytečné pro účely určení, zda je cestující způsobilý pro osvobození od spotřebních daní.

V případech, kdy se neshromažďují žádné přímé osobní údaje (příklady č. 1 a č. 3), by mohl být cestující identifikován pouze nepřímo. Tato praxe je v souladu s přijatými zásadami ochrany údajů, jelikož se shromažďuje jen velmi omezené množství údajů, tj. číslo nebo cílové místo letu, a tyto informace, pokud jsou uchovávány, se ukládají na omezenou dobu, aby se mohla provádět vládní kontrola k zamezení případů zneužívání.

Co se týče dob uchování údajů, zde uvedené příklady se také značně liší. Zatímco v případech uvedených pod číslem 3 a 4 se neukládají vůbec žádné údaje, v případech uvedených pod číslem 1 a 2 doba uchování údajů činí tři roky, respektive deset let.

Podle čl. 6 písm. e) směrnice 95/46/ES by údaje měly být uchovávány po dobu ne delší, než je nezbytné k uskutečnění cílů, pro které byly shromážděny.

Vzhledem k tomu, že členské státy musí přijmout nezbytná opatření, aby nedocházelo k zneužívání a daňovým únikům, mohlo by být vyžadováno ukládání některých údajů za účelem kontroly a analýz způsobu, jakým bezcelní prodejny provozují svou činnost.

Zatímco pro některé orgány je dostačující tříletá doba uchování údajů, je otázkou, proč jiné orgány potřebují desetiletou dobu uchování. Mělo by se zvážit zkrácení této doby a v každém případě by neměla být tato doba delší než jakékoli jiné doby uchování údajů za srovnatelných okolností, jako je například uchovávání faktur pro daňové účely. Doporučuje se také harmonizovat doby uchovávání údajů v rámci celé Evropy, jelikož se to týká všech cestujících, na něž se vztahuje tatáž směrnice 2008/118/ES.

Další zpracování osobních údajů celními orgány při jejich zákonné činnosti je v souladu se směrnicí 2008/118/ES a zásadami ochrany údajů. Jakékoli jiné zpracování osobních údajů shromážděných při nákupu položek zakoupených bez daně by mělo podléhat přísným omezením v souladu se zásadami směrnice 95/46/ES.

Závěr a doporučení

Bezcelní prodejny na letištích a v přístavech shromažďují a zpracovávají údaje včetně osobních údajů za účelem ověření, zda mohou být jejich zákazníci osvobozeni od spotřebních daní. Většinou tyto údaje uchovávají pro celní orgány jako doklad toho, že postupují správně. Celní orgány by také mohly zpracovávat a uchovávat tyto údaje pro své vlastní účely včetně statistických účelů.

Výše uvedené směrnice poskytují jasný právní základ, co se týče sběru, zpracování a uchovávání určitých údajů obsažených v dopravních dokladech cestujících, aniž by obsahovaly zvláštní ustanovení o ochraně údajů, takže je nutno používat zásady směrnice 95/46/ES.

Prodejny a celní orgány by si však měly uvědomit, že sběr údajů by měl být omezen na nezbytně nutnou míru při uplatnění zásady minimalizace údajů. V příkladu č. 2 nejsou respektovány zásady nezbytnosti a přiměřenosti. Většinou by měly prodejny potřebovat pouze zjišťovat číslo nebo cílové místo letu uvedené na palubní vstupence, aby určily příslušné spotřební daně, jak je uvedeno v příkladu č. 3 v tomto stanovisku. To by bylo přiměřené a nikoli nadměrné. Pokud se sbírá více údajů, měla by existovat jasná potřeba takových údajů v konkrétních případech.

Údaje by se neměly používat pro účely prosazování práva, pokud nejsou nezbytné jako důkazy zneužívání v konkrétních případech (žádné hromadné předávání policii).

Údaje by neměly být používány k jiným účelům neslučitelným s původním účelem (předávání údajů bez informování nebo souhlasu subjektů údajů třetím osobám, například dopravcům), pokud neslouží k statistickým účelům.

Neměly by se provádět žádné systematické přehledy nákupů zákazníků umožňující rozbor jejich chování a nákupních zvyklostí.

Doba uchování údajů by měla být omezena na nejnezbytnější dobu a měla by být harmonizována v celé Evropě.

Jedním z hlavních výsledků šetření pracovní skupiny zřízené podle článku 29 je to, že cestující jsou nedostatečně informováni. I když bezcelní prodejny údaje jen sbírají, ale neukládají, měl by o tom zákazník vědět. Pokud se však údaje ukládají, je o to nezbytnější poskytovat informace o tom, jaké údaje se ukládají, k jakému účelu, na jak dlouho a jak lze získat další podrobnosti. Zúčastněné strany by v této oblasti mohly dělat více, například vyvěšením příslušných informačních tabulí v bezcelních prodejnách nebo rozdáváním letáků. Množství informací, které lze cestujícím poskytovat, je uvedeno v dokumentu WP 100 a jeho přílohách, který pracovní skupina zřízená podle článku 29 přijala v listopadu 2004¹.

Stávající rozdílné praktiky popsané v tomto stanovisku vyvolávají obavu, že ustanovení směrnice o spotřebních daních ani ustanovení o ochraně údajů nejsou bezcelními prodejnami v rámci celé Evropy jednotně používána a dodržována. Zdá se nezbytné dále harmonizovat stávající praxi a zvýšit povědomí cestujících, co se týče sběru a zpracování údajů při nákupu položek bez daně.

Orgánům na ochranu údajů v členských státech EU se doporučuje navázat kontakt s majiteli prodejen a letištními orgány za účelem nápravy případných nedostatků tak, aby byla stávající praxe uvedena do souladu s použitelným právem a ustanoveními o ochraně údajů. Informování cestujících, co se týče nákupů bez daně, lze a mělo by se zlepšit. Prodejny, letiště, přístavy, spotřebitelské organizace a další zúčastněné strany by se měly snažit poskytovat cestujícím relevantní informace, aby cestující mohli uplatňovat svá práva při nákupu výrobků bez daně.

V Bruselu dne 1. prosince 2009

Za pracovní skupinu
předseda
Alex Türk

¹ http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_cs.pdf

**PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ
ZŘÍZENÁ PODLE ČLÁNKU 29**



**00264/10/CS
WP 169**

Stanovisko č. 1/2010 k pojmům „správce“ a „zpracovatel“

Přijaté dne 16. února 2010

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

Její sekretariát je na Ředitelství D (Základní práva a občanství) Evropské komise, Generální ředitelství pro spravedlnost, svobodu a bezpečnost, B-1049 Brusel, Belgie, kancelář č. LX-46 01/190.

Internetové stránky: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

OBSAH

Shrnutí.....	3197
I. Úvod	3198
II. Obecné poznámky a otázky politiky	3199
II.1. Úloha pojmů	3200
II.2. Příslušný kontext	3201
II.3. Některé hlavní problémy	3202
III. Analýza definic.....	3202
III.1. Definice správce	3202
III.1.a) Úvodní prvek: „určuje“	3203
III.1.b) Třetí prvek: „účel a prostředky zpracování“	3207
III.1.c) První prvek: „fyzická osoba, právnická osoba nebo jakýkoli jiný subjekt“	3209
III.1.d) Druhý prvek: „sám nebo společně s jinými“	3212
III.2. Definice zpracovatele	3218
III.3. Definice třetí osoby.....	3224
IV. Závěry	3225

Shrnutí

Pojem správce údajů a jeho vzájemný vztah s pojmem zpracovatel údajů hrají při uplatňování směrnice 95/46/ES zásadní úlohu, jelikož určují, kdo je odpovědný za dodržování pravidel pro ochranu údajů, jak mohou subjekty údajů vykonávat svá práva, jaké je použitelné vnitrostátní právo a jak účinně mohou působit orgány pro ochranu údajů.

Organizační diferenciaci ve veřejném a v soukromém sektoru, rozvoj IKT, jakož i globalizace zpracování údajů zvyšují složitost způsobu zpracovávání osobních údajů a vyžadují objasnění těchto pojmů v zájmu zajištění účinného uplatňování a dodržování v praxi.

Pojem správce je nezávislý v tom smyslu, že je nutno jej vykládat především podle právních předpisů Společenství v oblasti ochrany údajů, a praktický v tom smyslu, že má rozdělit odpovědnosti podle skutečného vlivu, je tudíž založen spíše na skutkové analýze než na formální analýze.

Definice ve směrnici obsahuje tři hlavní stavební kameny:

- osobní aspekt („*fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jakýkoli jiný subjekt*“);
- možnost mnohostranné kontroly („*který sám nebo společně s jinými*“) a
- zásadní prvky k odlišení správce od ostatních účastníků („*určuje účel a prostředky zpracování osobních údajů*“).

Analýza těchto stavebních kamenů vede k řadě závěrů, jež jsou shrnuty v bodě IV stanoviska.

Toto stanovisko analyzuje rovněž pojem zpracovatel, jehož existence závisí na rozhodnutí přijatém správcem, který může rozhodnout o zpracování údajů v rámci své organizace nebo o přenesení veškerých činností spojených se zpracováním či jejich části na externí organizaci. Dvěma základními podmínkami pro stanovení zpracovatele jsou na straně jedné to, že se s ohledem na správce jedná o samostatnou právnickou osobu, a na straně druhé je to zpracování osobních údajů pro správce.

Pracovní skupina uznává potíže při používání definic obsažených ve směrnici ve složitém prostředí, v němž lze předpokládat mnoho scénářů zahrnujících správce a zpracovatele, samostatně nebo společně, s různou mírou nezávislosti a odpovědnosti.

Ve své analýze pracovní skupina zdůraznila nutnost rozdělit odpovědnost tak, aby bylo v praxi dostatečně zajištěno dodržování pravidel pro ochranu údajů. Nezjistila však žádný důvod pro domněnku, že z tohoto hlediska již nebude stávající rozlišení mezi správcem a zpracovatelem relevantní a použitelné.

Pracovní skupina proto doufá, že vysvětlení obsažená v tomto stanovisku doložená konkrétními příklady převzatými z každodenních zkušeností orgánů pro ochranu údajů přispějí k účinným pokynům ke způsobu výkladu těchto hlavních definic směrnice.

Pracovní skupina pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů

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

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

s ohledem na svůj jednací řád,

přijala toto stanovisko:

I. Úvod

Pojem správce údajů a jeho vzájemný vztah s pojmem zpracovatel údajů hrají při uplatňování směrnice 95/46/ES zásadní úlohu, jelikož určují, kdo je odpovědný za dodržování pravidel pro ochranu údajů a jak mohou subjekty údajů v praxi vykonávat svá práva. Pojem správce údajů je rovněž zásadní pro určení použitelného vnitrostátního práva a účinné plnění úkolů v oblasti dozoru, které byly svěřeny orgánům pro ochranu údajů.

Je proto nanejvýš důležité, aby byl dostatečně jasný přesný význam těchto pojmů a kritéria pro jejich správné používání a aby byly sdíleny všemi subjekty v členských státech, které hrají úlohu při provádění směrnice a při uplatňování, hodnocení a prosazování vnitrostátních předpisů pro její uvedení v platnost.

Existují náznaky, že nemusí být zajištěna dostatečná jasnost, přinejmenším s ohledem na určité aspekty těchto pojmů, a že u odborníků v jednotlivých členských státech mohou existovat určité odlišné názory, jež mohou vést k odlišným výkladům stejných zásad a definic zavedených za účelem harmonizace na evropské úrovni. Pracovní skupina zřízená podle článku 29 se proto rozhodla věnovat v rámci svého strategického pracovního programu na období 2008–2009 zvláštní pozornost vypracování dokumentu, který stanoví společný přístup k těmto záležitostem.

Pracovní skupina uznává, že konkrétní použití pojmů správce údajů a zpracovatel údajů se stává stále složitějším. To je zapříčiněno především rostoucí složitostí prostředí, v němž jsou tyto pojmy používány, a zejména rostoucí tendencí k organizační diferenciaci v soukromém i veřejném sektoru společně s rozvojem IKT a globalizací způsobem, který může vést k novým a obtížným problémům a někdy může mít za následek nižší úroveň ochrany, jež je poskytována subjektům údajů.

Ačkoliv ustanovení směrnice byla z hlediska technologie formulována neutrálně, a dosud byla tudíž s to náležitě odolávat vyvíjejícímu se kontextu, tyto složitosti mohou skutečně vést k nejistotám, co se týká rozdělení odpovědnosti a oblasti působnosti použitelných vnitrostátních právních předpisů. Tyto nejistoty mohou mít negativní dopad na dodržování pravidel pro ochranu údajů v kritických oblastech a na účinnost celého práva v oblasti ochrany údajů. Pracovní skupina se již zabývala některými z těchto záležitostí

ve vztahu ke konkrétním otázkám¹, považuje však za nezbytné vydat nyní podrobnější pokyny a zvláštní vodítko s cílem zajistit jednotný a harmonizovaný přístup.

Pracovní skupina se proto rozhodla poskytnout v tomto stanovisku (podobně jak to již učinila ve stanovisku k pojmu osobní údaje²) určitá vysvětlení a některé konkrétní příklady³ s ohledem na pojmy správce údajů a zpracovatel údajů.

II. Obecné poznámky a otázky politiky

Směrnice v řadě ustanovení výslovně odkazuje na pojem správce. Definice „správce“ a „zpracovatele“ v čl. 2 písm. d) a e) směrnice 95/46/ES (dále jen „směrnice“) zní takto:

„správcem“ se rozumí fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jakýkoli jiný subjekt, který sám nebo společně s jinými určuje účel a prostředky zpracování osobních údajů; jsou-li účel a prostředky zpracování určeny právními a správními předpisy na úrovni jednotlivých států či Společenství, je možné určit správce nebo zvláštní kritéria pro jeho určení právem jednotlivých států nebo Společenství;

„zpracovatelem“ se rozumí fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jakýkoli jiný subjekt, který zpracovává osobní údaje pro správce.

