VĚSTNÍK
ÚŘADU PRO OCHRANU OSOBNÍCH ÚDAJŮ
2009

Částka 54 **10. prosince 2009** **Cena 80 Kč**

OBSAH

ÚVOD

Částka 54 Věstníku Úřadu pro ochranu osobních údajů publikuje přehled zrušených registrací za období od 16. 9. 2009 do 30. 11. 2009.

Rubrika Stanoviska Úřadu obsahuje dva materiály. Prvním je Stanovisko č. 5/2009 „Zveřejňování osobních údajů v médiích“. Aplikace zákona o ochraně osobních údajů v oblasti žurnalistiky je komplikovaná. Nicméně Úřad je toho názoru, že uplatnění principů ochrany osobních údajů je i v této oblasti zcela na místě, neboť významně doplňuje instituty občanského, mediálního i trestního práva. Cílem tohoto stanoviska je především nastínit postoje Úřadu k posuzované problematice, případně vyvolat diskusi o potřebě speciální právní úpravy ve smyslu čl. 9 Směrnice. Druhým materiálem je Stanovisko č. 6/2009 „Ochrana soukromí při zpracování osobních údajů“. Úřad se při své činnosti setkává se situacemi, kdy veřejnosti není zcela zřejmý vztah pojmů soukromí a ochrana osobních údajů, resp. jejich právní úprava a odlišnosti. Proto vydává toto stanovisko se záměrem přispět k odstranění této nejasnosti.

Rubrika Sdělení Úřadu přináší dokument Pracovní skupiny pro ochranu dat podle článku 29 Směrnice 95/46/ES (WP29), kterým je „Stanovisko č. 5/2009 k internetovým sociálním sítím“. Stanovisko se zaměřuje na to, jak může provozování internetových stránek sociálních sítí splňovat požadavky právních předpisů EU na ochranu údajů. Jeho cílem je především nabídnout poskytovatelům služeb sociálních sítí pokyny k opatřením, která je nutno zavést k zajištění souladu s právem EU. Stanovisko vyjadřuje velkou obavu pracovní skupiny podle článku 29 z šíření a využívání informací, které jsou dostupné na internetových stránkách sociálních sítí, pro jiné druhotné, nezamýšlené účely. Výraznou oblastí obav je také přístup k informacím o profilu. Pracovní skupina ve svém stanovisku dále zdůrazňuje, že zvláštní pozornost by měli poskytovatelé služeb sociálních sítí věnovat zpracování osobních údajů nezletilých osob. Úřad přetiskuje oficiální překlady právně nezávazných dokumentů WP29 v jejich původní podobě a nepřebírá odpovědnost za případné nepřesnosti překladů.

Částku uzavírá rubrika Materiály z Úředního věstníku Evropské unie, která obsahuje dokument „Stanovisko evropského inspektora ochrany údajů k návrhu směrnice Evropského parlamentu a Rady o jakostních a bezpečnostních normách pro lidské orgány určené k transplantaci“. Cílem dokumentu je vytvořit vysoké jakostní a bezpečnostní normy pro lidské orgány určené k transplantaci a zajistit tak vysokou úroveň ochrany lidského zdraví. Evropský inspektor ochrany údajů doporučuje, aby ve všech případech, kdy se provádějí opatření mající vliv na ochranu a bezpečnost údajů, byly konzultovány všechny příslušné zúčastněné strany včetně evropského inspektora ochrany údajů a pracovní skupiny podle článku 29 (WP29). Jedná se o překlad pořízený Evropskou komisí (přetisk v původní podobě).

Přehled zrušených registrací

Číslo registrace	Subjekt	Datum zrušení
00001188/051	UNILEVER ČR, SPOL. S R.O.	07.11.2009
00001471/025	MĚSTSKÁ ČÁST PRAHA 12	03.10.2009
00015834/001	ATLAS ADRIATIC S.R.O.	24.11.2009
00025217/001	CZECH COAL SERVICES A.S.	30.10.2009
00025217/002	CZECH COAL SERVICES A.S.	30.10.2009
00025217/003	CZECH COAL SERVICES A.S.	30.10.2009
00025217/004	CZECH COAL SERVICES A.S.	30.10.2009
00025217/005	CZECH COAL SERVICES A.S.	30.10.2009
00025217/006	CZECH COAL SERVICES A.S.	30.10.2009
00025217/007	CZECH COAL SERVICES A.S.	30.10.2009
00025217/008	CZECH COAL SERVICES A.S.	30.10.2009
00025217/009	CZECH COAL SERVICES A.S.	30.10.2009
00025217/010	CZECH COAL SERVICES A.S.	30.10.2009
00025217/011	CZECH COAL SERVICES A.S.	30.10.2009
00031056/001	ORGANON, S.R.O.	03.10.2009
00031056/002	ORGANON, S.R.O.	03.10.2009
00032144/005	MCDONALD´S ČR SPOL. S R.O.	10.11.2009
00033367/001	ING. LUDMILA HROCHOVÁ	06.11.2009
00033952/001	ZČP NET, S.R.O.	10.11.2009
00033952/002	ZČP NET, S.R.O.	10.11.2009
00033952/003	ZČP NET, S.R.O.	10.11.2009
00033952/004	ZČP NET, S.R.O.	10.11.2009
00033952/005	ZČP NET, S.R.O.	10.11.2009
00033953/001	STP NET, S.R.O.	10.11.2009
00033953/002	STP NET, S.R.O.	10.11.2009
00033953/003	STP NET, S.R.O.	10.11.2009
00033953/004	STP NET, S.R.O.	10.11.2009
00033953/005	STP NET, S.R.O.	10.11.2009
00034718/001	EISAI GMBH, ORGANIZAČNÍ SLOŽKA	28.10.2009

II. STANOVISKA ÚŘADU

Stanovisko č. 5/2009

listopad 2009

Zveřejňování osobních údajů v médiích

Úvod

Zveřejňování osobních údajů, tedy informací vztahujících se ke konkrétním fyzickým osobám ve smyslu § 4 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, v periodickém tisku, ale i v jiných médiích, je nepochybně jednou z problematických oblastí, kde se střetávají zcela odlišné zájmy a očekávání – na straně jedné oprávněný požadavek dotčených osob na ochranu soukromí a na straně druhé neméně důležitá svoboda šíření informací. Tento střet je přitom s nárůstem objemu informací šířených nejen klasickými periodiky, ale např. i na internetu, stále viditelnější a stále více se dotýká i jiných osob, než pouze mediálně známých celebrit či politiků.

Důkazem, že této skutečnosti je třeba čelit také na úrovni právních předpisů, jsou např. pravidla, která stanoví zákon č. 159/2006 Sb., o střetu zájmů, pro zveřejňování informací uchovávaných v registrech oznámení, nebo nedávná novela trestního řádu (zákon č. 52/2009 Sb.) posilující mj. ochranu svědků, poškozených a dalších osob zúčastněných v trestním řízení.

Také zákon o ochraně osobních údajů je především – dle § 1 – určen k ochraně jednotlivců před neoprávněnými zásahy do soukromí prostřednictvím zpracování osobních údajů. Úřad pro ochranu osobních údajů (dále jen „Úřad“) proto považuje za nezbytné vyjádřit se k problematice zveřejňování osobních údajů v médiích formou tohoto stanoviska.

Relevantní právní předpisy

Úvodem je třeba shrnout právní předpisy, ze kterých je při posuzování zpracování osobních údajů při činnosti médií nutno vycházet. Základy je nutno hledat jak v mezinárodních, tak i v českých ústavních normách, které jsou dále doplněny dílčími instituty soukromého i veřejného práva upravených v jednotlivých zákonech.

Mezinárodní dokumenty:

- Úmluva o ochraně lidských práv a základních svobod; dokument Rady Evropy podepsaný v roce 1950 v Římě (dále jen „Úmluva“)
  - čl. 8: právo na respektování soukromého a rodinného života,[1]
  - čl. 10: svoboda projevu, tj. právo přijímat a rozšiřovat informace;
- Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně jednotlivců v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen „Směrnice“)
  - čl. 9: povinnost členských států EU zavést pro zpracování osobních údajů pro účely žurnalistiky (tam, kde je to skutečně nezbytné pro vyvážení práva na soukromí a svobody projevu) odchylky a výjimky od obecné úpravy ochrany osobních údajů,
  - recitál č. 37: interpretační východisko pro požadavky Směrnice v oblasti žurnalistiky, tj. zdůvodnění odlišného přístupu při aplikaci pravidel pro ochranu osobních údajů v této oblasti.

České právní předpisy:

- Listina základních práv a svobod[2] (dále jen „Listina“)
  - čl. 10 odst. 3: právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním osobních údajů,
  - čl. 17: právo na svobodu projevu a právo na informace;
- zákon o ochraně osobních údajů;
- zákon č. 40/1964 Sb., občanský zákoník
  - § 11 až 16: ochrana osobnosti;
- zákony upravující činnost vydavatelů periodického tisku a provoz dalších médií.[3]

Z uvedeného výčtu lze dovodit, že jak nadnárodní normy, tak i české ústavní předpisy přiznávají stejnou váhu právu na informace, resp. svobodu projevu, i právu na ochranu osobnosti a soukromí, jejichž nedílnou složkou je právo na ochranu osobních údajů. Současně jsou těmito dokumenty stanoveny podmínky, kdy lze tato práva omezit – obecně řečeno je to možné pouze v zájmu ochrany důležitých zájmů demokratické společnosti (např. pořádku a bezpečnosti, předcházení zločinnosti, ochrany zdraví nebo významných hospodářských zájmů a ochrany práv a svobod jiných).

[1] Evropský soud pro lidská práva, který byl zmíněnou úmluvou zřízen, dovozuje z čl. 8 Úmluvy také právo na ochranu osobních údajů.

[2] Přesněji usnesení předsednictva České národní rady č. 2/1993 Sb., o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součásti ústavního pořádku České republiky.

[3] Např. zákon č. 46/2000 Sb., o právech a povinnostech při vydávání periodického tisku a o změně některých dalších zákonů (tiskový zákon), zákon č. 231/2001 Sb., o provozování rozhlasového a televizního vysílání a o změně dalších zákonů, nebo zákon č. 483/1991 Sb., o České televizi – tyto právní předpisy však zpracování osobních údajů v té či oné oblasti komplexně neupravují.

Dále lze konstatovat, že Směrnice uznává specifičnost žurnalistiky ve vztahu ke zpracování osobních údajů, avšak v žádném případě nepřipouští úplné vynětí této oblasti ze své působnosti, a tím tedy ani z národních právních předpisů upravujících ochranu osobních údajů. Důsledné vyvážení práva na šíření informací a práva na ochranu osobních údajů je dle Směrnice třeba řešit formou uzákonění nezbytných výjimek a omezení, jejichž konkrétní formu a hranice jejich limitů však ponechává na jednotlivých státech.

Východiska pro aplikaci zákona o ochraně osobních údajů

Praktická aplikace uvedených norem v České republice není snadná. Komplikace spočívají především v tom, že český zákonodárce nevyslyšel pokyn uvedený v citovaném čl. 9 a recitálu č. 37 Směrnice a zvláštní úpravu zpracování osobních údajů v rámci žurnalistiky, případně v médiích obecně, nepřijal.

Uvedené by mohlo vést k závěru, že zákon o ochraně osobních údajů se tedy v oblasti žurnalistiky uplatní jako v případě jakéhokoliv jiného zpracování osobních údajů, tedy že je nezbytné vyžadovat plnění (a sankcionovat neplnění) všech zde uvedených povinností. Avšak tento přístup naráží na principy výkladu ústavních norem definované Ústavním soudem, podle kterého nelze žádnému ze základních práv přiznat vyšší důležitost. Ústavní soud konkrétně judikoval, že základní právo podle čl. 17 Listiny je zásadně rovno základnímu právu upravenému v čl. 10 Listiny.[4] Dalším limitem pro aplikaci zákona o ochraně osobních údajů na novinářskou činnost jsou výše zmíněná ustanovení Směrnice, neboť dle Evropského soudního dvora je nutno vykládat národní zákony implementující komunitární normy tzv. eurokonformním způsobem (tedy v duchu a dle smyslu evropských právních předpisů).

Při posuzování zpracování osobních údajů v médiích se Úřad právě s ohledem na tyto autority ve své praxi vždy řídil názorem, že správný a opodstatněný je takový přístup k výkladu zákona o ochraně osobních údajů, který vyváženým způsobem odráží ústavní i evropské zásady. V oblasti žurnalistiky proto Úřad uplatňuje svěřené kompetence jen v krajních případech, které opodstatňují použití veřejnoprávních opatření (ve smyslu Ústavním soudem vyžadované zásady *ultima ratio* trestní represe[5]). Tento přístup Úřad dále opírá o již zmíněný fakt, že Směrnice dovoluje pro oblast žurnalistiky určité výjimky, nikoli však úplné vynětí z působnosti zákona o ochraně osobních údajů, a současně o postoj Ústavního soudu k otázce svobody projevu, dle kterého „právo na informace, jakož i právo tyto informace svobodně sdělovat, je jednoznačným spojením práva a současně povinnosti (či odpovědnosti) zejména tisku pravdivě, vyváženě a korektně informovat o otázkách důležitého veřejného zájmu“.[6]

Přístup Úřadu při posuzování zveřejnění osobních údajů v médiích

Pro aplikaci zákona o ochraně osobních údajů na oblast žurnalistiky je vhodné rozlišovat dvě situace, konkrétně přípravu reportáží nebo článků a jejich následné zveřejnění.