Tyto definice byly vypracovány v průběhu jednání o předloze návrhu směrnice počátkem 90. let minulého století a pojem „správce“ byl v zásadě převzat z Úmluvy Rady Evropy č. 108, která byla uzavřena v roce 1981. V průběhu těchto jednání došlo k několika významným změnám.

Především byl „správce souboru údajů“ v úmluvě č. 108 nahrazen „správcem“ v souvislosti se „zpracováním osobních údajů“. Jedná se o široký pojem vymezený v čl. 2 písm. b) směrnice jako „jakýkoli úkon nebo soubor úkonů s osobními údaji, které jsou prováděny pomocí či bez pomoci automatizovaných postupů, jako je shromažďování, zaznamenávání, uspořádávání, uchovávání, přizpůsobování nebo pozměňování, vyhledávání, konzultace, použití, sdělení prostřednictvím přenosu, šíření nebo jakékoli jiné zpřístupnění, srovnání či kombinování, jakož i blokování, výmaz nebo likvidace“. Pojem „správce“ se tudíž již nepoužívá pro statický objekt („soubor údajů“), nýbrž souvisí s činnostmi odrážejícími životní cyklus informací od jejich shromažďování po likvidaci, a na toto je nutno pohlížet jednotlivě i celkově („úkon nebo soubor úkonů“). Ačkoliv v mnoha případech může být výsledek týž, pojem tímto získal mnohem širší a dynamičtější význam a oblast působnosti.

Další změny zahrnovaly zavedení možnosti „mnohostranné kontroly“ („sám nebo společně s jinými“), požadavek, aby správce „určil účel a prostředky zpracování osobních údajů“, a myšlenku, aby bylo toto určení provedeno právem jednotlivých států

¹ Viz například stanovisko č. 10/2006 ke zpracovávání osobních údajů Společností pro celosvětovou mezibankovní finanční komunikaci (Society for Worldwide Interbank Financial Telecommunication (SWIFT)), přijaté dne 22. listopadu 2006 (WP 128) a nedávno stanovisko č. 5/2009 k internetovým sociálním sítím, přijaté dne 12. června 2009 (WP 163).

² Stanovisko č. 4/2007 k pojmu osobní údaje, přijaté dne 20. června 2007 (WP 136).

³ Tyto příklady jsou založeny na stávající vnitrostátní nebo evropské praxi a případně byly pozměněny nebo upraveny s cílem zajistit lepší srozumitelnost.

nebo Společenství či jinak. Směrnice zavedla rovněž pojem „zpracovatel“, který není v úmluvě č. 108 zmíněn. Tyto a další změny budou podrobněji analyzovány v tomto stanovisku.

II.1. Úloha pojmů

Zatímco v úmluvě č. 108 hraje pojem správce (souboru údajů) velmi omezenou úlohu⁴, ve směrnici je tomu zcela jinak. Ustanovení čl. 6 odst. 2 výslovně stanoví, že „dodržování odstavce 1 zajistí správce“. To se vztahuje na hlavní zásady týkající se kvality údajů, včetně zásady uvedené v čl. 6 odst. 1 písm. a), že „osobní údaje musejí být zpracovány korektně a zákonným způsobem“. To ve skutečnosti znamená, že veškerá ustanovení, jež stanoví podmínky pro zákonné zpracování, jsou v zásadě určena správci, ačkoliv to není vždy výslovně uvedeno.

Ustanovení o právech subjektu údajů na informování, přístup k údajům, jejich opravu, výmaz a blokování a vznesení námitky vůči zpracování osobních údajů (články 10 až 12 a článek 14) byla koncipována tak, aby vytvářela povinnosti pro správce. Správce je rovněž hlavním subjektem v ustanoveních o oznámení a předběžných kontrolách (články 18 až 21). Nepřekvapuje, že správce je v zásadě považován za odpovědného rovněž za jakoukoli škodu způsobenou nedovoleným zpracováním (článek 23).

To znamená, že hlavním významem pojmu správce je určit, kdo je odpovědný za dodržování pravidel pro ochranu údajů a jak mohou subjekty údajů uplatňovat svá práva v praxi⁵. Jinými slovy: přidělit odpovědnost.

To se dotýká podstaty směrnice, jejímž prvním cílem je „chránit fyzické osoby v souvislosti se zpracováním osobních údajů“. Tohoto cíle lze v praxi dosáhnout a zajistit jeho účinnost pouze tehdy, je-li možné subjekty odpovědné za zpracování údajů právními či jinými prostředky dostatečně podnítit, aby přijaly veškerá opatření, která jsou nezbytná, aby byla tato ochrana zajištěna v praxi. To je potvrzeno v čl. 17 odst. 1 směrnice, podle něhož správce „musí přijmout vhodná technická a organizační opatření na ochranu osobních údajů proti náhodnému nebo nedovolenému zničení, náhodné ztrátě, úpravám, neoprávněnému sdělování nebo přístupu, zejména pokud zpracování zahrnuje předávání údajů, jakož i proti jakékoli jiné podobě nedovoleného zpracování“.

Prostředky k podněcování odpovědnosti mohou být aktivní a zpětně působící. V prvním případě je cílem zajistit účinné provádění opatření na ochranu údajů a dostatečnou odpovědnost u správců. V druhém případě mohou zahrnovat občanskoprávní odpovědnost a sankce s cílem zajistit, aby byla nahrazena případná škoda a aby byla přijata přiměřená opatření k nápravě případných chyb nebo přestupků.

⁴ Není použit v jakémkoli z hmotněprávních ustanovení, vyjma v čl. 8 písm. a) ve vztahu k právu být informován (zásada transparentnosti). Správce jako odpovědná strana je uváděn pouze v některých částech důvodové zprávy.

⁵ Viz rovněž 25. bod odůvodnění směrnice 95/46/ES: „vzhledem k tomu, že zásady ochrany se musí odrazit jednak v povinnostech jednotlivců, orgánů veřejné moci, podniků, agentur nebo jiných subjektů odpovědných za zpracování údajů týkajících se zejména kvality údajů, technického zabezpečení, oznamování okolností, za jakých může být zpracování provedeno, orgánu dozoru a jednak v právu poskytnutému osobám, jejichž údaje jsou zpracovávány, být informován o tom, že jsou zpracovávány, právu přístupu k údajům, právu žádat jejich opravu a právu odmítnout za určitých okolností zpracování“.

II.2. Příslušný kontext

Rozdílný vývoj příslušného prostředí vedl k větší naléhavosti těchto otázek a rovněž jejich větší složitosti než dříve. V době podpisu úmluvy č. 108 a do značné míry rovněž při přijetí směrnice 95/46/ES byl kontext zpracování údajů dosud poměrně jasný a srozumitelný, nyní to však již neplatí.

To je zapříčiněno v prvé řadě rostoucí tendencí směrem k organizační diferenciaci v nejdůležitějších odvětvích. V soukromém sektoru vedlo rozdělení finančních či jiných rizik k probíhající diverzifikaci společností, která se jen zvyšuje spojením podniků a akvizicemi. Ve veřejném sektoru dochází k podobné diferenciaci v rámci decentralizace nebo oddělení politických orgánů a výkonných agentur. V obou sektorech se zvyšuje důraz na rozvoj dodavatelských řetězců nebo poskytování služeb napříč organizacemi a na využívání subdodávek či externího zajišťování služeb s cílem využít specializace a možných úspor z rozsahu. V důsledku toho se zvyšují různé služby nabízené poskytovateli služeb, kteří se ne vždy považují za odpovědné. Kvůli organizačním rozhodnutím společností (a jejich dodavatelů nebo subdodavatelů) se mohou příslušné databáze nacházet v jedné či více zemích v Evropské unii i mimo ni.

Rozvoj informačních a komunikačních technologií (dále jen „IKT“) tyto organizační změny velkou měrou usnadnil a připojil rovněž několik vlastních změn. Odpovědnosti na různých úrovních (často výsledek organizační diferenciaci) obvykle vyžadují a podporují rozsáhlé využívání IKT. Vývoj a využívání produktů a služeb v oblasti IKT vede rovněž k novým úlohám a odpovědnostem na jejich základě, které nejsou vždy jednoznačně ve vzájemném vztahu se stávajícími nebo vyvíjejícími se odpovědnostmi v organizacích zákazníků. Je proto důležité být si vědom příslušných rozdílů a v případě potřeby objasnit odpovědnosti. Zavedení mikrotechnologie – například čipů RFID ve spotřebních výrobcích – vyvolává podobné otázky v souvislosti s přesunem odpovědnosti. Na druhou stranu existují nové a složité problémy spojené s využíváním rozloženého výpočtu, zejména tzv. „cloud computing“ a „sítě“⁸.

Dalším komplikujícím činitelem je globalizace. Pokud organizační diferenciaci a rozvoj IKT zahrnují několik jurisdikcí, jako tomu často je například v případě internetu, otázky týkající se použitelného práva musí vzniknout nejen v rámci EU nebo EHP, nýbrž rovněž ve vztahu k třetím zemím. Příkladem může být antidopingový kontext, kdy Světová antidopingová agentura (WADA) se sídlem ve Švýcarsku provozuje databázi obsahující informace o sportovcích (ADAMS), která je spravována z Kanady ve spolupráci s vnitrostátními antidopingovými organizacemi po celém světě. Na rozdělení odpovědností a přidělení správy poukázala pracovní skupina zřízená podle článku 29 jako na záležitosti vyvolávající zvláštní problémy⁹.

To znamená, že hlavní záležitosti, jimiž se zabývá toto stanovisko, jsou v praxi velmi důležité a mohou mít značné důsledky.

⁸ „Cloud computing“ je druh výpočtu, kdy jsou přizpůsobitelné a pružné kapacity v oblasti IT poskytovány jako služba více zákazníkům prostřednictvím internetových technologií. Typické služby „cloud computing“ poskytují běžné internetové podnikové aplikace, které jsou dostupné z internetového prohlížeče, zatímco programové vybavení a údaje jsou uloženy na serverech. V tomto smyslu oblakem není ostrov, nýbrž globální článek spojující informace z celého světa a uživatele. Co se týká „sítě“, viz příklad č. 19.

⁹ Stanovisko č. 3/2008 ze dne 1. srpna 2008 k návrhu Mezinárodního standardu pro ochranu soukromí v rámci Světového antidopingového kodexu, WP156.

II.3. Některé hlavní problémy

Z hlediska cílů směrnice je nejdůležitější zajistit, aby byla odpovědnost za zpracování údajů jednoznačně vymezena a mohla být účinně uplatňována.

Není-li dostatečně jasné, co se požaduje od koho (například odpovědný není nikdo nebo existuje velký počet možných správců), existuje zjevné riziko, že se stane pouze velmi málo (pokud vůbec) a že právní předpisy nebudou účinné. Je rovněž možné, že nejednoznačnosti ve výkladu povedou k protikladným požadavkům a jiným sporným otázkám, přičemž v tomto případě budou kladné účinky nižší oproti očekáváním nebo by je mohly snížit či převážit nepředvídané negativní důsledky.

Ve všech těchto případech je tudíž zásadním problémem zaručit dostatečnou jasnost s cílem umožnit a zajistit účinné uplatňování a dodržování v praxi. V případě pochybností může být upřednostňovanou možností řešení, které s největší pravděpodobností podpoří tyto účinky.

Stejná kritéria, která zajišťují dostatečnou jasnost, však mohou vést rovněž k dodatečné složitosti a nežádoucím důsledkům. Například diferenciací kontroly v souladu s organizační realitou mohou vést ke složitosti z hlediska použitelného vnitrostátního práva, jsou-li zahrnuty různé jurisdikce.

Analýza by se proto měla zaměřit na rozdíl mezi přijatelnými důsledky na základě stávajících pravidel a možnou potřebou úpravy stávajících pravidel s cílem zajistit nadále účinnost a zamezit nepatřičným důsledkům za měnících se okolností.

To znamená, že tato analýza má velký strategický význam a měla by se používat obezřetně a s plným vědomím možného vzájemného vztahu mezi jednotlivými záležitostmi.

III. Analýza definic

III.1. Definice správce

Definice správce ve směrnici obsahuje tři hlavní stavební kameny, které budou pro účely tohoto stanoviska analyzovány zvlášť. Jedná se o tyto prvky:

- „fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jakýkoli jiný subjekt“,
- „který sám nebo společně s jinými“
- „určuje účel a prostředky zpracování osobních údajů“.

První stavební kámen souvisí s osobním aspektem definice. Třetí stavební kámen obsahuje základní prvky za účelem odlišení správce od ostatních účastníků, zatímco druhý stavební kámen se zabývá možností „mnohostranné kontroly“. Tyto stavební kameny jsou vzájemně úzce propojeny. Kvůli metodice použité v tomto stanovisku však bude každý z těchto prvků projednán zvlášť.

Z praktických důvodů je užitečné začít *prvním prvkem* třetího stavebního kamene – tj. významem slova „určuje“ – a pokračovat zbytkem třetího stavebního kamene a teprve poté se zabývat prvním a druhým stavebním kamenem.

III.1.a) Úvodní prvek: „určuje“

Jak již bylo zmíněno výše, pojem správce hrál v úmluvě č. 108 menší úlohu. Podle článku 2 úmluvy byl „správce souboru údajů“ vymezen jako instituce, „jež je ... příslušná rozhodnout“. Úmluva zdůrazňuje potřebu pravomoci, která je určena „podle vnitrostátního právního řádu“. Úmluva proto odkazovala zpět na vnitrostátní právní předpisy o ochraně údajů, které by podle důvodové zprávy měly obsahovat „přesná kritéria pro určení, kdo je příslušnou osobou“.