V případě první situace lze dospět k závěru, že činnost jednotlivých žurnalistů (fyzických osob) při shromažďování podkladů – včetně osobních údajů – za účelem přípravy článku či reportáže nebude ve smyslu čl. 9 Směrnice v rozporu se zákonem o ochraně osobních údajů. Tento přístup vychází z úvahy, že osobní údaje jsou v rámci této činnosti získávány a využívány v souladu s právem svobodně vyhledávat informace dle čl. 17 odst. 4 Listiny, přičemž v této fázi je riziko neoprávněného zásahu do soukromí dotčených osob (ve smyslu § 1 zákona o ochraně osobních údajů) minimální.

Pro uplatnění požadavků zákona o ochraně osobních údajů je zásadní situace, kdy dochází ke zveřejnění textu či reportáže, příp. jiné použití shromážděných údajů, neboť právě tímto okamžikem dochází k – mnohdy nevratnému – zásahu do soukromí a osobního života dotčených osob.

Pokud bylo ve fázi vyhledávání informací a přípravy materiálu možno konstatovat, že se jedná o činnost chráněnou čl. 17 odst. 4 Listiny, která nezasahuje významným způsobem do jiných základních práv, je tomu v situaci, kdy jsou osobní údaje již zveřejněny, zcela jinak. V tomto bodě již nepochybně dochází ke střetu dvou výše uvedených základních práv (práva na svobodu projevu a šíření informací a práva na ochranu soukromí), která mají stejnou váhu, a která je nutno šetřit v maximální míře (tj. zachovat co nejširší uplatnění obou práv) a je tedy i na místě uplatnit relevantní požadavky zákona o ochraně osobních údajů.

Odpovědnost za zpracování osobních údajů v publikovaných článcích či příspěvcích je tak primárně na vydavateli či provozovateli daného média, jehož prostřednictvím je šíření informací umožněno. V této souvislosti je nutno uvést, že z hlediska zákona o ochraně osobních údajů není podstatné, zda vydavatelem nebo provozovatelem je fyzická či právnická osoba, neboť uvedený zákon ukládá povinnosti správcům či zpracovatelům osobních údajů, kterými mohou být jak fyzické, tak i právnické osoby.

Dále je třeba vyřešit otázku, za jakých okolností je důvodné konstatovat, že publikováním určitých osobních údajů došlo k naplnění některé ze skutkových podstat správních deliktů či přestupků podle zákona o ochraně osobních údajů. Jako základní východisko pro tuto úvahu je opět nutno vzít smysl tohoto zákona, tedy zda v daném případě došlo k neoprávněnému zásahu do soukromí konkrétní

[4] Nález Ústavního soudu sp. zn. II. ÚS 357/96 a IV. ÚS 154/97.

[5] Nález Ústavního soudu sp. zn. I. ÚS 4/04.

[6] Usnesení Ústavního soudu sp. zn. II. ÚS 435/01.

osoby, anebo zda je na místě s ohledem na ochranu svobody projevu a roli médií ve společnosti[7] zásah jako neoprávněný nehodnotit. K zodpovězení této otázky lze dospět po posouzení okolností daného případu, kdy je třeba vyhodnotit zejména následující aspekty:

- Postavení osoby, které se zveřejněné údaje týkají. Je nepochybně nutno odlišovat informace týkající se soukromí např. politiků či tzv. celebrit od informací o „obyčejných" lidech[8] [viz § 5 odst. 2 písm. f) zákona o ochraně osobních údajů]. Přísněji je dále třeba přistupovat ke zveřejnění osobních údajů týkajících se dětí či mladistvých anebo osob, které se z jiného důvodu nejsou schopny bránit samy.
- Charakter publikovaných informací. Zákon o ochraně osobních údajů definuje v § 4 písm. b) citlivé údaje, jakožto subkategorii údajů osobních, jejichž zneužitím může dojít k citelnému zásahu do práv osob (jde např. o údaje o zdravotním stavu, etnickém původu, náboženském vyznání, sexuálním životě anebo údaje genetické), a kterým zákon poskytuje zvýšenou ochranu. Zveřejnění údajů spadajících do této kategorie je nutno posuzovat přísněji, a to i ve vztahu k tzv. celebritám. Opačná situace nastává v případě informací, k jejichž zveřejnění poskytla dotčená osoba souhlas, anebo které lze označit za oprávněně zveřejněné (tedy nikoli v rozporu s příslušnými zákony, které na danou oblast dopadají). Takové údaje je možné – při zachování práv subjektů údajů na ochranu soukromého života – dále volně využívat [viz návětí § 5 odst. 2 a § 5 odst. 2 písm. d) zákona o ochraně osobních údajů].
- Smysl a účel zveřejnění osobních údajů. Úřad je obecně toho názoru, že při aplikaci zákona o ochraně osobních údajů v oblasti žurnalistiky je na místě posoudit jako jedno z kritérií také to, zda má zveřejnění určitých informací sloužit čistě ke zvýšení „atraktivity" zprávy, nebo zda je zpracováním (zveřejněním) osobních údajů v daném případě skutečně sledován skutečný veřejný zájem. Veřejný zájem opodstatňující publikaci osobních údajů lze dle Úřadu spatřovat především tam, kde tyto údaje souvisejí s veřejnou činností dotčené osoby, případně mají svědčit o nezákonném nebo jinak nedovoleném či neetickém chování.

Uvedený výčet není samozřejmě vyčerpávající; Úřad posuzuje každý z případů individuálně, s ohledem na veškeré relevantní okolnosti (např. charakter média, tedy zda má zveřejnění údajů lokální či celostátní dopad, zda lze údaje i následně dohledat apod.).

Závěr

Aplikace zákona o ochraně osobních údajů v oblasti žurnalistiky je komplikovaná (tento zákon obsahuje mnoho ustanovení, např. § 11 nebo 16, která svobodu slova nijak neomezují, přesto jsou v této oblasti jen obtížně realizovatelná) a často na hranici kompetencí Úřadu, resp. působnosti zákona o ochraně osobních údajů. Nicméně Úřad je toho názoru, že uplatnění principů ochrany osobních údajů je i v této oblasti zcela na místě, neboť významně doplňuje instituty občanského, mediálního i trestního práva. S ohledem na výše popsaná východiska a důvody přistupuje Úřad k této problematice s maximální obezřetností a ve své praxi přihlíží ke všem relevantním aspektům práce žurnalistů i k funkci médií.

Není smyslem tohoto stanoviska detailně postihnout veškeré otázky, které se zpracováním (zejména zveřejňováním) osobních údajů v činnosti médií souvisejí. Každý z komunikačních prostředků má svá specifika, jejichž posouzení přesahuje možnosti tohoto textu. Navíc, jak bylo naznačeno již v úvodu, existují oblasti, které jsou upraveny zvláštními právními předpisy, a kde se zákon o ochraně osobních údajů uplatní pouze subsidiárně. Obdobně nelze bez dalšího výše uvedené názory vztáhnout na specifické informační kanály jako diskusní fóra, tematické weby či blogy.

Cílem tohoto stanoviska je především nastínit postoje Úřadu k posuzované problematice, případně vyvolat diskusi o potřebě speciální právní úpravy ve smyslu čl. 9 Směrnice.

Poznámka: Publikované stanovisko je také k dispozici na internetové adrese Úřadu www.uoou.cz v sekci Názory Úřadu/Stanoviska.

---

[7] K roli tzv. „hlídacího psa" společnosti viz usnesení Ústavního soudu sp. zn. II. ÚS 435/01, nález tohoto soudu sp. zn. I. ÚS 394/04 nebo také rozsudky Evropského soudu pro lidská práva ve věci Goodwin vs. Spojené království z roku 1996 a Bladet Tromsø a Stensaas vs. Norsko z roku 1999.

[8] Viz nálezy Ústavního soudu sp. zn. IV. ÚS 146/04, sp. zn. I. ÚS 453/03 a sp. zn. I. ÚS 367/03 nebo rozsudek Evropského soudu pro lidská práva ve věci Castells vs. Španělsko z roku 1992. Nicméně i informování o soukromém životě veřejně známých osob má své limity – viz rozsudek Evropského soudu pro lidská práva ve věci von Hannover vs. Německo z roku 2004.

Stanovisko č. 6/2009

listopad 2009

Ochrana soukromí při zpracování osobních údajů

Úvod

Úřad pro ochranu osobních údajů (dále jen „Úřad“) se při své činnosti setkává se situacemi, kdy veřejnosti není zcela zřejmý vztah pojmů soukromí a ochrana osobních údajů, resp. jejich právní úprava a odlišnosti. V některých případech jsou tyto pojmy používány, a to i při veřejné diskusi, jako synonyma nebo jiným způsobem, který plně neodpovídá platné legislativě. Úřad vydává toto stanovisko se záměrem přispět k odstranění této nejasnosti.

Pojem soukromí není v českém právu přímo definován. Soukromí můžeme stručně popsat jako osobní, intimní sféru člověka v jeho integritě, která zahrnuje všechny projevy osobnosti konkrétního a jedinečného lidského tvora. Pojem soukromí obsahuje rovněž hmotný i myšlenkový prostor jednotlivce, součástí soukromého života je i právo na vytváření a rozvíjení vztahů s dalšími lidskými bytostmi.

Relevantní právní úprava

Ochranu soukromí v českém právním řádu na prvním místě upravuje zákon č. 2/1993 Sb., usnesení předsednictva České národní rady ze dne 16. prosince 1992 o vyhlášení Listiny základních práv a svobod jako součásti ústavního pořádku České republiky, ve znění zákona č. 162/1998 Sb., kterým se mění Listina základních práv a svobod (dále jen „Listina základních práv a svobod“). Tento právní předpis ústavněprávního charakteru umisťuje právo na ochranu soukromí mezi základní lidská práva a svobody, když v čl. 10 odst. 2 uvádí, že každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.

Ochranu soukromí jako základního lidského práva upravují i významné mezinárodní dokumenty. Například Všeobecná deklarace lidských práv OSN v čl. 12 stanoví, že nikdo nesmí být vystaven svévolnému zasahování do soukromého života, do rodiny, domova nebo korespondence, ani útokům na svou čest a pověst. Každý má právo na zákonnou ochranu proti takovým zásahům nebo útokům. Obdobné ustanovení obsahuje i Úmluva o ochraně lidských práv a základních svobod Rady Evropy, která v čl. 8 odst. 1 říká, že každý má právo na respektování svého soukromého a rodinného života, obydlí a korespondence.

Z výše uvedené základní a obecné definice soukromí v kontextu s citovaným ustanovením Listiny základních práv a svobod vyplývá, že k zásahům do soukromí nezbytně dochází prakticky při každé interakci s dalšími lidmi, resp. jak při interakci přímé, tak v situaci, kdy někdo jiný disponuje a případně dále nakládá s informacemi o projevech naší osobnosti. Tyto zásahy však zásadně musejí být oprávněné, tedy legální, vycházející z práva. Jakýkoliv jiný stav je nežádoucí a protiprávní.

Ochranu před jednorázovými, resp. nesystematickými zásahy do soukromí jednotlivce upravuje především § 11 a násl. zákona č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů v rámci institutu ochrany osobnosti. Zde je rovněž obecně upraveno právo dotčené fyzické osoby domáhat se zadostiučinění, případně i finančního, za újmu, která jí byla neoprávněným zásahem do soukromí způsobena.

Pokud někdo s projevy osobní povahy či jinými informacemi týkajícími se určené nebo určitelné fyzické osoby systematicky provádí nějakou operaci nebo soustavu operací, potom již jde o zpracování osobních údajů a dostáváme se do režimu zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů. Tento zákon provádí další základní lidské právo stanovené v čl. 10 odst. 3 Listiny základních práv a svobod, tedy právo každého na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě, které je nedílnou součástí práva na ochranu soukromí.

Jak vyplývá ze samotné podstaty pojmu zpracování osobních údajů, k zásahům do soukromí při něm nutně a nezbytně dochází, neboť bez operace (ať už shromažďování, uchovávání, využívání atd.) prováděné s projevy osobní povahy identifikované nebo identifikovatelné osoby, dle dikce zákona o ochraně osobních údajů subjektu údajů, by ke zpracováním osobních údajů vůbec dojít nemohlo. Aby zpracování osobních údajů bylo legální a zásah do soukromí osoby oprávněný, je nutné při tomto zpracování dbát všech povinností stanovených zákonem o ochraně osobních údajů, případně zvláštními právními předpisy.

Zákon o ochraně osobních údajů pro správce údajů, tedy osobu, která stanoví účel a prostředky zpracování, provádí jej a také za něj zodpovídá, stanoví řadu povinností: např. povinnost stanovit účel a prostředky zpracování osobních údajů, povinnost zajištění právního titulu ke zpracování, povinnost zpracovávat pouze přesné osobní údaje v souladu se stanoveným účelem, důležité okolnosti směřující k ochraně zpracovávaných osobních údajů proti neoprávněnému či nahodilému přístupu, informační povinnost vůči subjektům údajů, registrační povinnost k Úřadu a další.

V kontextu tohoto stanoviska se zaměříme především na povinnost stanovenou v § 5 odst. 3 a v § 10 zákona o ochraně osobních údajů. Jedná se o povinnost správce, případně zpracovatele, při zpracování osobních údajů dbát na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů.

K zásahu do soukromí při zpracování osobních údajů nezbytně dochází. Tyto zásahy ovšem musejí být dle uvedených ustanovení zákona o ochraně osobních údajů oprávněné. Znamená to, že správce má mj. povinnost stanovit účel zpracování a prostředky, jimiž bude zpracování provádět. Za oprávněný zásah do soukromí lze považovat takové zpracování, které je prováděno způsobem a prostředky přiměřenými zvolenému legálnímu a legitimnímu, tedy právem připuštěnému, resp. nezakázanému, účelu zpracování. V opačném případě, byť by jinak zpracování odpovídalo všem požadavkům zákona, by šlo o zpracování nelegální, nezákonné a Úřad by mohl uplatnit své dozorové pravomoci. Nehodnotil by primárně účel zpracování samotný ani plnění ostatních povinností správce, ale zaměřil by se především na to, zda zvolený způsob zpracování osobních údajů je adekvátní a přiměřený stanovenému účelu a zda nadbytečně a tedy neoprávněně zasahuje, či nikoliv do soukromého života subjektů údajů.

Z praktického hlediska je účelné odlišit dvě kategorie správců – subjekty soukromého a subjekty veřejného práva.

Subjekty soukromoprávní si v zásadě účel i způsob zpracování osobních údajů stanoví samy, pokud nejde o zpracování, které jim ukládá zákon, a to v duchu ústavního pravidla, že každý může činit to, co není zakázáno. Po zvolení účelu zpracování osobních údajů si proto mohou vybrat prostředky a způsoby, jimiž bude zpracování probíhat. Ještě před zahájením samotného zpracování dat, ve fázi úvah o jeho potřebnosti a parametrech, musí správce uvážit, zda je určitý způsob zpracování adekvátní stanovenému účelu, a to s ohledem ke všem okolnostem zamýšleného zpracování, nebo zda by do soukromí zasáhl vzhledem k účelu nepřiměřeně. Pokud by tak neučinil a prováděl zpracování osobních údajů tak, že by nadbytečně zasahoval do soukromí subjektů údajů, mohl by Úřad uplatnit své dozorové kompetence. Po provedené kontrole v rámci uložených opatření k nápravě by mohl takovéto zpracování osobních údajů, byť by bylo jinak perfektní, i zcela zakázat.

Subjekt veřejného práva, pokud vystupuje v této roli, může zásadně činit jen to, co mu zákon umožňuje, a to pouze zákonem stanoveným způsobem. Pokud tedy správce, veřejnoprávní subjekt, provádí zpracování osobních údajů jediným způsobem, které mu právní řád umožňuje, pak jedná z principu vždy po právu a o nelegální, neoprávněný zásah do soukromí ve smyslu § 5 odst. 3, příp. § 10 zákona o ochraně osobních údajů se jednat nemůže. Rovněž v těch případech, kdy je právem stanovený způsob zpracování ne zcela adekvátní jeho účelu, musí dotyčný správce osobní údaje určeným způsobem zpracovávat. V těchto případech nezbývá Úřadu, který nedisponuje zákonodárnou iniciativou, než své připomínky k takto nevhodné právní úpravě uplatňovat jinak než uplatněním svých dozorových kompetencí.

Veřejnoprávní subjekt v postavení správce proto může způsob a prostředky zpracování osobních údajů ovlivnit, resp. je nucen posuzovat jejich dopad na soukromí, pouze v případech, kdy mu právní řád dává na výběr z více způsobů zpracování, jakými může stanoveného cíle dosáhnout. V tomto případě je i tento správce povinen posoudit konkrétní případ, účel zpracování osobních údajů a další okolnosti, které se zpracování dotýkají, a zvolit takový způsob zpracování osobních údajů, který do soukromí subjektů údajů zasáhne v menší míře. V tomto případě argumentace tím, že správce provádí zpracování jedním ze způsobů, který mu zákon umožňuje, neobstojí. Každý správce, tedy i subjekt veřejného práva, má povinnost se při zpracování osobních údajů řídit také právními předpisy upravujícími ochranu osobních údajů, tedy i zákonem o ochraně osobních údajů. A pokud má na výběr z více možností zpracování osobních údajů a zvolí ten invazivnější, soukromí dotčených osob méně respektující způsob, poruší výše uvedená ustanovení zákona o ochraně osobních údajů a ocitá se v kolizi s tímto právním předpisem (např. poměrně častý požadavek na identifikaci osoby pomocí „data narození nebo rodného čísla“, kdy správci musí bez dalšího stačit datum narození, protože se jedná o údaj, který nezahrnuje další informace a do soukromí dané osoby zasahuje méně). V tomto případě by možné opatření uložené k nápravě nemohlo zpracování, které je prováděno na základě zákona o zmocnění, zakázat, mohlo by však v konkrétním případě zakázat jeden z jeho více možných způsobů.

Závěr

Každé zpracování osobních údajů představuje zásah do soukromí jednotlivce. Aby tento zásah a celé zpracování bylo legální, je třeba, aby správce ve všech případech, kdy je to možné, posoudil případné způsoby zpracování a zvolil ten, který do soukromí subjektů údajů zasáhne v nejmenší míře. V opačném případě nebude zpracování v souladu se zákonem o ochraně osobních údajů a správce se vystavuje riziku kontroly a uplatnění opatření k nápravě ze strany Úřadu s tím, že toto opatření může v krajním případě představovat i zákaz celého prováděného zpracování osobních údajů.

Poznámka: Publikované stanovisko je také k dispozici na internetové adrese Úřadu www.uoou.cz v sekci Názory Úřadu/Stanoviska.

III. SDĚLENÍ ÚŘADU

PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29

01189/09/CS
WP 163

Stanovisko č. 5/2009 k internetovým sociálním sítím

Přijaté dne 12. června 2009

Tato pracovní skupina byla zřízena podle článku 29 směrnice 95/46/ES. Je nezávislým evropským poradním orgánem 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 Evropská komise, Generální ředitelství pro spravedlnost, svobodu a bezpečnost, ředitelství C (Občanská spravedlnost, práva a občanství), B-1049 Brusel, Belgie, kancelář č. LX-46 01/02.

Adresa internetových stránek: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

Obsah

Shrnutí

Toto stanovisko se zaměřuje na to, jak může provozování internetových stránek sociálních sítí splňovat požadavky právních předpisů EU na ochranu údajů. Jeho cílem je především poskytnout poskytovatelům služeb sociálních sítí pokyny k opatřením, která je nutno zavést k zajištění souladu s právem EU.

Ve stanovisku se uvádí, že poskytovatele služeb sociálních sítí a v mnoha případech poskytovatelé doplňkových aplikací jsou správci údajů s příslušnými odpovědnostmi vůči uživatelům služeb sociálních sítí. Stanovisko ukazuje, kolik uživatelů pracuje v čistě soukromé oblasti a kontaktuje jiné osoby jako součást spravování svých osobních, rodinných nebo domácích záležitostí. V těchto případech má stanovisko za to, že platí „výjimka pro domácí použití“ a že se nepoužijí předpisy upravující činnost správců údajů. Stanovisko rovněž upřesňuje situace, kdy se na činnosti uživatele služeb sociálních sítí nevztahuje „výjimka pro domácí použití“. Hlavní obavu pro pracovní skupinu podle článku 29 představuje šíření a využívání informací, které jsou dostupné na internetových stránkách sociálních sítí, pro jiné druhotné, nezamýšlené účely. V celém stanovisku je obhajováno silné standardní nastavení respektující bezpečnost a soukromí jako ideální výchozí bod, co se týká všech nabízených služeb. Hlavní oblastí obav je přístup k informacím o profilu. Stanovisko se zabývá rovněž tématy jako zpracování citlivých údajů a snímků, reklama a přímý marketing na internetových stránkách sociálních sítí a otázky týkající se uchovávání údajů.

Hlavní doporučení se zaměřují na povinnost poskytovatelů služeb sociálních sítí dodržovat směrnici o ochraně údajů a podporovat a posilovat práva uživatelů. Je nanejvýš důležité, aby poskytovatelé služeb sociálních sítí měli od počátku informovat uživatele o své totožnosti a měli by uvést veškeré jednotlivé účely zpracování osobních údajů. Zvláštní pozornost by měli poskytovatelé služeb sociálních sítí věnovat zpracování osobních údajů nezletilých osob. Stanovisko doporučuje, aby uživatelé přenášeli obrázky nebo informace o jiných fyzických osobách pouze se souhlasem dotyčné osoby, a domnívá se, že poskytovatelé služeb sociálních sítí mají rovněž povinnost informovat uživatele o právu ostatních osob na soukromí.

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

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

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

s ohledem na 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 jednací řád pracovní skupiny,

PŘIJALA TENTO DOKUMENT:

1. Úvod

Vývoj internetových komunit a hostovaných služeb, jako jsou služby sociálních sítí (dále jen „SSS"), je poměrně novým jevem, přičemž počet uživatelů těchto internetových stánek nadále roste geometrickou řadou.

Osobní údaje, které uživatel vyvěsí na internetu, spolu s údaji o činnostech uživatele a jeho vztazích s ostatními lidmi, mohou vytvořit bohatý profil zájmů a činností této osoby. Osobní údaje zveřejněné na internetových stránkách sociálních sítí mohou využít třetí strany k řadě účelů, včetně obchodních, a mohou představovat značná rizika, jako je krádež totožnosti, finanční ztráty, ztráta obchodních příležitostí či možnosti zaměstnání a tělesná újma.

Berlínská Mezinárodní pracovní skupina pro ochranu údajů v telekomunikacích přijala v březnu 2008 *Římské memorandum*[2]. Memorandum analyzuje rizika pro soukromí a bezpečnost, která představují sociální sítě, a poskytuje pokyny pro regulační orgány, poskytovatele a uživatele. Nedávno přijaté usnesení o ochraně soukromí ve službách sociálních sítí[3] rovněž vyzdvihuje problémy, které SSS přinášejí. Pracovní skupina rovněž bere v úvahu písemné stanovisko Evropské agentury pro bezpečnost sítí a informací (ENISA) s názvem „*Bezpečnostní otázky a doporučení pro internetové sociální sítě*"[4] zveřejněné v říjnu 2007, které je určeno regulačním orgánům a poskytovatelům sociálních sítí.

2. Vymezení „služby sociální sítě (SSS)" a obchodní model

SSS lze obecně vymezit jako on-line komunikační platformy, které jednotlivcům umožňují spojovat se se sítěmi nebo vytvářet sítě stejně smýšlejících uživatelů. Z právního hlediska jsou sociální sítě službami informační společnosti definovanými v čl. 1 odst. 2 směrnice 98/34/ES ve znění směrnice 98/48/ES. SSS sdílejí určité vlastnosti:

– uživatelé jsou vyzýváni, aby poskytli osobní údaje za účelem vytvoření svého popisu nebo „profilu",

[1] Úřední věstník L 281, 23.11.1995, s. 31, http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm

[2] http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf.

[3] Přijaté na 30. Mezinárodní konferenci inspektorů ochrany údajů a soukromého života ve Štrasburku, 17.10.2008, http://www.privacyconference2008.org/adopted_resolutions/STRASBOURG2008/resolution_social_networks_en.pdf.

[4] http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf.

– SSS rovněž poskytují nástroje, které uživatelům umožňují vyvěsit své vlastní materiály (obsah vytvořený uživatelem, např. fotografie nebo zápis v deníku, hudbu nebo videoklip či odkazy na jiné internetové stránky[5]),

– „vytváření sociálních sítí“ je umožněno pomocí nástrojů, které obsahují seznam kontaktů u každého uživatele a pomocí nichž mohou uživatelé vzájemně reagovat.

SSS získávají velkou část svých příjmů z reklamy, jež je poskytována spolu s internetovými stránkami, které vytvořili uživatelé a na něž mají uživatelé přístup. Uživatelé, kteří na svých profilech vyvěsí velké množství informací o svých zájmech, poskytují upřesněný trh inzerentům, kteří na základě těchto informací chtějí zasílat cílené reklamy.

Je proto důležité, aby SSS fungovaly způsobem, jenž respektuje práva a svobody uživatelů, kteří mají oprávněná očekávání, že osobní údaje, které zveřejní, budou zpracovány podle evropských a vnitrostátních právních předpisů v oblasti ochrany údajů a soukromí.