Ačkoliv první návrh Komise zohledňuje toto ustanovení, pozměněný návrh Komise odkazuje namísto toho na subjekt, „který rozhoduje“, vylučuje tudíž nutnost, aby pravomoc rozhodnout byla stanovena právem: stanovení právem je možné, nikoli však nezbytné. To je poté potvrzeno společným postojem Rady a přijatým textem, kdy oba dokumenty odkazují na subjekt, „který určuje“.

V tomto kontextu historický vývoj vyzdvihuje dva důležité prvky: za prvé, že je možné být správcem bez ohledu na zvláštní příslušnost nebo pravomoc ke správě údajů svěřenou právem; za druhé, že se v procesu přijímání směrnice 95/46 určení správce stalo pojmem Společenství, pojmem, který má v právu Společenství vlastní nezávislý význam, jenž se neliší z důvodu (případně odlišných) ustanovení vnitrostátního práva. Tento posledně uvedený prvek je zásadní v zájmu zajištění účinného uplatňování směrnice a vysoké úrovně ochrany v členských státech, která vyžaduje jednotný, a proto nezávislý výklad takového klíčového pojmu jako „správce“, který ve směrnici nabývá významu, jenž v úmluvě č. 108 neměl.

Z tohoto hlediska směrnice dokončuje tento vývoj tím, že stanoví, že i když schopnost „určit“ může vyplývat ze zvláštního přidělení právem, obvykle vyplývá z analýzy skutkových prvků nebo okolností daného případu: je nutno podívat se na konkrétní zpracování a pochopit, kdo je určuje, a to v první fázi zodpovězením těchto otázek: „Proč se uskutečňuje toto zpracování? Kdo je inicioval?“

Být správcem je v první řadě důsledkem skutkové okolnosti, že se subjekt rozhodl zpracovat osobní údaje pro vlastní účely. Pouze formální kritérium by ve skutečnosti nepostačovalo přinejmenším ze dvou důvodů: v některých případech by chybělo oficiální určení správce – stanovené například právem, ve smlouvě nebo oznámení orgánu pro ochranu údajů; v jiných případech se může stát, že by oficiální určení neodráželo realitu, a to oficiálním svěřením úlohy správce subjektu, který ve skutečnosti není schopen „určit“.

Význam skutečného vlivu je prokázán rovněž v případě SWIFT¹⁰, kdy se společnost SWIFT oficiálně považovala za zpracovatele údajů, avšak fakticky jednala – přinejmenším do jisté míry – jako správce údajů. V tomto případě bylo objasněno, že ačkoliv určení strany jako správce nebo zpracovatele ve smlouvě může poskytnout příslušné informace týkající se právního postavení této strany, takovéto smluvní určení

¹⁰ Tento případ se týká převodu bankovních údajů shromážděných společnostmi SWIFT za účelem provádění finančních transakcí jménem bank a finančních institucí na orgány USA v zájmu boje proti financování terorismu.

není nicméně rozhodující při určování jejího skutečného postavení, jež musí být založeno na konkrétních okolnostech.

Tento věcný přístup podporuje rovněž úvaha, že směrnice stanoví, že správcem je subjekt, který „určuje“, namísto „podle zákona určuje“ účel a prostředky. Účinná identifikace správy je rozhodující, i když určení se jeví jako neoprávněné nebo zpracování údajů je prováděno protiprávně. Není důležité, zda bylo rozhodnutí o zpracování údajů „zákonné“ v tom smyslu, že subjekt, který přijal toto rozhodnutí, tak mohl z právního hlediska učinit, nebo že správce byl oficiálně určen v souladu se zvláštním postupem. Otázka zákonnosti zpracování osobních údajů však bude důležitá v různých fázích a bude posouzena na základě ostatních článků (zejména článků 6 až 8) směrnice. Jinými slovy, je důležité zajistit, aby i v těch případech, kdy jsou údaje zpracovávány neoprávněně, bylo možno snadno zjistit správce a považovat jej za odpovědného za zpracování.

Poslední charakteristikou pojmu správce je jeho nezávislost v tom smyslu, že ačkoliv vnější právní zdroje mohou pomoci určit, kdo je správcem, je nutno toto vykládat především podle práva v oblasti ochrany údajů¹¹. Pojem správce by neměl být dotčen jinými – někdy kolidujícími nebo překrývajícími se – pojmy v ostatních oblastech práva, jako je autor nebo držitel práv k duševnímu vlastnictví. Být držitelem práv k duševnímu vlastnictví nevylučuje možnost být rovněž „správcem“, a tudíž podléhat povinnostem vyplývajícím z práva v oblasti ochrany údajů.

Potřeba typologie

Pojem správce je praktickým pojmem, který má přidělit odpovědnosti tam, kde existuje skutečný vliv, tudíž spíše na základě skutkové než formální analýzy. Určení kontroly může proto někdy vyžadovat podrobné a zdlouhavé šetření. Potřeba zajistit účinnost však vyžaduje, aby byl přijat pragmatický přístup s cílem zajistit předvídatelnost, pokud jde o kontrolu. Z tohoto hlediska jsou zapotřebí pravidla podle oka a praktické předpoklady za účelem usměrnění a zjednodušení uplatňování práva v oblasti ochrany údajů.

To vyžaduje výklad směrnice, který zajišťuje, že ve většině situací lze snadno a jednoznačně identifikovat „určující subjekt“ odkazem na – právní a/nebo skutkové – okolnosti, z nichž lze obvykle odvodit skutečný vliv, pokud ostatní prvky nenaznačují opak.

Tyto okolnosti lze analyzovat a ohodnotit podle těchto tří kategorií situací, které umožňují systematický přístup k těmto záležitostem:

1) Kontrola vyplývající z výslovné právní pravomoci. To je mimo jiné případ uvedený v druhé části definice, tj. když správce nebo zvláštní kritéria jeho určení jsou stanovena právem jednotlivých států nebo Společenství. Výslovné určení správce právem není časté a obvykle nepředstavuje velké problémy. V některých zemích vnitrostátní právní předpisy stanoví, že orgány veřejné moci jsou odpovědné za zpracovávání osobních údajů v rámci jejich úkolů.

¹¹ Viz níže vzájemný vztah s pojmy existujícími v ostatních oblastech práva (například pojem držitel práv k duševnímu vlastnictví nebo vědeckého výzkumu nebo odpovědnost podle občanského práva).

Častější je však případ, kdy právo namísto přímého určení správce nebo stanovení kritérií pro jeho určení vymezí úkol nebo ukládá někomu povinnost shromažďovat a zpracovávat určité údaje. Tak tomu je například v případě subjektu, který je pověřen určitými veřejnými úkoly (např. sociální zabezpečení), jež nelze vykonávat bez shromažďování alespoň některých osobních údajů, a vede rejstřík za účelem plnění těchto úkolů. V tomto případě z práva vyplývá, kdo je správce. Obecněji, právo může uložit veřejným nebo soukromým subjektům povinnost, aby uchovávaly nebo poskytovaly určité údaje. Tyto subjekty se pak obvykle považují za správce u jakéhokoli zpracování osobních údajů v tomto kontextu.

2) Kontrola vyplývající z implicitní pravomoci. Tak tomu je v případě, kdy schopnost určovat není výslovně stanovena právem, ani není přímým důsledkem explicitních právních předpisů, nýbrž vyplývá z obecných právních předpisů nebo ze zavedené právní praxe týkající se jednotlivých oblastí (občanské právo, obchodní právo, pracovní právo atd.). V tomto případě pomohou určit správce stávající tradiční úlohy, které obvykle znamenají určitou odpovědnost: například zaměstnavatel ve vztahu k údajům o zaměstnancích, vydavatel ve vztahu k údajům o předplatitelích, sdružení ve vztahu k údajům o členech nebo přispěvatelích.

Ve všech těchto případech lze schopnost určit činnosti spojené se zpracováním považovat za přirozeně spojenou s funkcí (soukromé) organizace, což znamená odpovědnosti rovněž z hlediska ochrany údajů. Z právního hlediska to bude platit bez ohledu na to, zda je schopnost určit svěřena zmíněným právníkům osobám, bude vykonávána příslušnými orgány jednajícími jejich jménem nebo fyzickou osobou, která má podobnou úlohu (viz níže k prvnímu prvku v písm. c)). Totéž však platí v případě veřejného orgánu s určitými správními úkoly v zemi, v níž právo výslovně nestanoví jeho odpovědnost za ochranu údajů.

Příklad č. 1: Telekomunikační operátoři

Zajímavý příklad právních pokynů pro soukromý sektor se vztahuje k úloze telekomunikačních operátorů. 47. bod odůvodnění směrnice 95/46/ES objasňuje, že „pokud je zpráva obsahující osobní údaje předávána prostřednictvím telekomunikací nebo elektronickou poštou, jejichž jediným účelem je přenos zpráv tohoto typu, bude za správce ve vztahu k údajům obsaženým ve zprávě obvykle považována spíše osoba, která zprávu podává, nežli osoba, která nabízí službu pro její přenos; (...) nicméně osoby, které nabízejí tyto služby, jsou obvykle považovány za správce ve vztahu ke zpracování doplňujících osobních údajů nezbytných pro fungování služby“. Poskytovatel telekomunikačních služeb by se proto měl v zásadě považovat za správce pouze u přenosu a účtování údajů, a nikoli u přenášených údajů¹². Tento právní pokyn ze strany zákonodárce Společenství je zcela v souladu s praktickým přístupem používaným v tomto stanovisku.

¹² Orgán pro ochranu údajů se zabýval kontrolou v případě předloženém subjektem údajů, který si stěžoval na nevyžádanou e-mailovou reklamu. V této stížnosti subjekt údajů požadoval, aby provozovatel komunikační sítě potvrdil nebo popřel, že byl odesílatelem reklamního e-mailu. Orgán pro ochranu údajů uvedl, že společnost, která pouze poskytuje zákazníkovi přístup ke komunikační síti, tj. společnost, která neinicuje předání údajů ani nevybírá adresáty nebo nemění údaje obsažené v předávané zprávě, nelze považovat za správce údajů.

3) *Kontrola vyplývající ze skutečného vlivu.* Tak tomu je v případě, kdy odpovědnost jakožto správce je přidělena na základě posouzení skutkových okolností. V mnoha případech toto bude zahrnovat posouzení smluvních vztahů mezi jednotlivými zúčastněnými stranami. Toto posouzení bere v úvahu vyvození externích závěrů, přidělení úlohy a odpovědností správce jedné či více stranám. To může být obzvláště užitečné ve složitém prostředí, často využívajícím nové informační technologie, kde mají příslušní účastníci často sklon považovat se za „usnadňovatele“, a nikoli za odpovědné správce.

Může se stát, že smlouva nehovoří nic o tom, kdo je správcem, obsahuje však dostatečné prvky pro přidělení odpovědnosti správce straně, která v tomto ohledu zjevně hraje dominantní úlohu. Může se taktéž stát, že smlouva je konkrétnější, co se týká správce. Není-li důvod pochybovat, že to přesně odráží realitu, neexistuje žádná námitka proti použití podmínek smlouvy. Podmínky smlouvy však nejsou rozhodující ve všech případech, jelikož to by stranám jednoduše umožnilo rozdělit si odpovědnost tak, jak to považují za vhodné.

Samotná skutečnost, že někdo určuje, jak jsou zpracovávány osobní údaje, může znamenat určení coby správce údajů, ačkoliv toto určení vzniká mimo oblast smluvního vztahu nebo je smlouvou výslovně vyloučeno. Jednoznačným příkladem tohoto byl případ společnosti SWIFT, kdy tato společnost vydala rozhodnutí o zpřístupnění určitých osobních údajů, jež byly původně zpracovávány k obchodním účelům pro finanční instituce, rovněž za účelem boje proti financování terorismu, jak požadovaly příkazy vydané ministerstvem financí USA.

V případě pochybností mohou být k zjištění správce užitečné jiné prvky než smluvní podmínky, například stupeň skutečné kontroly vykonávané některou ze stran, obraz poskytovaný subjektům údajů a přiměřená očekávání subjektů údajů na základě tohoto zviditelnění (viz rovněž třetí prvek v písmenu b)). Tato kategorie je obzvláště důležitá, jelikož umožňuje řešit a rozdělit odpovědnosti rovněž v případech protiprávního jednání, kdy skutečné činnosti spojené se zpracováním mohou být prováděny v rozporu se zájmem a vůlí některé ze stran.

Předběžný závěr

Z těchto kategorií umožňují první dvě v zásadě bezpečnější označení určujícího subjektu a mohou pokrývat více než 80 % příslušných situací v praxi. Oficiální určení právem by však mělo být v souladu s pravidly pro ochranu údajů, a to zajištěním, aby určený subjekt měl skutečnou kontrolu nad zpracováním nebo (jinými slovy) aby určení právem odráželo pravý stav věcí.

Třetí kategorie vyžaduje složitější analýzu a s větší pravděpodobností povede k odlišným výkladům. Při objasnění této záležitosti mohou často pomoci smluvní podmínky, nejsou však rozhodující ve všech případech. Existuje rostoucí počet účastníků, kteří nemají za to, že určují činnosti spojené se zpracováním, a nepovažují se tudíž za odpovědné za tyto činnosti. Jedinou přijatelnou možností je v těchto případech závěr na základě skutečného vlivu. Otázka zákonnosti tohoto zpracování však musí být posouzena podle ostatních článků (6–8).