3. Uplatňování směrnice o ochraně údajů

Na poskytovatele SSS se ve většině případů vztahují ustanovení směrnice o ochraně údajů, a to i tehdy, jestliže se jejich ústředí nacházejí mimo EHP. Pracovní skupina podle článku 29 odkazuje na své dřívější stanovisko k vyhledávačům, pokud jde o další pokyny k otázkám usazení a používání vybavení jako rozhodujících činitelů pro použitelnost směrnice o ochraně údajů a pravidel, které si vyžádalo protokolování IP adres a používání cookies[6].

3.1 Kdo je správce údajů?

Poskytovatelé SSS

Poskytovatelé SSS jsou správci údajů podle směrnice o ochraně údajů. Poskytují prostředky pro zpracování uživatelských údajů a veškeré „základní“ služby související se správou uživatelů (např. registrace a rušení účtů). Poskytovatelé SSS rovněž určují možné použití uživatelských údajů pro účely reklamy a marketingu – včetně reklamy zajišťované třetími stranami.

Poskytovatelé aplikací

Správci údajů mohou být rovněž poskytovatelé aplikací, pokud vyvíjejí aplikace, které fungují spolu s aplikacemi SSS, a o použití takových aplikací rozhodují uživatelé.

Uživatelé

Ve většině případů se uživatelé považují za subjekty údajů. Směrnice neukládá povinnosti správce údajů fyzické osobě, která zpracovává osobní údaje „*pro výkon výlučně osobních či domácích činností*“ – tzv. „výjimka pro domácí použití“. V některých případech se na činnosti uživatele SSS nemusí vztahovat výjimka pro domácí použití a lze mít za to, že uživatel přebírá určité odpovědnosti správce údajů. Níže jsou uvedeny některé z těchto příkladů:

[5] V případech, že SSS poskytují služby elektronických komunikací, se použijí rovněž ustanovení směrnice o soukromí a elektronických komunikacích 2002/58.

[6] WP148, „Stanovisko č. 1/2008 k otázkám ochrany údajů v souvislosti s vyhledávači“.

3.1.1. Účel a povaha

Rostoucím trendem SSS je „*přechod z „Web 2.0 pro zábavu na Web 2.0 pro produktivitu a služby*“[7], kdy činnosti některých uživatelů SSS mohou překročit výlučně osobní či domácí činnosti, je-li například SSS použita jako platforma pro spolupráci určitého sdružení nebo společnosti. Pokud uživatel SSS jedná jménem společnosti či sdružení nebo používá SSS převážně jako platformu na podporu obchodních, politických nebo charitativních cílů, zmíněná výjimka neplatí. V tomto případě uživatel přebírá veškeré odpovědnosti správce údajů, který poskytuje osobní údaje jinému správci údajů (poskytovateli SSS) a třetím stranám (ostatní uživatelé SSS nebo případně další správci údajů s přístupem k těmto údajům). V těchto případech musí mít uživatel souhlas dotčených osob nebo jiný legitimní základ stanovený ve směrnici o ochraně údajů.

Obvykle je přístup k údajům (údaje z profilu, vyvěšené zprávy, příběhy …) poskytnutým uživatelem omezen na kontakty, které si uživatel sám vybere. V některých případech však mohou uživatelé získat vysoký počet kontaktů třetích stran, z nichž některé nemusí ve skutečnosti znát. Vysoký počet kontaktů by mohl být signálem, že neplatí výjimka pro domácí použití a uživatel je proto považován za správce údajů.

3.1.2. Přístup k údajům o profilu

Poskytovatelé SSS by měli zdarma zajistit standardní nastavení respektující soukromí, které omezuje přístup ke kontaktům podle vlastního výběru.

Pokud přístup k údajům z profilu přesahuje kontakty podle vlastního výběru, je-li například přístup k profilu umožněn všem členům v rámci SSS[8] nebo jsou-li údaje indexovatelné vyhledávači, přístup přesahuje osobní nebo domácí oblast. Stejně tak v případě, že uživatel přijme informované rozhodnutí o rozšíření přístupu mimo „přátele“ podle vlastního výběru, nabývají platnosti odpovědnosti správce údajů. Pak bude platit stejný právní režim jako v případě, kdy jakákoli osoba používá jiné technologické platformy ke zveřejnění osobních údajů na internetu[9]. V řadě členských států neexistence omezení přístupu (tedy veřejný charakter) znamená, že platí směrnice o ochraně údajů, pokud jde o uživatele internetu, který nabývá odpovědnosti správce údajů[10].

Je nutno mít na paměti, že i v případě, že neplatí výjimka pro domácí použití, může uživatel SSS využít jiných výjimek, jako je výjimka pro publicistické účely, umělecký nebo literární projev. V těchto případech je nutno usilovat o rovnováhu mezi svobodou projevu a právem na soukromí.

3.1.3 Zpracování údajů třetích stran uživateli

Uplatnění výjimky pro domácí použití je omezeno rovněž nutností zaručit práva třetích stran, zejména co se týká citlivých údajů. Dále je nutné podotknout, že i v případě, že platí výjimka pro domácí použití, může být uživatel odpovědný podle obecných ustanovení dotyčných vnitrostátních občanskoprávních nebo trestních předpisů (např. pomluva, odpovědnost za

---

[7] „Internet budoucnosti: Evropa musí být hlavním hráčem“, projev Viviane Redingové, evropské komisařky pro informační společnost a média během zasedání iniciativy Lisabonské rady „Budoucnost internetu“, Brusel, 2. února 2009.

[8] Nebo lze-li tvrdit, že při přijetí kontaktů nebyl proveden skutečný výběr, tj. uživatelé akceptují „kontakty“ bez ohledu na existující vztahy.

[9] Např. u publikačních platforem, které nejsou SSS, nebo v případě programového vybavení ve vlastním prostředí.

[10] Ve svém rozsudku ve věci Satamedia ESD v bodě 44 naopak uvedl: „*Z toho plyne, že tato druhá výjimka musí být vykládána tak, že se vztahuje výhradně na činnosti spadající do rámce soukromého či rodinného života jednotlivců (viz výše uvedený rozsudek Lindqvist, bod 47). Tak tomu zjevně není, pokud jde o činnosti Markkinapörssi a Satamedia, jejichž předmětem je seznámit se shromážděnými údaji neomezený počet osob.*“

občanskoprávní delikty v souvislosti s porušením práva na ochranu osobnosti, trestní odpovědnost).

3.2 Standardní nastavení respektující bezpečnost a soukromí

Hlavním prvkem důvěry v SSS je bezpečné zpracování informací. Správci musí přijmout příslušná technická a organizační opatření „jak při přípravě systému zpracování, tak v průběhu vlastního zpracování“ s cílem zajistit bezpečnost a zabránit jakémukoli neoprávněnému zpracování, s přihlédnutím k rizikům vyplývajícím ze zpracování údajů a z povahy údajů[11].

Důležitým prvkem nastavení respektujícího soukromí je přístup k osobním údajům zveřejněným v profilu. Není-li tento přístup omezen, mohou třetí strany sestavovat jakýkoliv druh důvěrných údajů týkajících se uživatelů, buď jako členové SSS, nebo prostřednictvím vyhledávačů. Avšak pouze menšina uživatelů přihlašujících se ke službě provede změny standardního nastavení. Poskytovatelé SSS by proto měli nabízet standardní nastavení respektující soukromí, které uživatelům umožní svobodně a výslovně souhlasit s přístupem k obsahu jejich profilu kromě kontaktů podle vlastního výběru s cílem snížit riziko neoprávněného zpracování těchto údajů třetími stranami. Profily s omezeným přístupem by nemělo být možné vyhledat interními vyhledávači, včetně funkce vyhledávání podle parametrů jako věk nebo místo. Rozhodnutí o rozšíření přístupu nemohou být implicitní[12], například možnost „aktivního nesouhlasu“ poskytnutá správcem SSS.

3.3 Informace, které mají SSS poskytovat

Poskytovatelé SSS by měli uživatele informovat o své totožnosti a různých účelech zpracování osobních údajů podle ustanovení článku 10 směrnice o ochraně údajů, včetně například:

– použití údajů pro účely přímého marketingu,

– případné sdílení údajů se stanovenými kategoriemi třetích stran,

– přehled o profilech: jejich vytváření a hlavní zdroje dat,

– použití citlivých údajů.

Pracovní skupina doporučuje, aby:

– poskytovatelé SSS uživatele přiměřeně upozornili na ohrožení soukromí jich samotných i ostatních osob při přenášení údajů na SSS,

– uživatelům SNS by mělo být rovněž připomenuto, že přenášení informací o jiných fyzických osobách může porušit práva dotčených osob na soukromí a ochranu údajů,

– poskytovatelé SSS by měli uživatelům SSS rovněž doporučit, aby v případě, že chtějí přenést obrázky nebo informace o jiných fyzických osobách, tak učinili pouze s jejich souhlasem[13].

---

[11] Článek 17 a bod 46 odůvodnění směrnice o ochraně údajů.

[12] Zpráva a pokyny o soukromí v službách sociálních sítí („Římské memorandum“) uvádí rizika jako „klamný pojem komunity“, s. 2, „poskytnutí více osobních údajů, než si myslíte, že jste poskytli“, s. 3. Společnost pro počítačovou bezpečnost upozorňuje důležitou SSS na standardní přístup ke členům se stejnou zeměpisnou polohou: http://www.sophos.com/pressoffice/news/articles/2007/10/facebook-network.html.

[13] To by mohlo být usnadněno zavedením nástrojů ke správě označování na internetových stránkách sociálních sítí, např. zpřístupněním oblastí v osobním profilu za účelem uvedení, že se čeká na souhlas s uvedením jména uživatele na

3.4 Citlivé údaje

Údaje odhalující rasový nebo etnický původ, politické názory, náboženské nebo filozofické přesvědčení, členství v odborových svazech nebo údaje o zdraví či sexuálním životě jsou považovány za citlivé. Citlivé osobní údaje mohou být na internetu zveřejněny pouze s výslovným souhlasem subjektu údajů nebo tehdy, jestliže subjekt údajů zjevně sám zveřejnil tyto údaje[14].

V některých členských státech EU se snímky subjektů údajů považují za zvláštní kategorii osobních údajů, jelikož mohou být použity ke zjištění rasového/etického původu nebo k odvození náboženského přesvědčení či zdravotních údajů. Pracovní skupina obecně nepovažuje snímky na internetu za citlivé údaje[15], nejsou-li snímky jednoznačně použity k odhalení citlivých údajů o fyzických osobách.

Jako správci údajů nesmí poskytovatelé SSS zpracovávat citlivé údaje o členech či nečlenech SSS bez jejich výslovného souhlasu[16]. Pokud poskytovatel SSS zařadí do formuláře profilu uživatelů otázky týkající se citlivých údajů, musí objasnit, že zodpovězení těchto otázek je zcela dobrovolné.

3.5 Zpracování údajů nečlenů

Mnoho SSS uživatelům umožňuje, aby poskytli údaje o jiných osobách, například připojením jména k obrázku, ohodnocením osoby, uvedením „osob, které jsem potkal/a / s nimiž bych se chtěl/a setkat“ na akcích. Toto označování může rovněž identifikovat nečleny. Zpracování těchto údajů o nečlenech poskytovateli SSS lze provádět pouze v případě, je-li splněno jedno z kritérií stanovených v článku 7 směrnice o ochraně údajů.

Vytváření předem vyhotovených profilů nečlenů prostřednictvím seskupování údajů, které jsou nezávisle poskytnuty uživateli SSS, včetně údajů o vztahu odvozených z předaných adresářů, nemá právní základ[17].

V případě, že SSS má prostředky ke kontaktování neuživatele a informování tohoto neuživatele o existenci osobních údajů, které se ho týkají, by případný e-mail s výzvou, aby se tento přihlásil k SSS za účelem získání přístupu k těmto osobním údajům, znamenal porušení zákazu stanoveného v čl. 13 odst. 4 směrnice o soukromí a elektronických komunikacích, který se týká zasílání nevyžádaných elektronických sdělení pro účely přímého marketingu.

3.6 Přístup třetích stran

3.6.1 Přístup zprostředkovaný pomocí SSS

Kromě základní služby SSS nabízí většina SSS uživatelům dodatečné aplikace poskytované třetími stranami, které také zpracovávají osobní údaje.

---

označených snímcích nebo videonahrávkách, nebo stanovení termínu pro odstranění označení, pro něž označená fyzická osoba neposkytla souhlas.

14 Členské státy mohou stanovit výjimky z tohoto pravidla, viz čl. 8 odst. 2 písm. a) druhá věta a čl. 8 odst. 4 směrnice o ochraně údajů.

15 Zveřejňování obrázků na internetu však vyvolává rostoucí obavy ohledně ochrany soukromí s tím, jak se zlepšují technologie pro rozpoznávání tváří.

16 Souhlas musí být svobodný, výslovný a vědomý.

17 38. bod odůvodnění směrnice o ochraně údajů uvádí: „*Vzhledem k tomu, že korektní zpracování údajů předpokládá, že subjekty údajů jsou informovány o probíhajícím zpracování a že mají nárok, pokud jsou údaje získávány od nich, na přesné a úplné informace o okolnostech tohoto shromažďování*“. Pro některé SSS se zveřejňování profilů nečlenů údajně stává důležitým způsobem marketingu jejich „služeb“.

SSS by měly mít prostředky k zajištění toho, aby aplikace třetích stran splňovaly směrnici o ochraně údajů a směrnici o soukromí a elektronických komunikacích. To zejména znamená, že by měly uživatelům poskytnout jednoznačné a konkrétní informace o zpracování jejich osobních údajů a že mají přístup pouze k nezbytným osobním údajům. Třetím stranám – vývojářům aplikací by proto měl být ze strany SSS umožněn víceúrovňový přístup, takže lze rozhodnout o způsobu přístupu, který je ve své podstatě omezenější. Poskytovatelé SSS by měli dále zajistit, aby uživatelé mohli snadno sdělit své obavy týkající se těchto aplikací.

3.6.2 Přístup třetích stran zprostředkovaný uživateli

Poskytovatelé SSS někdy uživatelům umožňují přístup k údajům a jejich aktualizaci pomocí třetích aplikací. Uživatelé mohou být například s to:

– číst a vyvěšovat sdělení pro síť ze svého mobilního telefonu,

– synchronizovat kontaktní údaje svých přátel v rámci SSS s adresářem ve stolním počítači,

– aktualizovat svůj stav nebo polohu v SSS automaticky pomocí jiných internetových stránek.

Poskytovatelé SSS zveřejňují způsob, jakým lze toto programové vybavení vytvořit, a to formou „aplikačního programového rozhraní“ („API“). To umožňuje kterékoli třetí straně vytvořit programové vybavení k provádění těchto úkolů a uživatelé si mohou svobodně vybrat mezi několika třetími poskytovateli[18]. Při poskytování API, které umožňuje přístup k údajům kontaktů, by poskytovatelé SSS měli:

– zajistit úroveň granularity, jež uživateli umožňuje zvolit pro třetí stranu úroveň přístupu, která postačuje k provádění pouze určitého úkolu.

Při přístupu k osobním údajům prostřednictvím API třetí strany jménem uživatele by služby třetích stran měly:

– zpracovávat a uchovávat údaje pouze po dobu potřebnou k provedení určitého úkolu;

– neprovádět s převedenými údaji kontaktů uživatele jiné operace než osobní použití poskytujícím uživatelem.

3.7 Právní důvody pro přímý marketing

Přímý marketing je základní součástí obchodního modelu SSS; SSS mohou používat různé marketingové modely. Marketing s využitím osobních údajů uživatelů by však měl splňovat příslušná ustanovení směrnice o ochraně údajů i směrnice o soukromí a elektronických komunikacích[19].

Kontextový marketing je přizpůsoben obsahu, který si uživatel prohlíží nebo k němuž má přístup[20].

Segmentovaný marketing spočívá v zasílání reklamy cílovým skupinám uživatelů[21]; uživatel je zařazen do skupiny podle informací, které přímo sdělil SSS[22].

---

[18] Zatímco „API“ je obecný technický pojem, zde API odkazuje na přístup jménem uživatele, tj. uživatelé musí programovému vybavení poskytnout přihlašovací údaje, aby toto mohlo fungovat jejich jménem.

[19] Pracovní skupina se v blízké budoucnosti hodlá zabývat různými aspekty on-line reklamy ve zvláštním dokumentu.

[20] Např. je-li na zobrazené stránce uvedeno slovo „Paříž“, může se reklama týkat restaurace v tomto městě.

[21] Každá skupina je vymezená souborem kritérií.

Behaviorální marketing vybírá reklamu na základě pozorování a analýzy činnosti uživatelů během určité doby. Tyto techniky mohou podléhat různým právním požadavkům v závislosti na použitelných právních důvodech a charakteristikách použitých technik. Pracovní skupina doporučuje nepoužívat v modelech behaviorálního marketingu citlivé údaje, nejsou-li splněny všechny právní požadavky.

Bez ohledu na to, jaký model či kombinace modelů se použije, mohou být reklamy zasílány buď přímo SSS (zde poskytovatel SSS jedná jako zprostředkovatel), nebo inzerentem – třetí stranou. V prvním případě nemusí být osobní údaje uživatelů sděleny třetím stranám. V druhém případě však může osobní údaje o uživatelích zpracovávat inzerent – třetí strana, například pokud zpracovává IP adresu uživatele a cookie v počítači uživatele.

3.8 Uchovávání údajů

SSS nepatří do oblasti působnosti definice služeb elektronických komunikací uvedené v čl. 2 písm. c) rámcové směrnice (2002/21/ES). Poskytovatelé SSS mohou nabízet dodatečné služby, které spadají do oblasti působnosti služeb elektronických komunikací, například veřejně dostupnou e-mailovou službu. Takováto služba bude podléhat ustanovením směrnice o soukromí a elektronických údajích i směrnice o uchovávání údajů.

Některé SSS umožňují, aby jejich uživatelé zasílali výzvy třetím stranám. Zákaz používání elektronické pošty pro účely přímého marketingu se nevztahuje na osobní sdělení. Ke splnění výjimky pro osobní komunikaci musí SSS dodržet tato kritéria:

– odesílateli ani příjemci nejsou poskytnuty žádné pobídky,

– poskytovatel nevybírá příjemce sdělení[23],

– musí být jednoznačně uvedena totožnost odesílajícího uživatele,

– odesílající uživatel musí znát celý obsah sdělení, které bude zasláno jeho jménem.

Některé SSS uchovávají rovněž identifikační údaje uživatelů, kteří jsou vyloučeni ze služby, s cílem zajistit, aby se nemohli znovu zaregistrovat. V tomto případě musí být tito uživatelé informováni o tomto zpracování. Jedinou informací, kterou lze uchovávat, je mimoto identifikační údaj, nikoli důvody vyloučení těchto osob. Tento údaj by neměl být uchováván déle než jeden rok.

Osobní údaje předané uživatelem při registraci k SSS by měly být vymazány, jakmile se uživatel nebo poskytovatel SSS rozhodne účet zrušit[24]. Stejně tak by neměly být uchovávány údaje, které uživatel vymazal při aktualizaci svého účtu. Poskytovatelé SSS by před podniknutím těchto kroků měli uživatele informovat o době uchovávání pomocí prostředků, které mají k dispozici. Z bezpečnostních a právních důvodů by v určitých případech mohlo být opodstatněné uchovávání aktualizovaných nebo smazaných údajů a účtů po stanovenou dobu, aby se zamezilo nezákonnému úmyslnému jednání plynoucímu z krádeže totožnosti a jiných přestupků nebo trestných činů.

Pokud uživatel službu po stanovenou dobu nepoužívá, profil by se měl stát neaktivním, tj. ostatní uživatelé nebo vnější svět by neměli mít možnost si jej prohlížet, a po další době by

---

22 Např. při registraci ke službě.

23 Tj. praxe některých SSS zasílat výzvy bez rozdílu celému adresáři uživatele není přípustná.

24 Podle čl. 6 odst. 1 písm. e) směrnice o ochraně údajů musí být údaje *„uchovávány ve formě umožňující identifikaci subjektů údajů po dobu ne delší než je nezbytné pro uskutečnění cílů, pro které jsou shromažďovány nebo dále zpracovávány“*.

měly být údaje na nevyužívaném účtu smazány. Poskytovatelé SSS by před podniknutím těchto kroků měli uživatele vyrozumět pomocí jakýchkoli prostředků, které mají k dispozici.

3.9 Práva uživatelů

SSS by měly respektovat práva fyzických osob, jichž se zpracování údajů týká, podle ustanovení článků 12 a 14 směrnice o ochraně údajů.

Práva uživatelů na přístup k údajům a jejich opravu nejsou omezena na uživatele služby, nýbrž na všechny fyzické osoby, jejichž údaje jsou zpracovávány[25]. Členové a nečlenové SSS musí být prostředky k uplatnění svých práv na přístup, opravu a výmaz. Domovská stránka SSS by měla jednoznačně odkazovat na existenci „subjektu pro vyřizování stížností", který poskytovatel SSS zřídil za účelem řešení otázek týkajících se ochrany údajů a soukromí a vyřizování stížností podaných členy i nečleny.

Čl. 6 odst. 1 písm. c) směrnice o ochraně údajů vyžaduje, aby údaje byly *„přiměřené, podstatné a nepřesahující míru s ohledem na účely, pro které jsou shromažďovány a/nebo dále zpracovávány"*. V této souvislosti je možno poznamenat, že pro SSS může být nezbytné zaregistrování určitých identifikačních údajů členů, nesmí však zveřejnit skutečná jména členů na internetu. Poskytovatelé SSS by proto měli pečlivě uvážit, zda mohou odůvodnit to, že své uživatele nutí, aby vystupovali pod svou skutečnou identitou místo pod přezdívkou. Existují pádné argumenty pro to, poskytnout uživatelům v tomto ohledu možnost výběru, a nejméně v jednom členském státě to představuje právní požadavek. Argumenty jsou obzvláště pádné v případě SSS s velkým počtem členů.

Článek 17 směrnice o ochraně údajů vyžaduje, aby správce přijal vhodná technická a organizační opatření na ochranu osobních údajů. K těmto bezpečnostním opatřením patří zejména kontrola přístupu a mechanismy pro ověření totožnosti, které lze zavést i v případě, jsou-li používány přezdívky.

4. Děti a nezletilé osoby

Velkou část služeb SSS využívají děti nebo nezletilé osoby. Stanovisko pracovní skupiny WP147[26] se zaměřilo na uplatňování zásad ochrany údajů ve školním a vzdělávacím prostředí. Stanovisko vyzdvihlo potřebu zohlednit nejlepší zájem dítěte, jak je rovněž stanoveno v Úmluvě OSN o právech dítěte. Pracovní skupina chce zdůraznit význam této zásady také v souvislosti se SSS.

Orgány pro ochranu údajů po celém světě přijaly některé zajímavé iniciativy[27], které se zaměřují především na zvyšování informovanosti o SSS a možných rizicích. Pracovní skupina podporuje další výzkum týkající se odstranění potíží souvisejících s ověřením přiměřeného věku a prokázáním vědomého souhlasu k lepšímu řešení těchto problémů.

Na základě dosud zmíněných úvah se pracovní skupina domnívá, že by k řešení otázek ochrany údajů dítěte v rámci SSS byla vhodná mnohostranná strategie. Tato strategie by mohla být založena na:

– iniciativách na zvýšení informovanosti, které jsou zásadní pro zajištění aktivní účasti dětí (prostřednictvím škol, zařazením základů ochrany údajů do učebních osnov,

[25] Např. tak je tomu v případě, pokud SSS použila e-mailovou adresu této osoby k zaslání výzvy.
[26] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp147_en.pdf.
[27] Např. portugalská iniciativa „Dadus" http://dadus.cnpd.pt/, dánská iniciativa „Chat Check Badge", http://www.fdim.dk/.

vytvořením vzdělávacích nástrojů ad hoc, prostřednictvím spolupráce příslušných vnitrostátních orgánů),

– oprávněném a zákonném zpracování údajů s ohledem na nezletilé osoby, například nevyžadování sdělování citlivých údajů v přihlašovacích formulářích, žádný přímý marketing zaměřený výslovně na nezletilé osoby, předchozí souhlas rodičů před přihlášením a náležitý stupeň logického oddělení komunit dětí a dospělých,

– zavedení technologií zlepšujících ochranu soukromí – např. standardní nastavení respektující soukromí, vyskakovací okna s upozorněním při provádění příslušných kroků, programové vybavení k ověření věku,

– samoregulaci ze strany poskytovatelů s cílem podporovat přijetí kodexů s účinnými donucovacími opatřeními, rovněž kázeňské povahy,

– v případě potřeby legislativních opatřeních ad hoc s cílem odrazovat od nekalých a/nebo podvodných postupů v rámci SSN.

5. Shrnutí povinností/práv

Použitelnost směrnic ES

1. Směrnice o ochraně údajů se obecně vztahuje na zpracování osobních údajů poskytovateli SSS i v případě, že se jejich ústředí nachází mimo EHP.

2. Poskytovatelé SSS jsou považováni za správce údajů podle směrnice o ochraně údajů.

3. Poskytovatelé aplikací mohou být považováni za správce údajů podle směrnice o ochraně údajů.

4. Uživatelé jsou s ohledem na zpracování jejich údajů poskytovateli SSS považováni za subjekty údajů.

5. Zpracování osobních údajů uživateli ve většině případů spadá do výjimky pro domácí použití. Existují rovněž případy, kdy se tato výjimka na činnosti uživatele nevztahuje.

6. SSS nespadají do oblasti působnosti definice služby elektronických komunikací, na SSS se proto nevztahuje směrnice o uchovávání údajů.