Není-li použitelná žádná z výše uvedených kategorií, určení správce je nutno považovat za „neplatné od samého počátku“. Subjekt, který nemá právní ani skutečný vliv na určování způsobu zpracování osobních údajů, nelze považovat za správce.

Z formálního hlediska je aspektem, který potvrzuje tento přístup, to, že definici správce údajů je nutno považovat za závazné právní ustanovení, od něhož se strany nemohou jednoduše odchýlit nebo odklonit. Ze strategického hlediska by takovéto určení bylo v rozporu s účinným uplatňováním práva v oblasti ochrany údajů a zrušilo by odpovědnost, kterou zpracování údajů znamená.

III.1.b) Třetí prvek: „účel a prostředky zpracování“

Třetí prvek představuje hmotněprávní část kritéria: co by strana měla určit, aby byla považována za správce.

Historie tohoto ustanovení ukazuje mnoho vývojových trendů. Úmluva č. 108 odkazovala na účel automatizovaných souborů údajů, druhy osobních údajů a postupy, jakými budou zpracovány. Komise převzala tyto podstatné prvky s menšími jazykovými úpravami a přidala pravomoc rozhodnout, které třetí osoby mohou mít přístup k údajům. Pozměněný návrh Komise postoupil o krok kupředu a přesunul „účel souboru údajů“ na „účel a cíl zpracování“, znamenal tudíž přechod ze statické definice spojené se souborem údajů k dynamické definici související s činností spojenou se zpracováním. Pozměněný návrh nadále odkazoval na čtyři prvky (účel/cíl, osobní údaje, úkony a třetí strany, které mají přístup k údajům), jež byly sníženy na dva („účel a prostředky“) teprve ve společném postoji Rady.

Ve slovnících je „účel“ vymezen jako „předjímaný výsledek, který je zamýšlen nebo kterým se řídí plánované činnosti“, a „prostředky“ jako „způsob, jak docílit určitého výsledku nebo dosáhnout určitého účelu“.

Směrnice na druhou stranu stanoví, že údaje musí být shromažďovány pro stanovené účely, výslovně vyjádřené a legitimní, a nesmějí být dále zpracovávány způsobem neslučitelným s těmito účely. Určení „účelu“ zpracování a „prostředků“ k jeho dosažení je proto obzvláště důležité.

Lze rovněž uvést, že určení účelu a prostředků se rovná určení „proč“ a „jak“ s ohledem na určité činnosti spojené se zpracováním. Z tohoto hlediska a s přihlédnutím ke skutečnosti, že oba prvky spolu souvisí, je nutno poskytnout vodítko, pokud jde o to, jaká úroveň vlivu na „proč“ a „jak“ může znamenat, že daný subjekt je považován za správce.

Pokud jde o posouzení určení účelu a prostředků za účelem přisouzení úlohy správce údajů, zásadní otázkou je, na jaké úrovni podrobnosti by někdo měl určit účel a prostředky, aby byl považován za správce. A v souvislosti s tím, jaký manévrovací prostor směrnice poskytuje zpracovateli údajů. Tyto definice jsou obzvláště důležité, když se na zpracování osobních údajů podílejí různí účastníci a je nezbytné určit, kdo z nich je správcem údajů (sám nebo společně s jinými) a kdo má být namísto toho považován za zpracovatele údajů (pokud vůbec zpracovatelé existují).

Důraz, jenž se klade na účel nebo prostředky, se může lišit v závislosti na konkrétním kontextu, v němž se zpracování uskutečňuje.

Je zapotřebí pragmatický přístup, který klade větší důraz na rozhodovací pravomoc při určování účelu a volnost jednání při vydávání rozhodnutí. V těchto případech je otázkou, proč se uskutečňuje zpracování a jaká je úloha možných vzájemně spojených účastníků, například společností poskytujících externí služby: zpracovala by externí společnost údaje, pokud by to nepožadoval správce, a za jakých podmínek? Zpracovatel může působit podle obecných pokynů poskytnutých především ohledně účelu a nezabývajících se podrobně prostředky.

Příklad č. 2: Marketing prostřednictvím pošty

Společnost ABC uzavře smlouvy s různými organizacemi za účelem provádění marketingových kampaní prostřednictvím pošty a vedení mzdového účetnictví. Vydá jasné pokyny (jaké marketingové materiály mají být rozeslány a komu a komu má být zaplacen, jaké částky, do kdy atd.). Ačkoliv organizace mají určitou rozhodovací pravomoc (včetně toho, jaké programové vybavení bude používáno), jejich úkoly jsou naprosto jasné a úzce vymezené, a ačkoliv poštovní centrum může vydávat doporučení (např. doporučení nezasílat poštovní zásilky v srpnu), jsou jednoznačně povinny jednat podle pokynů společnosti ABC. Mimoto pouze jeden subjekt, společnost ABC, je oprávněn používat údaje, které jsou zpracovávány, všechny ostatní subjekty musí spoléhat na právní základ společnosti ABC, pokud je zpochybněna jejich právní způsobilost zpracovávat údaje. V daném případě je zřejmé, že společnost ABC je správcem údajů a každou z jednotlivých organizací lze považovat za zpracovatele údajů, co se týká konkrétního zpracování údajů prováděného pro tuto společnost.

Pokud jde o určení prostředků, výraz „prostředky“ zjevně zahrnuje velmi odlišné druhy prvků, což dokládá rovněž historie této definice. V původním návrhu by úloha správce vyplývala z určení čtyř prvků (účel/cíl, osobní údaje, úkony a třetí strany, které mají přístup k údajům). Konečnou formulaci ustanovení odkazující pouze na „účel a prostředky“ nelze vykládat jako verzi, která je v rozporu se starší verzí, jelikož nelze pochybovat o skutečnosti, že správce musí například určit, které údaje budou zpracovány pro plánovaný účel (účely). Konečnou definici je proto nutno chápat spíše pouze jako zkrácenou verzi zahrnující nicméně smysl starší verze. Jinými slovy, „prostředky“ neodkazují pouze na technické způsoby zpracování osobních údajů, nýbrž rovněž na to, „jak“ se bude zpracování provádět, což zahrnuje otázky jako „jaké údaje mají být zpracovány“, „které třetí strany mají přístup k těmto údajům“, „kdy budou údaje vymazány“ atd.

Určení „prostředků“ proto zahrnuje jak technické a organizační otázky, pokud rozhodnutí může být přeneseno na zpracovatele (např. „které technické nebo programové vybavení se použije?“), tak i základní prvky, které jsou tradičně a přirozeně vyhrazeny k určení správci, například „jaké údaje jsou zpracovávány?“, „jak dlouho budou zpracovávány?“, „kdo k nim má přístup?“ atd.

V této souvislosti platí, že zatímco určování účelu zpracování v každém případě vede k označení coby správce, určení prostředků znamená kontrolu pouze v případě, týká-li se určení základních prvků prostředků.

Z tohoto hlediska je možné, aby technické a organizační prostředky určil výhradně zpracovatel údajů.

V těchto případech (pokud existuje náležité vymezení účelu, avšak málo pokynů či žádné pokyny k technickým a organizačním prostředkům) by prostředky měly představovat přiměřený způsob dosažení účelu (účelů) a správce údajů by měl být plně informován o použitých prostředcích. Má-li dodavatel vliv na účel a provádí-li zpracování (rovněž) pro vlastní prospěch, například využitím obdržených osobních údajů za účelem vytvoření služeb s přidanou hodnotou, je to správce (nebo případně společný správce) pro jinou činnost spojenou se zpracováním, a proto se na něj vztahují veškeré povinnosti stanovené v použitelném právu v oblasti ochrany údajů.

Příklad č. 3: Společnost uvedená jako zpracovatel údajů, která však jedná jako správce

Společnost MarketinZ poskytuje různým společnostem služby v oblasti propagační reklamy a přímého marketingu. Společnost GoodProductZ uzavře se společností MarketinZ smlouvu, podle níž posledně uvedená společnost zajišťuje obchodní reklamu pro zákazníky společnosti GoodProductZ a je označena za zpracovatele údajů. Společnost MarketinZ se však rozhodne využít databázi zákazníků společnosti GoodProductsZ rovněž pro účely propagace výrobků ostatních zákazníků. Toto rozhodnutí o připojení dalšího účelu k účelu, pro nějž byly osobní údaje předány, mění společnost MarketinZ na správce údajů pro toto zpracování. Otázka zákonnosti tohoto zpracování však bude posouzena podle ostatních článků (6–8).

V některých právních systémech jsou obzvláště důležitá přijatá rozhodnutí o bezpečnostních opatřeních, jelikož bezpečnostní opatření jsou výslovně považována za základní charakteristiku, která má být stanovena správcem. To vyvolává otázku, která rozhodnutí o bezpečnosti mohou znamenat hodnocení jakožto správce v případě společnosti, které bylo zpracování zadáno externě.

Předběžný závěr

Určení „účelu“ zpracování je vyhrazeno „správci“. Ten, kdo přijímá toto rozhodnutí, je proto (*fakticky*) správce. Určení „prostředků“ zpracování může správce přenést na jiné subjekty, co se týká technických nebo organizačních otázek. Podstatné otázky, které jsou zásadní pro podstatu zákonnosti, jsou vyhrazeny správci. Osoba nebo subjekt, který rozhoduje například o tom, jak dlouho budou údaje uchovávány nebo kdo bude mít přístup ke zpracovaným údajům, jedná jako „správce“, co se týká této části použití údajů, musí proto dostát veškerým povinnostem správce.

III.1.c) První prvek: „fyzická osoba, právnická osoba nebo jakýkoli jiný subjekt“

První prvek definice odkazuje na osobní stránku: kdo může být správcem, a tudíž koho lze považovat za odpovědného za povinnosti plynoucí ze směrnice. Definice odráží přesně formulaci článku 2 úmluvy č. 108 a v rámci rozhodovacího procesu směrnice nebyla předmětem zvláštní diskuse. Vztahuje se na velkou řadu subjektů, které mohou hrát úlohu správce, počínaje u fyzických osob po právnické osoby a včetně „jakéhokoli jiného subjektu“.

Je důležité, aby výklad tohoto prvku zajistil účinné uplatňování směrnice, a to upřednostněním pokud možno jasného a jednoznačného určení správce ve všech případech bez ohledu na to, zda bylo učiněno a zveřejněno oficiální určení.

Především je důležité zůstat co nejbližší praxi zavedené jak ve veřejném, tak i soukromém sektoru ostatními oblastmi práva, jako je občanské právo, správní a trestní právo. Ve většině případů tato ustanovení určí, kterým osobám nebo subjektům by měly být přiděleny odpovědnosti, a v zásadě pomůže určit, kdo je správcem údajů.

Ze strategického hlediska rozdělení odpovědností je nutno s cílem poskytnout subjektům údajů stálejší a spolehlivější referenční subjekt pro výkon jejich práv podle směrnice upřednostnit to, aby se za správce považovaly společnost nebo orgán jako takové namísto konkrétní osoby v rámci společnosti nebo orgánu. Je to společnost nebo orgán, které se považují za odpovědné za zpracování údajů a povinnosti vyplývající z právních předpisů v oblasti ochrany údajů, ledaže existují jednoznačné prvky, které naznačují, že odpovědná je fyzická osoba. Obecně je nutno předpokládat, že společnost nebo orgán veřejné moci jsou jako takové odpovědné za činnosti spojené se zpracováním, jež se uskutečňují v rámci jejich oblasti činností a rizik.

Někdy společnosti a orgány veřejné moci určí konkrétní osobu odpovědnou za provedení zpracování. Avšak rovněž v tomto případě, kdy je určena konkrétní fyzická osoba, aby zajistila dodržování zásad v oblasti ochrany údajů nebo zpracovávala osobní údaje, nebude tato osoba správcem, nýbrž bude jednat pro právnickou osobu (společnost nebo orgán veřejné moci), která bude jakožto správce odpovědná v případě porušení zásad¹³.

Zejména v případě velkých a složitých struktur je zásadní otázkou „správy ochrany údajů“ zajištění jednoznačné odpovědnosti fyzické osoby zastupující společnost a konkrétních praktických odpovědností v rámci struktury, například pověřením jiných osob, aby jednaly jako zástupci nebo kontaktní místa pro subjekty údajů.

Zvláštní analýza je zapotřebí v případech, kdy fyzická osoba jednající v rámci právnické osoby použije údaje pro vlastní účely mimo oblast působnosti a možnou kontrolu činností právnické osoby. V tomto případě by dotyčná fyzická osoba byla správcem v případě zpracování, o němž rozhodla, a nesla by odpovědnost za toto použití osobních údajů. Původní správce by však mohl mít určitou odpovědnost v případě nového zpracování, k němuž došlo kvůli neexistenci odpovídajících bezpečnostních opatření.

Jak již bylo uvedeno výše, úloha správce je zásadní a obzvláště důležitá, pokud jde o určení odpovědnosti a uložení sankcí. Ačkoliv se odpovědnost a sankce budou lišit podle jednotlivých členských států, jelikož jsou ukládány podle vnitrostátních právních předpisů, nutnost jednoznačně určit fyzickou nebo právnickou osobu odpovědnou za porušení práva v oblasti ochrany údajů je bezesporu základním předpokladem účinného uplatňování směrnice.

Určení „správce“ z hlediska ochrany údajů je v praxi spojeno s pravidly občanského, správního nebo trestního práva, které stanoví rozdělení odpovědností nebo uložení sankcí, jimž může podléhat právnická nebo fyzická osoba¹⁴.