Povinnosti poskytovatelů SSS

7. Poskytovatelé SSS by měli uživatelům sdělit svou totožnost a poskytnout úplné a jednoznačné informace o zamýšlených účelech a různých způsobech zpracování osobních údajů.

8. Poskytovatelé SSS by měli zajistit standardní nastavení respektující soukromí.

9. Poskytovatelé SSS by měli uživatelům poskytnout informace a přiměřené upozornění na rizika pro soukromí při přenášení údajů na SSS.

11. Poskytovatelé SSS by měli uživatelům doporučit, aby obrázky nebo informace o jiných fyzických osobách byly přenášeny pouze se souhlasem dotčených osob.

12. Minimálně domovská stránka SSS by měla obsahovat odkaz na subjekt pro vyřizování stížnosti zabývající se otázkami ochrany údajů, a to pro členy i nečleny.

13. Marketingová činnost musí dodržovat pravidla stanovená ve směrnici o ochraně údajů a ve směrnici o soukromí a elektronických komunikacích.

14. Poskytovatelé SSS musí stanovit maximální lhůty pro uchovávání údajů o neaktivních uživatelích. Nevyužívané účty je nutno zrušit.

15. Co se týká nezletilých osob, poskytovatelé SSS by měli přijmout příslušná opatření k omezení rizik.

<u>Práva uživatelů</u>

16. Členové a popřípadě nečlenové SSS mají práva subjektů údajů podle ustanovení článků 10–14 směrnice o ochraně údajů.

17. Členové i nečlenové by měli mít přístup k snadnému postupu vyřizování stížností zavedenému poskytovatelem SSS.

18. Uživatelé by měli mít obecně možnost používat přezdívku.

V Bruselu dne 12. června 2009
Za pracovní skupinu
předseda
Alex TÜRK

IV. MATERIÁLY Z ÚŘEDNÍHO VĚSTNÍKU EVROPSKÉ UNIE

Příloha Věstníku Úřadu pro ochranu osobních údajů (s. 3130 – 3138)

Stanovisko evropského inspektora ochrany údajů k návrhu směrnice Evropského parlamentu a Rady o jakostních a bezpečnostních normách pro lidské orgány určené k transplantaci

(2009/C 192/02)

EVROPSKÝ INSPEKTOR OCHRANY ÚDAJŮ,

s ohledem na Smlouvu o založení Evropského společenství, a zejména na článek 286 této smlouvy,

s ohledem na Listinu základních práv Evropské unie, a zejména na článek 8 této listiny,

s ohledem na směrnici Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů,

s ohledem na nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů, a zejména na článek 41 tohoto nařízení,

s ohledem na žádost o stanovisko v souladu s čl. 28 odst. 2 nařízení (ES) č. 45/2001 zaslané evropskému inspektorovi ochrany údajů dne 8. prosince 2008,

ZAUJAL TOTO STANOVISKO:

I. ÚVOD

Návrh směrnice o jakostních a bezpečnostních normách pro orgány určené k transplantaci.

1. Dne 8. prosince 2008 přijala Komise návrh směrnice Evropského parlamentu a Rady o jakostních a bezpečnostních normách pro lidské orgány určené k transplantaci (dále pouze „návrh“) [1]. Návrh zaslala Komise v souladu s čl. 28 odst. 2 nařízení (ES) č. 45/2001 evropskému inspektorovi ochrany údajů ke konzultaci.

2. Cílem návrhu je zajistit vysoké jakostní a bezpečnostní normy pro lidské orgány určené k transplantaci a zajistit tak vysokou úroveň ochrany lidského zdraví. V návrhu se zejména:

   — stanoví základní jakostní a bezpečnostní požadavky na transplantační systémy členských států a vytvoření nebo jmenování příslušného vnitrostátního orgánu, který by zajistil soulad s těmito požadavky. Za tímto účelem budou ve všech zemích zavedeny národní programy jakosti pro odběr a přepravu lidských orgánů, mimo jiné včetně systému *hlášení o závažných nežádoucích účincích a reakcích* a *mechanismů sledovatelnosti*, aby byla zajištěna možnost sledování všech orgánů od darování až po přijetí a opačně,

   — stanoví ochranu dárců a příjemců. Zejména v souvislosti s žijícími dárci jsou v návrhu zahrnuta opatření na posouzení zdravotního stavu dárce, podrobné informace o rizicích spojených s darováním, zavedení *registrů žijících dárců* a opatření k zajištění altruistického a dobrovolného dárcovství orgánů žijícími dárci,

   — stanoví usnadnění spolupráce mezi členskými státy a *přeshraniční výměny orgánů* (rovněž mezi členskými státy a třetími zeměmi) díky standardizaci sběru příslušných informací o charakteristikách orgánů a díky stanovení mechanismů předávání informací.

3. Uskutečňování navrhovaných režimů dárcovství orgánů a transplantací vyžaduje zpracovávání osobních údajů týkajících se zdraví („údajů o zdravotním stavu“) dárců a příjemců orgánů pověřenými organizacemi a zdravotnickými pracovníky různých členských států. Tyto údaje jsou považovány za citlivé a vztahují se na ně přísnější pravidla ochrany údajů, jak stanoví článek 8 směrnice 95/46/ES o zvláštních kategoriích údajů.

4. Přesněji řečeno, údaje o dárcích se zpracovávají v organizacích provádějících odběr, které provedou charakterizaci dárce a orgánu a určí, zda je posuzovaný orgán vhodný k transplantaci (seznam těchto údajů je uveden v příloze návrhu). Údaje o příjemcích (pacientech) se zpracovávají v transplantačních centrech, kde se provádí samotná operace. Ačkoli se údaje o dárci příjemci (a opačně) nesdělují, požaduje se, aby příslušné vnitrostátní orgány zajistily plnou sledovatelnost orgánu od dárce k příjemci (a opačně), což by mělo být možné rovněž v případě přeshraniční výměny orgánů.

Konzultace s evropským inspektorem ochrany údajů

5. Evropský inspektor ochrany údajů vítá, že je v této otázce konzultován a že odkaz na tuto konzultaci je v souladu s článkem 28 nařízení (ES) č. 45/2001 uveden v preambuli návrhu.

[1] KOM(2008) 818 v konečném znění.

6. Návrh chce podpořit dárcovství orgánů a transplantační postupy, aby se tak zvýšila dostupnost orgánů a snížila úmrtnost čekatelů zařazených do pořadníků na orgány. Doplňuje stávající legislativní rámec s ohledem na používání biologického materiálu lidského původu ([1]). Navíc je možné jej považovat za část celkového přístupu EU ke stanovování různých typů společných norem v oblasti poskytování zdravotnických služeb v členských státech, jejichž základním cílem je podpořit přeshraniční dostupnost těchto služeb po celé Evropě ([2]). Evropský inspektor ochrany údajů tento přístup podporuje, jak již uvedl ve stanovisku k právům pacientů v přeshraniční zdravotní péči. Znovu však zdůrazňuje, že je v různých iniciativách v oblasti zdravotnické péče nutný dobře koordinovaný a jednotný pohled na ochranu údajů ([3]).

7. V návrhu již byly zohledněny potřeby v oblasti ochrany údajů, a to jak v případě dárců, tak i v případě příjemců orgánů. Nejdůležitějším prvkem je požadavek na zachování anonymity dárců a příjemců (11. a 16. bod odůvodnění, články 10 a 17). V některých částech návrhu je možné dále najít obecné odkazy na ochranu údajů (17. bod odůvodnění, článek 16, čl. 4 odst. 3 písm. a), čl. 15 odst. 3, čl. 19 odst. 1 písm. a) a příloha), jakož i konkrétnější odkazy na potřebu spolupráce s vnitrostátními orgány pro ochranu údajů (čl. 18 písm. f) a čl. 20 odst. 2).

8. Evropský inspektor ochrany údajů výše uvedený obsah vítá. Rád by však vyjádřil znepokojení nad některými ustanoveními, která nejsou jasně definována nebo rozpracována, a vedou tudíž k dvojznačnosti, což by mohlo ovlivnit jednotné provádění návrhu členskými státy.

9. Konkrétněji řečeno, je nutné více ujasnit a upřesnit rozporuplné používání pojmů „sledovatelnost orgánů“ a „anonymita dárců a příjemců“. V souvislosti s tím by se měla dále zdůraznit nutnost přijmout přísnější bezpečnostní opatření, pokud jde o ochranu údajů dárců a příjemců na úrovni členských států, zaručit zvýšenou úroveň ochrany údajů v různých evropských zemích a zajistit ochranu údajů při přeshraniční výměně orgánů (v rámci Evropy nebo mimo Evropu).

10. Toto stanovisko se bude výše uvedenými otázkami zabývat ještě podrobněji s cílem zlepšit stávající obsah v souvislosti s ochranou údajů, a to co do jasnosti i do soudržnosti.

II. VYJASNĚNÍ POJMU SLEDOVATELNOST A ANONYMITA

Použitelnost směrnice 95/46/ES

11. Podle čl. 2 písm. a) směrnice 95/46/ES o ochraně osobních údajů se pod pojmem „osobní údaje“ rozumí: „veškeré informace o identifikované nebo identifikovatelné osobě; identifikovatelnou osobou se rozumí osoba, kterou lze přímo či nepřímo identifikovat, zejména s odkazem na identifikační číslo nebo na jeden či více zvláštních prvků její fyzické, fyziologické, psychické, ekonomické, kulturní nebo sociální identity“.

12. Biologický materiál lidského původu, jako jsou orgány, tkáně, buňky nebo krev, je možné definovat jako materiál, který je možné získat z lidského těla. Je sporné, zda je možné tento materiál jako takový považovat za osobní údaje. Tento materiál však může být nesporně použit jako *zdroj* osobních informací o jeho původci. Biologický materiál se často zpracovává právě kvůli získání těchto informací. A i když to není účelem, bývají k biologickému materiálu takto získané informace přiloženy. V takovýchto situacích platí pravidla směrnice 95/46/ES ([4]). To znamená, pokud je původce biologického materiálu *identifikovaná* nebo *identifikovatelná* (fyzická) osoba.

13. Jak určit, zda je osoba identifikovatelná, se vysvětluje ve 26. bodě odůvodnění směrnice 95/46/ES: „je třeba brát v úvahu všechny prostředky, které mohou být rozumně použity jak správcem, tak jakoukoli jinou osobou pro identifikaci dané osoby“. V tomtéž bodě odůvodnění se dále vysvětluje, že pravidla stanovená ve směrnici 95/46/ES neplatí, jestliže se informace týkají osoby, která není nebo již není identifikovatelná: takové údaje se považují za *anonymní*.

14. V doporučení (2006) 4 se Rada Evropy zabývá konkrétní otázkou identifikovatelnosti biologického materiálu, přičemž se rozlišuje mezi identifikovatelným a neidentifikovatelným materiálem ([5]).

15. Podle uvedeného doporučení je *identifikovatelný biologický materiál* „takový biologický materiál, který sám nebo spolu s doprovodnými údaji umožňuje identifikaci příslušných osob, a to buď přímou, nebo za použití kódu“ ([6]). V případě druhé možnosti nemá mít uživatel biologického materiálu přístup ani ke kódu („kódovanému materiálu“), ani ke kódu, který je ve správě třetí strany („související anonymizovaný materiál“). Pracovní skupina článku 29 ve stanovisku 4/2007 o pojetí osobních údajů (dále jen „pracovní skupina podle článku 29“) používá pojem *vysledovatelné pseudonymizované údaje*, kterým označuje nepřímo identifikovatelné informace o jednotlivcích, které je ještě možné za předem stanovených podmínek použít ke

([1]) Tento rámec tvoří směrnice 2002/98/ES, 2004/33/ES, 2005/61/ES a 2005/62/ES, pokud jde o krev a krevní deriváty, a směrnice 2004/23/ES, 2006/17/ES a 2006/86/ES, pokud jde o lidské tkáně a buňky.

([2]) Viz rovněž návrh směrnice Evropského parlamentu a Rady o uplatňování práv pacientů v přeshraniční zdravotní péči, KOM(2008) 414 v konečném znění.

([3]) Stanovisko evropského inspektora ochrany údajů ze dne 2. prosince 2008 k návrhu směrnice o uplatňování práv pacientů v přeshraniční zdravotní péči.

([4]) Pracovní skupina pro ochranu údajů zřízená podle článku 29, stanovisko 4/2007 o pojetí osobních údajů, s. 9.

([5]) Doporučení výboru ministrů členským státům Rec(2006) 4 k výzkumu biologického materiálu lidského původu.

([6]) Čl. 3 písm. i) doporučení Rec(2006) 4.

zpětnému vyhledávání a k identifikaci jednotlivců ([1]). Jako příklad toho, kdy jsou osobní údaje vyjádřeny kódem, přičemž klíč, který v sobě skrývá vztah mezi kódem a společnými identifikátory jednotlivce, se uchovává odděleně, se uvádějí *údaje kódované s využitím klíče*. Jestliže jsou použité kódy pro každou konkrétní osobu jedinečné, je možná identifikace pomocí kódovacího klíče.

16. Doporučení se vztahuje rovněž na *neidentifikovatelný biologický materiál* (neboli *„nesouvisející anonymizovaný biologický materiál“*), jakožto na „takový biologický materiál, který sám nebo spolu s doprovodnými údaji za přiměřeného úsilí neumožňuje identifikaci dotyčných osob“ ([2]). Takový materiál se bude považovat za anonymní údaj podle směrnice 95/46/ES.

17. Z uvedeného vyplývá, že se směrnice 95/46/ES vztahuje na sběr, skladování a zpracovávání identifikovatelných orgánů a na následné získávání informací z těchto orgánů, dokud trvá možnost identifikace osoby za pomoci všech prostředků, které mohou být rozumně použity. Jak se ukáže, stálá sledovatelnost orgánů, jak se předpokládá v navrhované směrnici, zachová možnost identifikace osob v průběhu celého procesu.

Sledovatelnost versus anonymita lidských orgánů

18. Sledovatelností biologického materiálu se rozumí možnost zpětně dohledat původce materiálu a tak jej identifikovat. Jinými slovy, kdykoli je možná sledovatelnost původce biologického materiálu, ať již přímo nebo nepřímo, je možné jej považovat za identifikovatelný a opačně. Pojmy „sledovatelnost“ a „identifikovatelnost“ jsou tudíž spolu v zásadě pevně propojené. Sledovatelnost a anonymita údajů se naopak vylučují. Tyto pojmy jsou protichůdné. Je-li určitá informace skutečně anonymní, není možné jednotlivce identifikovat a zpětně dohledat.

19. Pokud jde o současný návrh, je sledovatelnost povinným požadavkem, který má být stanoven v rámci národních programů jakosti v jednotlivých členských státech, a to pro obě strany, jak pro dárce, tak i pro příjemce. To znamená, že informace o orgánech jsou identifikovatelné, zatímco informace o dárcích a příjemcích jsou důvěrné. To je rovněž součástí definice sledovatelnosti v článku 3 návrhu: „schopnost příslušného orgánu lokalizovat a identifikovat orgán v každé fázi postupu od darování po transplantaci nebo likvidaci, přičemž tento orgán je za okolností uvedených v této směrnici oprávněn identifikovat dárce a organizaci provádějící odběr, identifikovat příjemce v transplantačním centru, lokalizovat a identifikovat všechny příslušné jiné než osobní údaje týkající se produktů a materiálů přicházejících do styku s orgánem“.

20. Článek 10 návrhu o sledovatelnosti navíc v prvním odstavci stanoví: „Členské státy zajistí, aby všechny orgány odebrané a přidělené na jejich území mohly být vysledovány od dárce k příjemci a opačně, v zájmu zabezpečení zdraví dárců a příjemců.“ V odstavci 3 téhož článku se uvádí: „Členské státy zajistí, aby a) příslušné orgány nebo jiné subjekty podílející se na postupu od darování po transplantaci nebo likvidaci uchovávaly údaje potřebné k zajištění sledovatelnosti ve všech fázích postupu od darování po transplantaci nebo likvidaci, v souladu s národními programy jakosti; b) údaje požadované pro plnou sledovatelnost byly uchovávány po dobu nejméně 30 let od darování. Tyto údaje lze uchovávat v elektronické podobě.“

21. Ačkoli proces sledovatelnosti podléhá prováděcím opatřením (viz článek 25 návrhu), jeví se jako nejpravděpodobnější řešení režim nepřímé identifikace dárců a příjemců, který by se měl buď řídit podle směrnice 2004/23/ES ([3]) o tkáních a buňkách a podle evropského identifikačního kódu, nebo by s nimi aspoň měl být interoperabilní ([4]). V takovém případě se zpracování týkající se dárců a příjemců v kontextu návrhu týká souvisejícího

([1]) Pracovní skupina pro ochranu údajů zřízená podle článku 29, stanovisko 4/2007, s. 18.

([2]) Čl. 3 písm. ii) doporučení Rec(2006) 4.

([3]) Protože dárcové orgánů jsou velmi často i dárci tkání, je nutné sledovat a ohlásit jakékoli neočekávané nežádoucí reakce rovněž v systému vigilance pro tkáně, a proto se požaduje interoperabilita s metodou nepřímé identifikace využívané v tomto systému. Viz směrnice Evropského parlamentu a Rady 2004/23/ES ze dne 31. března 2004 o stanovení jakostních a bezpečnostních norem pro darování, odběr, vyšetřování, zpracování, konzervaci, skladování a distribuci lidských tkání a buněk, Úř. věst. L 102/48, 7.4.2004 a směrnice Komise 2006/86/ES ze dne 24. října 2006, kterou se provádí směrnice Evropského parlamentu a Rady 2004/23/ES, pokud jde o požadavky na sledovatelnost, oznamování závažných nežádoucích reakcí a účinků a některé technické požadavky na kódování, zpracování, konzervaci, skladování a distribuci lidských tkání a buněk, Úř. věst. L 294/32, 25.10.2006.

([4]) Součástí tohoto kódu je jedinečné identifikační číslo každého darování, s jehož pomocí a za pomoci tkáňového zařízení a identifikací přípravku lze zpětně dohledat dárce a příjemce. Konkrétněji, podle článku 10 směrnice 2006/86/ES „veškerým darovaným materiálům se v tkáňovém zařízení přidělí jedinečný evropský identifikační kód, aby se zajistila řádná identifikace dárce a sledovatelnost všech darovaných materiálů a zajistily informace o hlavních charakteristikách a vlastnostech tkání a buněk“. Jak bylo popsáno v příloze VII uvedené směrnice, má tento kód dvě části: a) identifikaci darování včetně jedinečného identifikačního čísla a identifikace tkáňového zařízení a b) identifikaci přípravku včetně kódu přípravku, číslo frakce a data ukončení doby použitelnosti.

anonymizovaného biologického materiálů nebo, použijeme-li terminologii z oblasti ochrany údajů, vysledovatelných pseudonymizovaných údajů (viz výše uvedený bod 15), k nimž se vztahují ustanovení směrnice 95/46/ES.

22. Je však třeba poukázat na to, že navzdory jasným požadavkům na sledovatelnost a identifikovatelnost se v některých částech návrhu v souvislosti s údaji o dárcích a příjemcích používá pojem „anonymita" nebo „anonymní údaje". Toto je, jak vyplývá z předchozích bodů, neslučitelné a nesmírně matoucí ([1]).

23. Přesněji řečeno, v čl. 10 odst. 2 návrhu, který stanoví nezbytnost identifikačního systému dárců, se uvádí: „Členské státy zajistí provádění identifikačního systému dárců, jehož prostřednictvím lze identifikovat každé darování a každý s tím spojený orgán. Členské státy zajistí, aby tento identifikační systém dárců byl navrhován v souladu s cílem nesbírat, nezpracovávat ani nevyužívat žádné osobní údaje nebo co nejméně osobních údajů. Využije se zejména možnosti použít pseudonym nebo neuvádět jména jedinců.". ([2]) Evropský inspektor ochrany údajů je toho názoru, že podtržená slova v tomto odstavci jsou v rozporu s pojmem sledovatelnost, protože není možné mít sledovatelné a identifikovatelné údaje, pokud jsou dárci a příjemci anonymizováni. Kromě toho stojí za povšimnutí, že se tento odstavec vztahuje k identifikaci dárců, přičemž identifikace příjemců (která je rovněž součástí procesu) není zmíněna vůbec.

24. Výše uvedený rozpor je ještě zjevnější v článku 17 o anonymizaci dárců a příjemců, ve kterém se uvádí: „Členské státy přijmou veškerá nezbytná opatření, aby zajistily anonymizaci všech osobních údajů dárců a příjemců zpracovávaných v rámci oblasti působnosti této směrnice, tak aby nemohla být zjištěna totožnost ani dárce ani příjemce". Tento článek je v naprostém rozporu s články návrhu věnovanými sledovatelnosti.

Důvěrnost místo anonymity

25. Evropský inspektor ochrany údajů se domnívá, že pojem anonymita se zřejmě používá ke zdůraznění potřeby větší *důvěrnosti* ([3]) údajů dárců a příjemců, což znamená, že informace jsou dostupné pouze osobám oprávněným k přístupu. Evropský inspektor ochrany údajů předpokládá, že se anonymizace konkrétněji využívá tak, aby implikovala nepřímé identifikační schéma používané pro dárce a příjemce ([4]), což může být rovněž matoucí vzhledem k tomu, jakým způsobem je tento pojem používán ve směrnici 2004/23/ES o tkáních a buňkách. Jak již bylo uvedeno dříve, anonymita tady není pro tento účel vyhovující pojem.

26. Jako příklad toho, jak je možné v procesu transplantace přistupovat k ochraně údajů i ke sledovatelnosti, je možné nalézt v dodatkovém protokolu k Úmluvě o lidských právech a biomedicíně Rady Evropy ([5]). Tady se místo pojmu anonymita používá pojem důvěrnost. Konkrétněji se v čl. 23 odst. 1 tohoto protokolu uvádí, že „veškeré osobní údaje týkající se osoby, které byly orgány nebo tkáně odebrány, a údaje týkající se příjemce se považují za důvěrné. Tyto údaje je možné sbírat, zpracovávat a sdělovat pouze v souladu s pravidly o profesní důvěrnosti a ochraně osobních údajů." Odstavec 2 téhož článku pokračuje takto: „ustanovení odstavce 1 se interpretuje, aniž jsou dotčena ustanovení umožňující, s výhradou vhodných ochranných opatření, sběr, zpracovávání a sdělování nutných informací o osobě, jíž byly orgány nebo tkáně odebrány, nebo o příjemci či příjemcích orgánů a tkání, pokud je to nutné z lékařského hlediska, včetně sledovatelnosti, jak je stanoveno v článku 3 tohoto protokolu."

27. Na základě uvedených skutečností evropský inspektor ochrany údajů doporučuje změnit znění určitých částí návrhu s cílem vyhnout se nejednoznačnosti a výslovně zohlednit skutečnost, že údaje nejsou anonymní, ale že by se při jejich zpracování měla uplatňovat přísná pravidla důvěrnosti a bezpečnosti. Konkrétně navrhuje evropský inspektor ochrany údajů tyto změny:

([1]) Tato připomínka se objevila již v poznámkách evropského inspektora ochrany údajů ze dne 19. září 2006 o veřejné konzultaci o budoucích opatřeních EU v oblasti dárcovství orgánů a transplantací.

([2]) Podtržení doplněno.

([3]) Zajištění toho, aby k informacím měly přístup pouze oprávněné osoby (definice ISO, zdroj: http://www.wikipedia.org).

([4]) Pojem „anonymizace" se někdy v závislosti na tom, v jakém kontextu se používá, vztahuje k nepřímému naznačení identifikovatelných údajů, jak je tomu v případě statistik. To však není z hlediska ochrany údajů správné, jak už vysvětlil evropský inspektor ochrany údajů ve stanovisku k návrhu nařízení Evropského parlamentu a Rady o statistice Společenství v oblasti veřejného zdraví a bezpečnosti a ochrany zdraví při práci (KOM(2007) 46 v konečném znění) a k návrhu nařízení Evropského parlamentu a Rady o evropské statistice (KOM(2007) 625 v konečném znění).

([5]) Rada Evropy, Dodatkový protokol k Úmluvě o lidských právech a biomedicíně o transplantacích orgánů a tkání lidského původu, Štrasburk 24. 1. 2002, ratifikační listina viz http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=186&CM=8&DF=2/13/2009&CL=ENG. Viz také: Rada Evropy, Úmluva na ochranu lidských práv a důstojnosti lidské bytosti v souvislosti s aplikací biologie a medicíny: Úmluva o lidských právech a biomedicíně, Oviedo, 4. dubna 1997, ratifikační listina viz http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=164&CM=8&DF=2/13/2009&CL=ENG

— V 16. bodě odůvodnění, poslední věta: „V souladu s uvedenou listinou a případně s přihlédnutím k Úmluvě o lidských právech a biomedicíně by měly být programy pro transplantaci orgánů založeny na zásadách dobrovolného a bezplatného darování, altruismu dárce a solidarity mezi dárcem a příjemcem a současně by se mělo zajistit zavedení přísných pravidel důvěrnosti a bezpečnostních opatření za účelem ochrany osobních údajů dárců a příjemců.“,

— V čl. 10 odst. 2: „Členské státy zajistí provádění identifikačního systému dárců a příjemců, jehož prostřednictvím lze identifikovat každé darování a každý s tím spojený orgán. Členské státy zajistí, aby tento identifikační systém dárců a příjemců byl navrhován a vybírán v souladu s cílem sbírat, zpracovávat a využívat co nejméně osobních údajů, přičemž se využijí zejména metody používání pseudonymů a zavedou se rovněž i nutná technická a organizační opatření za účelem bezpečnosti těchto údajů“,

— Článek 17 jako takový by mohl být vypuštěn a jeho obsah (pokud jde o potřebu důvěrnosti) by se začlenil do nového odstavce článku 16 o ochraně osobních údajů, důvěrnosti a bezpečnosti zpracování (viz níže uvedený bod 36).