¹³ Obdobné odůvodnění je použito s ohledem na nařízení (ES) č. 45/2001, jehož čl. 2 písm. d) odkazuje na „orgán nebo instituci Společenství, generální ředitelství, jednotku či jakýkoli jiný organizační celek“. V rámci praxe v oblasti dozoru bylo objasněno, že úředníci orgánů a institucí EU, kteří byli určeni jako „správci“, jednají jménem instituce, pro niž pracují.

¹⁴ Viz „srovnávací studie Komise o situaci v 27 členských státech, co se týká práva použitelného na mimosmluvní závazkové vztahy, které vznikají z narušení soukromí a osobnostních práv“ (Comparative Study on the Situation in the 27 Member States as regards the Law Applicable to Non-contractual Obligations Arising out of Violations of Privacy and Rights relating to Personality), únor 2009, k dispozici na adrese

Občanskoprávní odpovědnost by neměla v tomto ohledu vyvolávat zvláštní problémy, jelikož se v zásadě vztahuje na právnické i fyzické osoby. Trestní a/nebo správní odpovědnost se však podle vnitrostátního práva může někdy vztahovat pouze na fyzické osoby. Pokud podle příslušného vnitrostátního práva existují trestní nebo správní sankce za porušení ochrany údajů, toto právo obvykle rovněž rozhoduje o tom, kdo je odpovědný: není-li uznána trestní nebo správní odpovědnost právnických osob, může být tato odpovědnost převzata vedoucími pracovníky právnických osob podle zvláštních pravidel vnitrostátního práva¹⁵.

Evropské právo obsahuje užitečné příklady kritérií, která přisuzují trestní odpovědnost¹⁶, zejména v případě, dojde-li k spáchání přestupku ve prospěch právnické osoby. Odpovědnost lze v takovémto případě přisoudit jakékoli osobě, „jež v právnické osobě působí ve vedoucím postavení, jednající samostatně nebo jako člen orgánu této právnické osoby na základě:

- a) oprávnění zastupovat tuto právnickou osobu;
- b) pravomoci činit rozhodnutí jménem této právnické osoby;
- c) pravomoci vykonávat kontrolu v rámci této právnické osoby.“

Předběžný závěr

Po shrnutí výše uvedených úvah lze vyvodit závěr, že subjektem, který se považuje za odpovědného za porušení ochrany údajů, je vždy správce, tj. právnická osoba (společnost nebo orgán veřejné moci) nebo fyzická osoba oficiálně určená podle kritérií stanovených ve směrnici. Pokud fyzická osoba pracující ve společnosti nebo orgánu veřejné moci použije údaje pro vlastní účely mimo činnost společnosti, považuje se tato osoba fakticky za správce a bude jako taková odpovědná.

Příklad č. 4: Tajné sledování zaměstnanců

Člen představenstva společnosti rozhodne o tajném sledování zaměstnanců společnosti, ačkoliv toto rozhodnutí není představenstvem oficiálně schváleno. Společnost je nutno považovat za správce a tato společnost čelí možným žalobám a odpovědnosti, co se týká zaměstnanců, jejichž osobní údaje byly zneužity.

Odpovědnost společnosti je zapříčiněna zejména skutečností, že jako správce je povinna zajistit dodržování pravidel týkajících se bezpečnosti a důvěrné povahy. Zneužití vedoucím pracovníkem společnosti nebo zaměstnancem lze považovat za výsledek nepřiměřených bezpečnostních opatření. To platí bez ohledu na skutečnost, zda lze v pozdější fázi považovat rovněž člena představenstva nebo jiné fyzické osoby ve společnosti za odpovědné z hlediska občanského práva (také vůči společnosti), jakož i z hlediska trestního práva. Tak tomu může být například v případě, kdy člen představenstva použil shromážděné údaje k získání osobních výhod od zaměstnanců: je nutno jej považovat za „správce“ a za odpovědného za toto konkrétní použití údajů.

http://ec.europa.eu/justice_home/doc_centre/civil/studies/doc/study_privacy_en.pdf

¹⁵ To nevylučuje, aby vnitrostátní právní předpisy stanovily trestní nebo správní odpovědnost nejen v případě správce, nýbrž rovněž jakékoli osoby, která poruší právo v oblasti ochrany údajů.

¹⁶ Viz například směrnice 2008/99/ES ze dne 19. listopadu 2008 o trestněprávní ochraně životního prostředí, rámcové rozhodnutí Rady ze dne 13. června 2002 o boji proti terorismu. Právní nástroje jsou založeny na článku 29, čl. 31 písm. e) a čl. 34 odst. 2 písm. b) Smlouvy o EU, nebo odpovídají právním základům nástrojů použitých v rámci prvního pilíře, jak vyplývá z judikatury ESD ve věcech C-176/03, Komise v. Rada, Sb. rozh. 2005, s. I-7879 a C-440/05, Komise v. Rada, Sb. rozh. 2007, s. I-9097. Viz rovněž sdělení KOM (2005) 583 v konečném znění).

III.1.d) Druhý prvek: „sám nebo společně s jinými“

Tento odstavec vycházející z předchozí analýzy obvyklých charakteristik správce se bude zabývat těmi případy, kdy při zpracování osobních údajů vzájemně jedná více účastníků. Skutečně se zvyšuje počet případů, v nichž různí účastníci jednají jako správci, a definice stanovená ve směrnici se tímto zabývá.

Možnost, aby správce působil „sám nebo společně s jinými“, nebyla v úmluvě č. 108 zmíněna a byla zavedena až Evropským parlamentem před přijetím směrnice. Ve stanovisku Komise k pozměňovacímu návrhu EP Komise odkazuje na možnost, aby „v případě jednoho zpracování mohla řada stran společně určit účel a prostředky zpracování, jež má být provedeno“, a proto v takovém případě „je nutno každého ze společných správců považovat za omezeného povinnostmi uloženými ve směrnici, co se týká ochrany fyzických osob, jejichž údaje jsou zpracovávány“.

Stanovisko Komise neodráží zcela složitosti ve stávající realitě zpracování údajů, jelikož se zaměřuje pouze na případ, kdy všichni správci ve stejné míře určují a jsou stejnou měrou odpovědní za jedno zpracování. Realita však ukazuje, že se jedná pouze o jeden z různých druhů „mnohostranné kontroly“, který může existovat. Z tohoto hlediska je nutno „společně“ vykládat ve smyslu „spolu s“ nebo „nikoli sám“ v různých formách a kombinacích.

Především je nutno uvést, že pravděpodobnost více účastníků podílejících se na zpracování osobních údajů je přirozeně spojena s více druhy činností, které mohou podle směrnice představovat „zpracování“, jež je konečným předmětem „společné kontroly“. Definice zpracování uvedená v čl. 2 písm. b) směrnice nevylučuje možnost, aby se na jednotlivých úkonech nebo souborech úkonů s osobními údaji podíleli různí účastníci. Tyto úkony se mohou uskutečňovat současně nebo v různých fázích.

V takovémto složitém prostředí je ještě důležitější jednoznačné přidělení úloh a odpovědností s cílem zajistit, aby složitost společné kontroly nevedla k nepraktickému rozdělení odpovědností, jež může bránit účinnosti práva v oblasti ochrany údajů. Kvůli mnoha možným ujednáním není bohužel možné vypracovat vyčerpávající „uzavřený“ seznam nebo kategorizaci jednotlivých druhů „společné kontroly“. Je však užitečné poskytnout rovněž v tomto kontextu vodítko jak prostřednictvím některých kategorií a příkladů společné kontroly, tak i pomocí určitých skutkových prvků, z nichž lze odvodit nebo předpokládat společnou kontrolu.

Posouzení společné kontroly by mělo obecně odrážet posouzení „jediné“ kontroly uvedené v bodě III.1.a až c. Stejně tak je nutno rovněž při posuzování společné kontroly zaujmout věcný a praktický přístup, jak byl uveden výše, zaměřující se na to, zda jsou účely a prostředky určeny více než jednou stranou.

Příklad č. 5: Instalace kamer pro videodohled

Vlastník budovy uzavře s bezpečnostní společností smlouvu, podle níž tato společnost nainstaluje pro správce v různých částech budovy kamery. Účel videodohledu a způsob, jakým jsou shromažďovány a uchovávány snímky, je určen výhradně vlastníkem budovy, kterého je proto nutno považovat za jediného správce pro toto zpracování.

V tomto kontextu mohou být při posuzování společné kontroly užitečná rovněž smluvní ujednání, je však vždy nutno ověřit je na základě skutkových okolností vztahu mezi stranami.

Příklad č. 6: Lovci mozků

Společnost Headhunterz Ltd pomáhá společnosti Enterprize Inc při náboru nových zaměstnanců. Ve smlouvě je jednoznačně uvedeno, že „společnost Headhunterz Ltd jedná jménem společnosti Enterprize a při zpracování osobních údajů vystupuje jako zpracovatel údajů. Společnost Enterprize je jediným správcem údajů“. Společnost Headhunterz Ltd však má nejednoznačné postavení: na straně jedné hraje úlohu správce vůči uchazečům o zaměstnání, na straně druhé se předpokládá, že je zpracovatelem, který jedná pro správce, například společnost Enterprize Inc a jiné společnosti, které jejím prostřednictvím hledají zaměstnance. Společnost Headhunterz se svou proslulou službou s přidanou hodnotou „global matchz“ hledá vhodné uchazeče z životopisů, jež obdrží přímo společnost Enterprize, i ze životopisů, které již má ve své rozsáhlé databázi. To zajišťuje, že společnost Headhunterz, která je podle smlouvy placena pouze za skutečně podepsané smlouvy, zlepšuje srovnávání mezi nabídkami pracovních míst a uchazeči o zaměstnání, zvyšuje tudíž své příjmy. Na základě výše uvedených prvků lze mít za to, že navzdory smluvnímu určení je společnost Headhunterz Ltd považována za správce, který společně se společností Enterprize Inc spravuje přinejmenším ty soubory úkonů, jež souvisí s náborem zaměstnanců pro společnost Enterprize.

Z tohoto hlediska společná kontrola vznikne v případě, kdy s ohledem na konkrétní zpracování různé strany určují účel nebo základní prvky prostředků, jež jsou typické pro správce (viz body III.1.a až c).

V rámci společné kontroly však může mít účast stran na společném určení různé formy a nemusí být rovnoměrně rozdělená. V případě většího počtu účastníků mohou mít tito velmi úzký vzájemný vztah (například sdílet veškeré účely a prostředky zpracování) nebo volnější vztah (například sdílet pouze účely nebo prostředky či jejich část). Je proto nutno uvážit širokou škálu typologií společné kontroly a posoudit jejich právní důsledky, což umožní určitou flexibilitu s cílem pokrýt rostoucí složitost stávající reality v oblasti zpracování údajů.

V tomto kontextu je nezbytné zabývat se různou mírou, v jaké může více stran vzájemně působit nebo být ve vzájemném vztahu při zpracovávání osobních údajů.

Za prvé, pouhá skutečnost, že při zpracovávání osobních údajů spolupracují různé subjekty, například v řetězci, neznamená, že jsou ve všech případech společnými správci, jelikož výměnu údajů mezi dvěma stranami bez sdílení účelu nebo prostředků ve společném souboru úkonů je nutno považovat pouze za předání údajů mezi dvěma samostatnými správci.

Příklad č. 7: Cestovní agentura (1)

Cestovní agentura zasílá osobní údaje svých zákazníků letecké společnosti a hotelovému řetězci za účelem rezervací v rámci souborných služeb pro cesty. Letecká společnost a hotel potvrdí dostupnost požadovaných sedadel a pokojů. Cestovní agentura vystaví pro své zákazníky cestovní doklady a poukázky. V tomto případě budou cestovní agentura, letecká společnost a hotel třemi různými správci údajů, z nichž každý podléhá povinnostem týkajícím se ochrany údajů, jež souvisí s jeho vlastním zpracováním osobních údajů.

Hodnocení se však může změnit, pokud se různí účastníci rozhodnou vytvořit společnou infrastrukturu pro své individuální účely. Pokud při vytváření této infrastruktury tyto účastníci určí základní prvky prostředků, které budou používány, považují se v každém případě za společné správce údajů, a to i tehdy, nesdílejí-li stejné účely.

Příklad č. 8: Cestovní agentura (2)

Cestovní agentura, hotelový řetězec a letecká společnost se rozhodnou vytvořit společnou internetovou platformu v zájmu zlepšení své spolupráce při správě rezervací. Dohodnou se na důležitých prvcích prostředků, jež budou používány, například jaké údaje budou uchovávány, jak budou rezervace přidělovány a potvrzovány a kdo může mít přístup k uchovávaným údajům. Mimoto se rozhodnou, že budou sdílet údaje svých zákazníků za účelem provádění integrovaných marketingových akcí.

V tomto případě budou cestovní agentura, letecká společnost a hotelový řetězec vykonávat společnou kontrolu nad způsobem zpracování osobních údajů svých příslušných zákazníků, budou proto společnými správci, co se týká zpracování souvisejících se společnou internetovou platformou pro rezervace. Každý z nich však bude mít nadále výhradní kontrolu s ohledem na ostatní činnosti spojené se zpracováním, například činnosti v souvislosti s řízením lidských zdrojů.

V některých případech zpracovávají různí účastníci stejné osobní údaje v řadě. V těchto případech je pravděpodobné, že na mikroúrovni se jednotlivá zpracování jeví jako nesouvislá, jelikož každé z nich může mít jiný účel. Je však nezbytné provést dvojí ověření, zda by na makroúrovni neměla být tato zpracování považována za „soubor zpracování“ sledujících společný účel nebo používajících společně stanovené prostředky.

Tuto myšlenku objasňují dva níže uvedené příklady uvádějící dva různé možné scénáře.

Příklad č. 9: Předání údajů zaměstnanců finančním úřadům

Společnost XYZ shromažďuje a zpracovává osobní údaje svých zaměstnanců za účelem správy mezd, služebních cest, zdravotního pojištění atd. Zákon však této společnosti ukládá rovněž povinnost zasílat veškeré údaje týkající se mezd finančním úřadům za účelem posílení daňové kontroly.

Ačkoliv společnost XYZ i finanční úřady zpracovávají stejné údaje o mzdách, neexistence společného účelu nebo prostředků s ohledem na toto zpracování údajů v tomto případě povede k tomu, že tyto dva subjekty budou považovány za dva samostatné správce údajů.

Příklad č. 10: Finanční transakce

Vezměme například banku, která využívá doručovatele finančních zpráv za účelem provádění svých finančních transakcí. Banka i doručovatel se dohodnou na prostředcích zpracování finančních údajů. Zpracování osobních údajů v souvislosti s finančními transakcemi provádí v první fázi finanční instituce a teprve posléze doručovatel finančních zpráv. I když na mikroúrovni každý z těchto subjektů sleduje svůj vlastní účel, na makroúrovni jsou různé fáze a účely a prostředky úzce spojené. V tomto případě lze banku a doručovatele zpráv považovat za společné správce.

Existují další případy, kdy různí dotčení účastníci společně určují (v určitých případech v různé míře) účel a/nebo prostředky zpracování.

Existují případy, kdy je každý správce odpovědný pouze za část zpracování, údaje jsou však seskupovány a zpracovány prostřednictvím platformy.

Příklad č. 11: Portály elektronické veřejné správy

Portály elektronické veřejné správy vystupují jako zprostředkovatelé mezi občany a jednotkami veřejné správy: portál předává žádosti občanů a uchovává dokumenty jednotky veřejné správy, dokud si je občan nevyžádá. Každá jednotka veřejné správy je i nadále správcem údajů zpracovávaných pro její účely. Za správce však lze považovat rovněž samotný portál. Portál ve skutečnosti zpracovává (tj. shromažďuje a předává příslušné jednotce) žádosti občanů a rovněž veřejné dokumenty (tj. uchovává je a řídí přístup k těmto dokumentům, například jejich stažení občany) pro další účely (usnadnění služeb elektronické veřejné správy), než pro něž byly údaje původně zpracovány jednotlivými jednotkami veřejné správy. Tito správci budou muset mimo jiné povinnosti zajistit, aby byl systém pro předávání osobních údajů od uživatele do systému veřejné správy bezpečný, jelikož na makroúrovni je toto předávání základní součástí souboru zpracování prováděných prostřednictvím portálu.

Další možnou strukturou je „přístup založený na původu“, který vzniká, pokud každý správce odpovídá za údaje, jež zavede do systému. Tak tomu je u některých databází zahrnujících celou EU, kdy je kontrola (a tudíž povinnost jednat na základě žádosti o přístup k údajům a o jejich opravu) přidělena na základě původu osobních údajů v jednotlivých členských státech.

Další zajímavý scénář poskytují internetové sociální sítě.

Příklad č. 12: Sociální síť

Poskytovatelé služeb sociálních sítí zajišťují internetové komunikační platformy, které jednotlivcům umožňují zveřejňovat a vyměňovat si informace s ostatními uživateli. Tito poskytovatelé služeb jsou správci údajů, jelikož určují účel i prostředky zpracování těchto informací. Uživatelé těchto sítí, kteří zasílají rovněž osobní údaje třetích osob, se považují za správce, pokud se na jejich činnosti nevztahuje tzv. „výjimka pro domácí použití“¹⁷.

¹⁷ Další podrobnosti a příklad viz stanovisko pracovní skupiny zřízené podle článku 29 č. 5/2009 k internetovým sociálním sítím, přijaté dne 12. června 2009 (WP 163).

Po analýze případů, kdy různé subjekty určují společně pouze část účelů a prostředků, je velmi jasným a bezproblémovým případem případ, kdy více subjektů společně určuje a sdílí veškeré účely a prostředky činností spojených se zpracováním, což vede k plnohodnotné společné kontrole.

V posledně uvedeném případě lze snadno určit, kdo je příslušný a je schopen zajistit práva subjektů údajů, jakož i splnit ostatní povinnosti týkající se ochrany údajů. Avšak úkol určit, který správce je příslušný (a odpovědný) za která práva subjektů údajů a které povinnosti, je mnohem složitější v případě, kdy různí společní správci sdílejí účely a prostředky zpracování nesymetricky.

Nutnost objasnit rozdělení kontroly

Nejprve je třeba podotknout, že zejména v případech společné kontroly neschopnost přímo plnit veškeré povinnosti správce (zajištění informací, právo na přístup atd.) nevylučuje možnost být správcem. Může se stát, že v praxi mohou tyto povinnosti pro správce snadno plnit jiné strany, které jsou někdy blíže subjektu údajů. Správce je však každopádně odpovědný za své povinnosti a odpovídá za jakékoli jejich porušení.

Podle předchozího textu předloženého Komisí v průběhu přijímání směrnice by přístup k určitým osobním údajům znamenal existenci (společného) správce pro tyto údaje. Tato formulace však nebyla v konečném znění zachována a zkušenosti ukazují, že na straně jedné přístup k údajům neznamená kontrolu jako takovou, zatímco na straně druhé přístup k údajům není nezbytnou podmínkou pro to, aby byl určitý subjekt správcem. Ve složitých systémech s více účastníky, kteří mají přístup k osobním a ostatním údajům, mohou být práva subjektů údajů zajištěna na různých úrovních různými účastníky.

Právní důsledky souvisí rovněž s odpovědností správců, což vyvolává zejména otázku, zda „společná kontrola“ zavedená směrnicí znamená vždy společnou a nerozdílnou odpovědnost. Článek 26 o odpovědnosti používá jednotné číslo „správce“, což naznačuje kladnou odpověď. Jak však již bylo zmíněno, realita může představovat různé způsoby jednání „společně“, tj. „spolu s“. To může v určitých případech vést k společné a nerozdílné odpovědnosti, nemusí to však platit vždy: v mnoha případech mohou být různí správci odpovědní (a tudíž ručit) za zpracování osobních údajů v různých fázích a v různé míře.

Minimálním požadavkem by mělo být zajištění, aby i ve složitém prostředí zpracování údajů, kdy při zpracování osobních údajů hrají úlohu různí správci, bylo dodržování pravidel pro ochranu údajů a odpovědností za možné porušení těchto pravidel jednoznačně přiděleno s cílem zamezit tomu, aby byla snížena ochrana osobních údajů nebo aby vznikl „negativní kompetenční spor“ a mezery, kdy některé povinnosti nebo práva plynoucí ze směrnice nejsou zajištěny žádnou ze stran.

V těchto případech je více než kdy jindy důležité, aby bylo subjektům údajů poskytnuto jednoznačné informační oznámení, které objasňuje různé fáze a účastníky zpracování. Mimoto by mělo být objasněno, zda je každý správce příslušný pro dodržení všech práv subjektu údajů, nebo který správce je příslušný pro které právo.

Příklad č. 13: Banky a soubory informací o zákaznických neplněních závazky

Několik bank může vytvořit společný „soubor informací“ (pokud vnitrostátní právní předpisy povolují takovéto soubory), kdy každá z nich poskytuje informace (údaje), jež se týkají zákazníků neplnění své závazky, a všechny banky mají přístup k veškerým informacím. Některé právní předpisy stanoví, že veškeré žádosti subjektů údajů, například o přístup k údajům nebo o výmaz, je třeba podat pouze jednomu „vstupnímu místu“, poskytovateli. Poskytovatel odpovídá za nalezení správného správce a za zajištění toho, aby subjekt údajů obdržel náležitou odpověď. Totožnost poskytovatele je zveřejněna v rejstříku zpracování údajů. V jiných jurisdikcích mohou takovéto soubory informací spravovat jiné právnické osoby než správce, zatímco žádosti o přístup subjektu k údajům vyřizují zúčastněné banky, které jednají jako zprostředkovatelé.

Příklad č. 14: Reklama zaměřená na chování

Reklama zaměřená na chování používá informace shromážděné s ohledem na chování jednotlivce na internetu, například navštívené stránky nebo vyhledávání, za účelem výběru reklam, které se tomuto jednotlivci zobrazí. Vydavatelé, kteří na svých internetových stránkách velmi často pronajímají reklamní prostory, i provozovatelé reklamních sítí, kteří tyto prostory plní cílenou reklamou, mohou shromažďovat a vyměňovat si informace o uživatelích v závislosti na konkrétních smluvních ujednáních.

Z hlediska ochrany údajů se vydavatel považuje za nezávislého správce, pokud shromažďuje osobní údaje od uživatele (profil uživatele, IP adresa, umístění, jazyk operačního systému atd.) pro vlastní účely. Provozovatel reklamní sítě bude rovněž správcem, určuje-li účel (sledování uživatelů na internetových stránkách) nebo základní prostředky zpracování údajů. Podle podmínek spolupráce mezi vydavatelem a provozovatelem reklamní sítě, pokud například vydavatel umožní předání osobních údajů provozovateli reklamní sítě, včetně prostřednictvím přesměrování uživatele na internetové stránky provozovatele reklamní sítě, mohou být společnými správci souboru zpracování vedoucích k reklamě zaměřené na chování.

Ve všech případech (společní) správci zajistí, aby složitost a technické aspekty systému reklamy zaměřené na chování nebránily v nalezení vhodných způsobů plnění povinností správců a zajištění práv subjektů údajů. To zahrnuje zejména:

- *informování* uživatele o skutečnosti, že jeho údaje jsou zpřístupněny třetí osobě: to může účinněji provést vydavatel, který je hlavním účastníkem dialogu s uživatelem,
- a podmínky *přístupu* k osobním údajům: společnost provozující reklamní síť musí odpovídat na žádosti uživatelů ohledně způsobu provádění cílené reklamy podle údajů uživatelů a vyhovět žádostem o opravu a výmaz.

Vydavatelé a provozovatelé reklamních sítí mohou mimoto podléhat dalším povinnostem vyplývajícím z občanského práva nebo práva v oblasti ochrany spotřebitele, včetně práva občanskoprávních deliktů a nekalých obchodních praktik.

Předběžný závěr

Strany jednající společně mají určitou míru flexibility při rozdělování a přidělování povinností a odpovědností, pokud zajistí jejich plné dodržování. Pravidla týkající se výkonu společných odpovědností by měla být v zásadě stanovena správci. Rovněž v tomto případě je nutno vzít v úvahu skutkové okolnosti s cílem posoudit, zda ujednání odráží realitu zpracování údajů.

Z tohoto hlediska by posouzení společné kontroly mělo vzít v úvahu na straně jedné nutnost zajistit plné dodržování pravidel pro ochranu údajů a na straně druhé to, že větší počet správců může vést rovněž k nežádoucí složitosti a případné nedostatečné jasnosti, pokud jde o rozdělení odpovědností. To by představovalo riziko, že celé zpracování bude nezákonné kvůli nedostatečné transparentnosti a porušení zásady korektního zpracování.

Příklad č. 15: Platformy spravující zdravotní údaje

V určitém členském státě orgán veřejné moci zřídí národní kontaktní místo řídící výměnu údajů o pacientech mezi jednotlivými poskytovateli zdravotní péče. Větší počet správců – desítky tisíc – vede k tak nejasné situaci pro subjekty údajů (pacienty), že je ohrožena ochrana jejich práv. Subjektům údajů nebude jasné, na koho se mohou obrátit v případě stížností, dotazů a žádostí o informace, opravy nebo o přístup k osobním údajům. Orgán veřejné moci odpovídá za skutečnou podobu zpracování a způsob jeho použití. Tyto prvky vedou k závěru, že se orgán veřejné moci, který zřídí kontaktní místo, považuje za společného správce stejně jako kontaktní místo pro žádosti subjektů údajů.

V tomto kontextu lze tvrdit, že by se společná a nerozdílná odpovědnost všech dotčených stran měla považovat za způsob odstranění nejistoty, a proto by se měla předpokládat pouze v případě, že dotyčné strany nestanovily jiné, jasné a stejně účinné rozdělení povinností a odpovědností nebo toto rozdělení nevychází jednoznačně ze skutkových okolností.

III.2. Definice zpracovatele

Pojem zpracovatele nebyl v úmluvě č. 108 stanoven. Úloha zpracovatele byla poprvé uznána v prvním návrhu Komise, avšak bez zavedení tohoto pojmu, s cílem „*zamezit situacím, kdy zpracování třetí osobou pro správce souboru údajů vede k snížení úrovně ochrany poskytnuté subjektu údajů*“. Teprve v pozměněném návrhu Komise je na návrh Evropského parlamentu pojem zpracovatel výslovně a nezávisle vysvětlen, načež stávající formulaci získal ve společném postoji Rady.

Stejně jako u definice správce předpokládá definice zpracovatele širokou škálu účastníků, kteří mohou hrát úlohu zpracovatele („... fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jakýkoli jiný subjekt ...“).

Existence zpracovatele závisí na rozhodnutí přijatém správcem, který může rozhodnout, že údaje budou zpracovány v rámci jeho organizace, například zaměstnanci oprávněnými ke zpracování údajů přímo podléhajícími správci (viz naopak čl. 2 písm. f), nebo přenesou veškeré činnosti spojené se zpracováním či jejich část na externí organizaci, tj. jak uvádí důvodová zpráva pozměněného návrhu Komise, „samostatnou právnickou osobou jednající jeho jménem“.

Dvěma základními podmínkami pro určení jakožto zpracovatele je na straně jedné existence samostatné právnické osoby s ohledem na správce a na straně druhé zpracování osobních údajů pro správce. Tato činnost spojená se zpracováním může být omezená na konkrétní úkol či kontext nebo může být obecnější a širší.

Úloha zpracovatele nevyplývá z povahy subjektu zpracovávajícího údaje, nýbrž z jeho konkrétních činností v určitém kontextu. Jinými slovy, tentýž subjekt může jednat současně u určitého zpracování jako správce a u jiných zpracování jako zpracovatel a určení jakožto správce nebo zpracovatele je nutno posoudit s ohledem na konkrétní soubory údajů nebo úkonů.

Příklad č. 16: Internetoví poskytovatelé hostingových služeb

Internetový poskytovatel zajišťující hostingové služby je v zásadě zpracovatelem osobních údajů zveřejněných na internetu jeho zákazníky, kteří využívají tohoto internetového poskytovatele pro hostování a údržbu svých internetových stránek. Pokud však internetový poskytovatel dále zpracovává údaje obsažené na internetových stránkách pro vlastní účely, pak je pro toto konkrétní zpracování správcem údajů. Tato analýza se liší od internetového poskytovatele, který zajišťuje e-mailové služby nebo služby přístupu na internet (viz rovněž příklad č. 1: telekomunikační operátoři).

Nejdůležitějším prvkem je ustanovení, že zpracovatel jedná „...pro správce ...“. Jednat pro někoho znamená sloužit zájmům někoho jiného a připomíná právní pojem „pověření“. V případě práva v oblasti ochrany údajů je zpracovatel vyzván, aby splnil pokyny vydané správcem, přinejmenším s ohledem na účel zpracování a základní prvky prostředků.

Z tohoto hlediska je zákonnost činnosti zpracovatele v souvislosti se zpracováním údajů určena pověřením, které vydal správce. Zpracovatel, který překročí své pověření a získá příslušnou úlohu při určování účelu nebo základních prostředků zpracování, je (společným) správcem místo zpracovatelem. Otázka zákonnosti tohoto zpracování však bude posouzena na základě ostatních článků (6–8). Pověření však může znamenat určitou míru rozhodovací pravomoci, jak co nejlépe sloužit zájmům správce, která zpracovateli umožňuje vybrat nejvhodnější technické a organizační prostředky.

Příklad č. 17: Externí zadávání poštovních služeb

Soukromé subjekty poskytují poštovní služby pro (veřejné) agentury – např. rozesílání rodičovských a mateřských příspěvků prováděné pro Státní správu sociálního zabezpečení. V tomto případě orgán pro ochranu údajů uvedl, že by dotyčné soukromé subjekty měly být považovány za zpracovatele vzhledem k tomu, že jejich úkol, který je sice vykonáván s určitou mírou nezávislosti, je omezen pouze na část zpracování, která je nezbytná pro účely stanovené správcem údajů.

V zájmu zajištění, aby externí zadávání a pověření nevedlo k snížení standardu ochrany údajů, obsahuje směrnice dvě ustanovení, jež jsou výslovně určena zpracovateli a která stanoví velmi podrobně jeho povinnosti s ohledem na důvěrnou povahu a bezpečnost.

– Článek 16 stanoví, že samotný zpracovatel, jakož i jakákoli osoba, která jedná z pověření zpracovatele, jež má přístup k osobním údajům, je může zpracovávat pouze podle pokynů správce.

– Článek 17 s ohledem na bezpečnost zpracování stanoví nutnost smlouvy nebo závazného právního aktu, který upravuje vztahy mezi správcem údajů a zpracovatelem údajů. Tato smlouva musí být potvrzena písemně pro zachování důkazů a musí mít minimální obsah a stanovit zejména, že zpracovatel jedná pouze podle pokynů správce a přijme vhodná technická a organizační opatření na ochranu osobních údajů. Smlouva by měla obsahovat dostatečně podrobný popis pověření zpracovatele.

V tomto ohledu je nutno podotknout, že v mnoha případech vytváří poskytovatelé služeb, kteří se specializují na určité zpracování údajů (například výplatu mezd) standardní služby a smlouvy, jež mají být podepsány správcem údajů, takže fakticky stanoví určitý standardní způsob zpracování osobních údajů¹⁸. Avšak skutečnost, že smlouva a její podrobné obchodní podmínky jsou vyhotoveny poskytovatelem služeb místo správcem, není *sama o sobě* dostatečným základem pro vyvození závěru, že by se měl poskytovatel služeb považovat za správce, pokud správce svobodně přijal smluvní podmínky, převzal tudíž plnou odpovědnost za tyto podmínky.

Stejně tak by se nerovnováha s ohledem na smluvní sílu malého správce údajů vůči velkým poskytovatelům služeb neměla považovat za důvod, aby správce přijal ustanovení a podmínky smluv, jež nejsou v souladu s právem v oblasti ochrany údajů.

Příklad č. 18: E-mailové platformy

John Smith hledá e-mailovou platformu, kterou bude používat on a pět zaměstnanců jeho podniku. Zjistí, že vhodná uživatelsky přívětivá platforma (a rovněž jediná platforma, která je nabízena zdarma) uchovává osobní údaje příliš dlouhou dobu a předává je do třetích zemí bez přiměřených bezpečnostních opatření. Smluvní podmínky jsou mimoto „ber, nebo nech být“.

V tomto případě by se pan Smith měl buď poohlédnout po jiném poskytovateli, nebo v případě údajného nedodržení pravidel pro ochranu údajů nebo nedostupnosti jiných vhodných poskytovatelů na trhu postoupit záležitost příslušným orgánům, například orgánům pro ochranu údajů, orgánům pro ochranu spotřebitele a antimonopolním orgánům atd.

Skutečnost, že směrnice vyžaduje k zajištění bezpečnosti zpracování písemnou smlouvu, neznamená, že mezi správcem a zpracovatelem nemohou existovat vztahy bez předchozích smluv. Z tohoto hlediska není smlouva podstatná ani rozhodující, i když může pomoci lépe pochopit vztahy mezi stranami¹⁹. Proto rovněž v tomto případě se použije praktický přístup, který analyzuje skutkové prvky vztahů mezi jednotlivými subjekty a způsob určování účelu a prostředků zpracování. Pokud se zdá, že mezi správcem a zpracovatelem existuje vztah, jsou tyto strany podle právních předpisů povinny uzavřít smlouvu (viz článek 17 směrnice).

¹⁸ Vypracováním smluvních podmínek poskytovatelem služby není dotčena skutečnost, že základní aspekty zpracování, jak bylo popsáno v bodě III.1.b, jsou určeny správcem.

¹⁹ V některých případech však může existence písemné smlouvy představovat nezbytnou podmínku pro to, aby se daný subjekt v určitých situacích považoval automaticky za zpracovatele. Například ve Španělsku zpráva o telefonních centrech vymezuje jako zpracovatele všechna telefonní centra ve třetích zemích, pokud plní smlouvu. To platí i v případě, že smlouvu vypracoval zpracovatel a správce ji pouze „dodržuje“.

Větší počet zpracovatelů

V rostoucí míře dochází k tomu, že zpracování osobních údajů je správcem zadáváno externě několika zpracovatelům údajů. Tito zpracovatelé mohou mít přímý vztah se správcem údajů nebo být subdodavateli, na něž zpracovatelé přenesli část činností spojených se zpracováním, které jim byly svěřeny.

Tyto složité (víceúrovňové nebo roztržité) struktury zpracování osobních údajů se objevují častěji s novými technologiemi a některé vnitrostátní právní předpisy na ně výslovně odkazují. Směrnice nebrání tomu, aby z důvodu organizačních požadavků bylo za zpracovatele údajů nebo dílčí zpracovatele určeno několik subjektů, a to rozdělením příslušných úkolů. Všechny tyto subjekty však musí při provádění zpracování dodržovat pokyny vydané správcem údajů.

Příklad č. 19: Počítačové sítě

Velké výzkumné infrastruktury využívají stále více distribuovaná výpočetní zařízení, zejména sítě, s cílem využít výpočetní a úložnou kapacitu. Sítě jsou nainstalovány v různých výzkumných infrastrukturách zřízených v různých zemích. Evropská síť se může například skládat z vnitrostátních sítí, za něž zase odpovídá vnitrostátní orgán. Tato evropská síť však nemusí mít ústřední orgán, který odpovídá za její fungování. Výzkumní pracovníci, kteří využívají takovou síť, obvykle nemohou určit, kde jsou jejich údaje přesně zpracovávány, a tudíž kdo je odpovědným zpracovatelem údajů (případ je ještě složitější, jestliže se síťové infrastruktury nacházejí ve třetích zemích). Pokud by síťová infrastruktura použila údaje nedovoleným způsobem, lze tuto stranu považovat za správce údajů, nejedná-li pro výzkumné pracovníky.

Strategickou otázkou je, aby v případě většího počtu účastníků zapojených do procesu byly povinnosti a odpovědnosti plynoucí z právních předpisů o ochraně údajů jednoznačně rozděleny a nebyly rozptýleny v celém řetězci externího zadávání / subdodávek. Jinými slovy, je třeba vyhnout se řetězci (dílčích) zpracovatelů, který by snížil či dokonce znemožnil účinnou kontrolu a jednoznačnou odpovědnost za činnosti spojené se zpracováním, ledaže jsou jednoznačně stanoveny odpovědnosti jednotlivých stran v řetězci.

Z tohoto hlediska je stejně, jak je popsáno v bodě III.1.b (ačkoliv není nutné, aby správce stanovil a schválil veškeré podrobnosti prostředků použitých k dosažení předpokládaného účelu), nezbytné, aby byl přinejmenším informován o hlavních prvcích struktury zpracování (například dotčené subjekty, bezpečnostní opatření, záruky za zpracování v třetích zemích atd.), takže je nadále schopen kontrolovat údaje, které jsou pro něj zpracovávány.

Je třeba rovněž uvážit, že ačkoliv směrnice ukládá odpovědnost správci, nebrání vnitrostátním právním předpisům o ochraně údajů, aby se v určitých případech považoval za odpovědného i zpracovatel.

Při určování postavení různých zúčastněných subjektů mohou být užitečná některá kritéria:

- úroveň předchozích pokynů vydaných správcem údajů, která určuje manévrovací prostor, jenž je ponechán zpracovateli údajů;

- sledování poskytování služby ze strany správce údajů. Trvalý a důkladný dozor ze strany správce s cílem zajistit důsledné dodržování pokynů a smluvních podmínek zpracovatelem naznačuje, že správce nadále vykonává úplnou a výhradní kontrolu nad zpracováním;
- zviditelnění/obraz poskytnutý správcem subjektu údajů a očekávání subjektů údajů na základě tohoto zviditelnění.

Příklad č. 20: Telefonní centra

Správce údajů zadá externě některé ze svých úkonů telefonnímu centru a vydá telefonnímu centru pokyny, aby se při volání zákazníků správce údajů představovalo s použitím totožnosti správce údajů. V tomto případě vedou očekávání zákazníků a způsob, jakým se správce těmto zákazníkům představuje prostřednictvím externí společnosti, k závěru, že externí společnost jedná jako zpracovatel údajů pro (jménem) správce.

- Odborné znalosti stran: v určitých případech hrají tradiční úloha a odborné znalosti poskytovatele služby rozhodující roli, která může znamenat jako určení jakožto správce údajů.

Příklad č. 21: Advokáti

Advokát zastupuje svého klienta u soudu a v souvislosti s tímto úkolem zpracovává osobní údaje související s případem tohoto klienta. Právním důvodem pro využití potřebných informací je pověření klienta. Toto pověření se však nezaměřuje na zpracování údajů, nýbrž na zastupování u soudu, přičemž pro tuto činnost mají tato povolání tradičně vlastní právní základ. Příslušníci těchto povolání jsou proto při zpracovávání údajů v průběhu právního zastupování svých klientů považováni za nezávislé „správce“.

V jiném kontextu může být rozhodující rovněž podrobnější posouzení prostředků zavedených k dosažení účelu.

Příklad č. 22: Internetové stránky „Ztrát a nálezů“

Internetové stránky „Ztrát a nálezů“ byly představeny pouze jako zpracovatel, jelikož osoby, které vyvěšují oznámení o ztracených předmětech, určují obsah, a tudíž na mikroúrovni účel (např. nalezení ztracené brože, papouška atd.). Orgán pro ochranu údajů tento argument odmítl. Internetové stránky byly vytvořeny za účelem dosažení zisku z toho, že umožní vyvěsit oznámení o ztracených předmětech, a skutečnost, že neurčují, které konkrétní předměty byly vyvěšeny (na rozdíl od určení kategorií předmětů), nebyla zásadní, jelikož definice „správce údajů“ nezahrnuje výslovně určení obsahu. Internetové stránky určují podmínky vyvěšení atd. a odpovídají za vhodnost obsahu.

Ačkoliv může existovat tendence obecně označit externí zadávání jako úkol zpracovatele, současné situace a hodnocení jsou často mnohem složitější.

Příklad č. 23: Účetní

Hodnocení postavení účetních se může lišit v závislosti na kontextu. Pokud účetní poskytují služby široké veřejnosti a malým obchodníkům na základě velmi obecných pokynů („vypracovat přiznání k dani“), pak bude (stejně jako v případě právních zástupců jednajících v podobných situacích a z podobných důvodů) účetní správcem údajů. Je-li však účetní zaměstnán podnikem a podléhá podrobným pokynům vydaným podnikovým účetním, například provést podrobný audit, pak obvykle v případě, že se nejedná o řádného zaměstnance, bude zpracovatelem, a to z důvodu jasnosti pokynů a následného omezeného rozsahu rozhodovací pravomoci. Toto však podléhá jedné důležité námitce, a sice že v případě, pokud se účetní domnívá, že zjistil nesprávný postup, který je povinen oznámit, pak z důvodu profesních povinností, které se na něj vztahují, jedná nezávisle jako správce.

Někdy může složitost zpracování vést k většímu zaměření se na manévrovací prostor subjektů pověřených zpracováním osobních údajů, například v případě, že zpracování znamená zvláštní riziko narušení soukromí. Zavedení nových prostředků zpracování může vést k tomu, že se upřednostňuje hodnocení jakožto správce údajů namísto zpracovatele údajů. Tyto případy mohou mít rovněž za následek objasnění a určení správce výslovně stanovené právem.

Příklad č. 24: Zpracování údajů pro historické, vědecké a statistické účely

Vnitrostátní právo může v souvislosti se zpracováním osobních údajů pro historické, vědecké a statistické účely zavést pojem zprostředkovatelské organizace s cílem určit subjekt pověřený převedením nekódovaných údajů na kódované údaje, takže správce zpracování pro historické, vědecké a statistické účely není schopen zpětně identifikovat subjekty údajů.

Pokud několik správců původních zpracování předá údaje jedné či více třetím osobám k dalšímu zpracování pro historické, vědecké a statistické účely, údaje jsou nejprve zakódovány zprostředkovatelskou organizací. V tomto případě lze zprostředkovatelskou organizaci považovat za správce podle zvláštních vnitrostátních předpisů a na tuto organizaci se vztahují veškeré výsledné povinnosti (relevantnost údajů, informování subjektu údajů, oznámení atd.). To je odůvodněno skutečností, že jsou-li spojeny údaje pocházející z různých zdrojů, existuje zvláštní hrozba pro ochranu údajů, která odůvodňuje vlastní odpovědnost zprostředkovatelské organizace. Tato organizace proto není považována jednoduše za zpracovatele, nýbrž podle vnitrostátního práva se považuje plně za správce.

Stejně tak je důležitá nezávislá rozhodovací pravomoc ponechaná jednotlivým stranám podílejícím se na zpracování. Příklad klinických zkoušek léků ukazuje, že vztah mezi zadávajícími společnostmi a externími subjekty pověřenými provedením zkoušek závisí na rozhodovací pravomoci ponechané externím subjektům v souvislosti se zpracováním údajů. To znamená, že může existovat více než jeden správce, avšak rovněž více než jeden zpracovatel nebo osoba pověřená zpracováním.

Příklad č. 25: Klinické zkoušky léků

Farmaceutická společnost XYZ zadá určité zkoušky léků a po posouzení příslušné způsobilosti a zájmů vybere z uchazečů zkušební střediska; vypracuje protokol o zkoušce, vydá střediskům potřebné pokyny v souvislosti se zpracováním údajů a ověřuje dodržování protokolu a příslušných vnitřních postupů ze strany těchto středisek.

Ačkoliv zadavatel neshromažďuje přímo žádné údaje, získává údaje pacientů shromážděné zkušebními středisky a zpracovává tyto údaje různými způsoby (vyhodnocení informací obsažených v lékařské dokumentaci; obdržení údajů o nepříznivých reakcích; zadávání těchto údajů do příslušné databáze; provádění statistických analýz za účelem dosažení výsledků zkoušek). Zkušební středisko provádí zkoušku nezávisle, ačkoliv v souladu s pokyny zadavatele; poskytuje informační oznámení pacientům a získává jejich souhlas v souvislosti se zpracováním údajů, které se jich týkají; umožňuje spolupracovníkům zadavatele přístup k původní lékařské dokumentaci pacientů za účelem provádění monitorovacích činností a zajišťuje a odpovídá za uchovávání těchto dokumentů. Zdá se proto, že jednotlivým účastníkům jsou svěřeny konkrétní odpovědnosti.

V tomto případě provádějí zkušební střediska i zadavatelé důležitá určení s ohledem na způsob zpracování osobních údajů souvisejících s klinickými zkouškami. Lze je proto považovat za společné správce údajů. Vztah mezi zadavatelem a zkušebními středisky by bylo možno vykládat odlišně v případech, že zadavatel určuje účel a základní prvky prostředků a výzkumnému pracovníkovi je ponechán velmi malý manévrovací prostor.

III.3. Definice třetí osoby

Pojem „třetí osoba“ nebyl v úmluvě č. 108 stanoven, byl však zaveden pozměněným návrhem Komise v návaznosti na pozměňovací návrh předložený Evropským parlamentem. Podle důvodové zprávy byl pozměňovací návrh přepracován s cílem objasnit, že třetí osoby nezahrnují subjekt údajů, správce a osoby, které jsou oprávněny ke zpracování údajů, a to z přímého pověření správce nebo pro správce, stejně jako zpracovatele. To znamená, že *„osoby pracující pro jinou organizaci, i když ta patří do stejné skupiny nebo holdingu společností, budou obvykle třetími osobami“*, zatímco na druhou stranu *„pobočky banky spravující účty klientů z přímého pověření svého ústředí nebudou třetími osobami“*.

Směrnice používá pojem „třetí osoba“ způsobem, jenž se neliší od způsobu, jakým je tento pojem obvykle používán v občanském právu, kde je třetí osoba obvykle subjektem, jenž není součástí organizace nebo dohody. V souvislosti s ochranou údajů je nutno tento pojem vykládat jako pojem odkazující na jakýkoli subjekt, který při zpracování osobních údajů nemá zvláštní oprávnění nebo povolení, jež by vyplývaly například z jeho úlohy správce, zpracovatele nebo jejich zaměstnance.

Směrnice tento pojem používá v mnoha ustanoveních, obvykle za účelem stanovení zákazu, omezení nebo povinností v případech, kdy by osobní údaje mohly být zpracovány jinými osobami, u nichž se původně nepředpokládalo, že budou zpracovávat určité osobní údaje.

V této souvislosti lze vyvodit závěr, že třetí osoba, která obdrží osobní údaje, a to legálně nebo protiprávně, bude v zásadě novým správcem, jsou-li splněny ostatní podmínky pro hodnocení této strany jako správce a použití právních předpisů o ochraně údajů.

Příklad č. 26: Neoprávněný přístup ze strany zaměstnance

Zaměstnanec společnosti se při plnění svých úkolů doví o osobních údajích, k nimž nemá povolen přístup. V tomto případě je nutno tohoto zaměstnance považovat za „třetí osobu“ vůči jeho zaměstnavateli se všemi důsledky a závazky z toho plynoucími, pokud jde o zákonnost sdělení a zpracování údajů.

IV. Závěry

Pojem správce údajů a jeho vzájemný vztah s pojmem zpracovatel údajů hrají při uplatňování směrnice 95/46/ES zásadní úlohu, jelikož určují, kdo je odpovědný za dodržování pravidel pro ochranu údajů, jak mohou subjekty údajů vykonávat svá práva, jaké je použitelné vnitrostátní právo a jak účinně mohou působit orgány pro ochranu údajů.

Organizační diferenciaci ve veřejném a v soukromém sektoru, rozvoj IKT, jakož i globalizace zpracování údajů zvyšují složitost způsobu zpracovávání osobních údajů a vyžadují objasnění těchto pojmů v zájmu zajištění účinného uplatňování a dodržování v praxi.

Pojem správce je nezávislý v tom smyslu, že je nutno jej vykládat především podle právních předpisů Společenství v oblasti ochrany údajů, a praktický v tom smyslu, že má přidělit odpovědnosti podle skutečného vlivu, je tudíž založen spíše na skutkové analýze než na formální analýze.

Definice ve směrnici obsahuje tři hlavní stavební kameny: osobní aspekt (*„fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jakýkoli jiný subjekt“*); možnost mnohostranné kontroly (*„který sám nebo společně s jinými“*) a zásadní prvky k odlišení správce od ostatních účastníků (*„určuje účel a prostředky zpracování osobních údajů“*).

Analýza těchto stavebních kamenů vede k těmto hlavním výsledkům:

- Schopnost „určit účel a prostředky“ může vyplývat z různých právních a/nebo skutkových okolností: výslovná právní pravomoc, kdy právo určuje správce nebo svěřuje úkol či povinnost shromažďovat a zpracovávat určité údaje; běžné právní předpisy nebo existující tradiční úlohy, které obvykle znamenají určitou odpovědnost v rámci určitých organizací (například zaměstnavatel ve vztahu k údajům zaměstnanců); skutkové okolnosti a jiné prvky (např. smluvní vztahy, skutečná kontrola některé strany, zviditelnění vůči subjektům údajů atd.).

Není-li použitelná žádná z výše uvedených kategorií, určení správce je nutno považovat za „neplatné od samého počátku“. Subjekt, který nemá právní ani skutečný vliv na určování způsobu zpracování osobních údajů, nelze považovat za správce.

Určení „účelu“ zpracování znamená postavení (fakticky) správce. Určení „prostředků“ zpracování může být správcem přeneseno na jiný subjekt, co se týká

technických nebo organizačních záležitostí. O podstatných otázkách, které jsou zásadní pro zákonnost zpracování – například jaké údaje mají být zpracovávány, délka uchovávání, přístup atd. – musí rozhodnout správce.

- *Osobní* aspekt definice odkazuje na širokou škálu subjektů, které mohou hrát úlohu správce. Ze strategického hlediska rozdělení odpovědností je však nutno upřednostnit to, aby se za správce považovaly společnost nebo orgán jako takové namísto konkrétní osoby v rámci této společnosti nebo orgánu. Je to společnost nebo orgán, které se považují za odpovědné za zpracování údajů a povinnosti vyplývající z právních předpisů v oblasti ochrany údajů, ledaže existují jednoznačné prvky, které naznačují, že odpovědná je fyzická osoba, například pokud fyzická osoba pracující ve společnosti nebo orgánu veřejné moci použije údaje pro vlastní účely mimo rámec činností společnosti.
- Možnost *mnohostranné kontroly* pokrývá rostoucí počet situací, kdy jako správci jednají různé strany. Posouzení této společné kontroly by mělo odrážet posouzení „jediné“ kontroly, a to přijetím věcného a praktického přístupu a zaměřením se na otázku, zda jsou účel a základní prvky prostředků určeny více než jednou stranou.

Účast stran na určení účelu a prostředků zpracování v rámci společné kontroly může mít různé formy a nemusí být sdílena rovnou měrou. Toto stanovisko uvádí mnoho příkladů různých druhů a stupňů společné kontroly. Různé stupně kontroly mohou vést k různé míře povinností a odpovědnosti a ne ve všech případech lze předpokládat „společnou a nerozdílnou“ odpovědnost. Je možné, aby ve složitých systémech s více účastníky byl přístup k osobním údajům a výkon ostatních práv subjektů údajů zajištěn na různých úrovních různými účastníky.

Toto stanovisko analyzuje rovněž pojem zpracovatel, jehož existence závisí na rozhodnutí přijatém správcem, který může rozhodnout o zpracování údajů v rámci své organizace nebo o přenesení veškerých činností spojených se zpracováním či jejich části na externí organizaci. Dvěma základními podmínkami pro určení jakožto zpracovatele jsou na straně jedné to, že se jedná o samostatnou právnickou osobu s ohledem na správce, a na straně druhé je to zpracování osobních údajů pro správce. Tato činnost spojená se zpracováním může být omezená na konkrétní úkol nebo kontext nebo může být přizpůsobena určité míře rozhodovací pravomoci, pokud jde o to, jak sloužit zájmům správce, jež zpracovateli umožňuje zvolit nejvhodnější technické a organizační prostředky.

Úloha zpracovatele nevyplývá z povahy účastníka zpracovávajícího osobní údaje, nýbrž z konkrétních činností v určitém kontextu a s ohledem na určitý soubor údajů nebo úkonů. Při určování postavení různých zúčastněných subjektů mohou být užitečná některá kritéria: úroveň předchozích pokynů vydaných správcem údajů; sledování poskytování služby ze strany správce údajů; zviditelnění vůči subjektům údajů; odborné znalosti stran; nezávislá rozhodovací pravomoc ponechaná různým stranám.

Zbývající kategorie „třetí osoby“ je definována jako účastník, který při zpracování osobních údajů nemá žádné zvláštní oprávnění nebo povolení, jež by vyplývaly například z jeho úlohy správce, zpracovatele nebo jejich zaměstnance.

Pracovní skupina uznává potíže při používání definic obsažených ve směrnici ve složitém prostředí, v němž lze předpokládat mnoho scénářů zahrnujících správce a zpracovatele, samostatně nebo společně, s různou mírou nezávislosti a odpovědnosti.

Ve své analýze pracovní skupina zdůraznila nutnost rozdělit odpovědnost tak, aby bylo v praxi dostatečně zajištěno dodržování pravidel pro ochranu údajů. Nejistila však žádný důvod pro domněnku, že z tohoto hlediska již nebude stávající rozlišení mezi správci a zpracovateli relevantní a použitelné.

Pracovní skupina proto doufá, že vysvětlení obsažená v tomto stanovisku doložená konkrétními příklady převzatými z každodenních zkušeností orgánů pro ochranu údajů přispějí k účinným pokynům ke způsobu výkladu těchto hlavních definic směrnice.

V Bruselu dne 16. února 2010.

*Za pracovní skupinu
předseda
Jacob KOHNSTAMM*

Věstník Úřadu pro ochranu osobních údajů

Vydavatel: Úřad pro ochranu osobních údajů

Adresa redakce: Úřad pro ochranu osobních údajů, Pplk. Sochora 27, 170 00 Praha 7

Redakce: Miluše Nejedlá, tel.: 234 665 232, fax: 234 665 505

e-mail: posta@uoou.cz

internetová adresa: www.uoou.cz

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

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

ISSN 1213-3442