28. Evropský inspektor ochrany údajů navíc navrhuje dále se zabývat potřebou *zvýšené ochrany* údajů o dárcích a příjemcích prostřednictvím využití *přísných bezpečnostních opatření* na vnitrostátní i na přeshraniční úrovni; jeho návrhu jsou věnovány následující části tohoto stanoviska.

III. **Důraz na vnitrostátní opatření v oblasti bezpečnosti údajů**

Základní potřeby a požadavky v oblasti bezpečnosti

29. Jak vyplývá z návrhu, zpracování osobních údajů týkajících se dárců a příjemců se uskutečňuje hlavně na vnitrostátní úrovni, tj. ve střediscích členských států, kde dochází k odběru a k transplantaci. Právě na této úrovni se také vede registr živých dárců. Ačkoli dosud nebyly definovány mechanismy sledovatelnosti, je možné očekávat, že se nějaká aktivita v oblasti kodifikace objeví i na vnitrostátní úrovni, a to i v případě, že se používá evropský systém kódování, protože identifikace dárců a příjemců je možná pouze prostřednictvím příslušných vnitrostátních orgánů.

30. Nesmírně důležité je provádět politiku v oblasti bezpečnosti informací založenou na *přísných a rozumných bezpečnostních opatřeních* na úrovni příslušných vnitrostátních služeb, zejména s cílem vyhovět požadavkům na důvěrnost v případě dárců a příjemců uvedeným v návrhu a zabezpečit *integritu* ([1]), *vymezení odpovědnosti* ([2]) a *dostupnost* ([3]) těchto údajů. V tomto ohledu by měla politika v oblasti bezpečnosti informací zahrnovat rovněž prvky fyzické a logické bezpečnosti zaměřené mimo jiné i na kontrolu vkládání, zaznamenávání, předávání a sdělování údajů a na přístup k nim, jakož i na nosiče údajů a kontrolu jejich uchovávání.

31. Pokud jde o důvěrnost, mohou lékařské údaje o příjemcích ([4]) i údaje používané pro charakteristiku a ověřování dárců (rovněž ve vztahu k „širší skupině dárců“ ([5])) odhalovat o těchto osobách citlivé osobní informace, které mohou ovlivnit rovněž jejich sociální, profesionální a osobní život. Dále je velmi důležitá ochrana údajů pro identifikaci dárců, protože by se žijící dárcové nebo osoby, které daly souhlas s tím, že po smrti darují jeden či více svých orgánů, mohly stát oběťmi obchodování s lidskými orgány a tkáněmi, pokud by tato skutečnost vyšla najevo. Integrita údajů týkajících se orgánů je rovněž velmi zásadní, protože i sebemenší chyba v předávaných informacích může příjemce ohrozit na životě. Totéž platí i o přesnosti údajů o zdravotním stavu dárců před transplantací, protože na základě těchto údajů se zjišťuje, zda je příslušný orgán vhodný či nikoli. Pokud jde o vymezení odpovědnosti, jelikož je do celkového schématu dárcovství a transplantací zahrnuto mnoho různých organizací, měl by existovat způsob, jak by si všechny subjekty byly vědomy odpovědnosti za své aktivity a dokázaly za ně přijmout odpovědnost, například v případě, kdy se údaje pro identifikaci dárců dostanou do rukou neoprávněných osob, nebo kdy nejsou lékařské údaje týkající se orgánů

([1]) Zajištění „celistvosti“ neboli úplnosti údajů, tj. stavu, v němž se s údaji během jakékoli operace (jako je předávání, uchovávání nebo vyhledávání) manipuluje jednotným způsobem, zajištění uchovávání údajů k jejich zamýšlenému využití nebo, pokud jde o konkrétní operace, *a priori* předpokladu kvality údajů. Jednoduše řečeno, integrita údajů je zajištění toho, aby údaje byly konzistentní a správné (zdroj: http://www.wikipedia.org); zajištění toho, aby byl k informacím přístup a mohly být měněny pouze na základě pověření (zdroj: http://searchdatacenter.techtarget.com).

([2]) Závazek odpovědnosti za vlastní jednání; nepopiratelnost: zajištění toho, aby byly údaje posílány stranami, které byly požádány o jejich zaslání, a aby je obdržely strany, které o ně požádaly: zajištění toho, aby strana sporu nemohla popřít nebo vyvrátit platnost nějakého tvrzení (zdroj: http://www.wikipedia.org).

([3]) Míra okamžité dostupnosti údajů (zdroj: http://www.pcmag.com).

([4]) Je třeba poznamenat, že pouhá skutečnost, že byl příjemci transplantován nějaký orgán, představuje citlivý osobní údaj o zdraví tohoto člověka.

([5]) Potenciální dárci, kteří nejsou ideálními kandidáty dárcovství, ale je možné o nich za určitých okolností uvažovat, např. v případě starších příjemců. Viz: Pracovní dokument útvarů Komise k návrhu směrnice Evropského parlamentu a Rady o jakostních a bezpečnostních normách pro lidské orgány určené k transplantaci a ke sdělení Komise – Akční plán pro dárcovství a transplantaci orgánů (2009 až 2015): posílená spolupráce mezi členskými státy, posouzení dopadu, 8.12.2008.

přesné. V neposlední řadě, jelikož je celý systém založen na předávání údajů týkajících se orgánů a na mechanismu sledovatelnosti od dárce k příjemci, měly by tyto údaje být v případě potřeby bez prodlení k dispozici oprávněným osobám (jinak by nedostupnost poškozovala bezproblémové fungování systému).

32. V tomto ohledu by měly být zavedeny příslušné *mechanismy udílení oprávnění*, které by navazovaly na konkrétní *politiky v oblasti kontroly přístupu*, a to jak u vnitrostátních databází, tak i v případě přeshraničních výměn orgánů. Tyto politiky by měly být nejprve definovány v organizační rovině, zejména pokud jde o přesné identifikační postupy u dárců i příjemců (například kdo má přístup k jakým informacím a za jakých okolností). Tímto způsobem budou stanovena *práva přístupu* spolu se *scénáři přístupu*, kdy lze tato práva uplatňovat (např. okolnosti a postup pro zpřístupňování údajů organizací provádějící odběr příslušnému orgánu, určité případy, kdy je třeba příjemci zpřístupnit identitu dárce, pokud takové situace nastanou, a postupy, jak to provést, atd.). Aby tyto politiky byly účinné, měla by se na osoby provádějící zpracování vztahovat zvláštní *pravidla důvěrnosti*.

33. Jakmile budou tyto politiky stanoveny, mohou se provádět na technické úrovni, tj. pokud jde o kontrolu přístupu uživatele do systému a o žádosti na základě předem definovaných přístupových práv. K tomu je možné využívat vyzkoušené technologie jako *šifrování* a *digitální certifikáty* ([1]) (např. založené na *schématech infrastruktury veřejných klíčů*) ([2]). K omezení přístupových práv uživatele na základě úlohy v procesu lze využít rovněž *ověřovací mechanismy založené na úlohách* (např. možnost měnit lékařské údaje příjemců a dárců ve vnitrostátních databázích by měli mít pouze lékaři).

34. Kontrola přístupu by měla být doplněna o možnost *zaznamenávání* činnosti uživatelů (např. přístup k lékařským údajům pro čtení a psaní), zejména pokud se používají elektronické systémy. Měla by se rovněž zavést fyzická a logická bezpečnostní opatření, aby se zajistilo *plné fungování* databází dárců a orgánů jakožto ústřední prvek navrhovaného systému v oblasti dárcovství a transplantací. Za základní kámen systému by se měla považovat dostupnost údajů. V tomto ohledu by měla politika v oblasti bezpečnosti informací vycházet z řádné *analýzy a posouzení rizika* a měla by rovněž zahrnovat prvky, jako jsou mimořádné události a řízení kontinuity provozu. Všechny tyto prvky by se měly udržovat a zlepšovat za pomoci pravidelného procesu monitorování a přezkumu. Účinnost a systém mohou zlepšit rovněž *nezávislé audity*, při nichž by se věnovala zvláštní pozornost používání pseudonymů, sledovatelnosti a postupům při předávání údajů.

([1]) Elektronická obdoba občanského průkazu, která identifikuje původce digitálního podpisu (zdroj: http://www.ffiec.gov/ffiecinfobase/booklets/e_banking/ebanking_04_appx_b_glossary.html).

([2]) Infrastruktura veřejných klíčů (PKI) zahrnuje hardware, software, lidi, politiky a postupy nutné k vytvoření, řízení, skladování, distribuci a odnímání digitálních certifikátů (zdroj: http://www.wikipedia.org).

35. Evropský inspektor ochrany údajů by byl rád, kdyby se v kontextu navrhované směrnice kladl větší důraz na potřebu takových opatření.

Zlepšení ustanovení o bezpečnosti v uvedeném návrhu

36. V článku 16 návrhu věnovanému ochraně osobních údajů, důvěrnosti a bezpečnosti zpracování se uvádí: „Členské státy zajistí plné a účinné dodržování základního práva na ochranu osobních údajů při všech činnostech souvisejících s transplantací orgánů v souladu s předpisy Společenství o ochraně osobních údajů, jako je směrnice 95/46/ES a zejména čl. 8 odst. 3, články 16, 17 a čl. 28 odst. 2 uvedené směrnice.“ Evropský inspektor ochrany údajů doporučuje, aby byl k tomuto článku doplněn ještě *druhý odstavec*, v němž by se popisovaly základní zásady zajišťování bezpečnosti na úrovni členských států, včetně minimálního odkazu na tyto body:

— Měla by se zavést politika v oblasti bezpečnosti informací uplatňující technická a organizační opatření k zajištění důvěrnosti, integrity, vymezení odpovědnosti a dostupnosti osobních údajů dárců a příjemců,

— Měla by se definovat konkrétní politika v oblasti důvěrnosti a kontroly přístupu, která by se používala ve všech členských státech a v průběhu celého řetězce sledovatelnosti by upřesňovala přístupová práva, úlohy a povinnosti všech zúčastněných stran (dárce, organizace provádějící odběr, transplantačního centra, příjemce, příslušného vnitrostátního orgánu, příslušného přeshraničního orgánu). Pro osoby provádějící zpracovávání údajů, zejména pokud se na tyto osoby nevztahuje povinnost zachování lékařského tajemství (např. kodexy chování v oblasti důvěrnosti a opatření zaměřená na informovanost) by se měly zavést konkrétní záruky důvěrnosti údajů,

— Měla by se zdůraznit potřeba zaměřit se na bezpečnostní mechanismy (jako například šifrování a digitální certifikáty). Zejména pokud jde o registry dárců, měla by se uplatňovat zásada „soukromí coby aspektu návrhu“, aby se do počátečních fází tohoto rozvoje zahrnuly všechny potřebné požadavky v oblasti bezpečnosti,

— Je třeba rovněž stanovit postupy pro zajištění práv na ochranu údajů dárců a příjemců, zejména práv na přístup a opravu, jakož i práva na informace. Zvláštní pozornost bude rovněž věnována případům dárců, kteří by svůj souhlas chtěli zrušit nebo nebyli jako dárci přijati (po charakterizaci dárce a orgánu). V takovém případě je třeba definovat konkrétní postup a lhůtu pro uchovávání jejich údajů,

— Politika v oblasti bezpečnosti informací by tedy měla zahrnovat opatření zaměřená na zajištění integrity a nepřetržité dostupnosti údajů. Úlohu posouzení rizika v oblasti bezpečnosti informací je třeba doplnit o prvky týkající se mimořádných událostí a rozšířit ji o řízení kontinuity provozu,

— Politiky v oblasti bezpečnosti informací by se měly pravidelně monitorovat a přezkoumávat, a to i prostřednictvím nezávislých auditů.

37. Evropský inspektor ochrany údajů doporučuje, aby se výše uvedené prvky začlenily do článku 16 a pak aby se dále upřesnily v rámci prováděcích opatření článku 25, zejména odst. 1 písm. a), b) a c).

IV. **OCHRANNÁ OPATŘENÍ VZTAHUJÍCÍ SE K PŘESHRANIČNÍM VÝMĚNÁM ORGÁNŮ**

Harmonizace bezpečnosti v členských státech

38. Přeshraniční výměna orgánů bude v praxi vždy zahrnovat zpracování osobních údajů, protože orgány (i když se použije kódování) zůstávají prostřednictvím příslušných vnitrostátních orgánů (nepřímo) identifikovatelné.

39. Evropský inspektor ochrany údajů již vyjádřil své stanovisko ohledně potřeb v oblasti bezpečnosti, pokud jde o ochranu osobních údajů v přeshraniční zdravotní péči v rámci Evropy, v němž zdůraznil mimo jiné potřebu harmonizace politik v oblasti bezpečnosti informací mezi členskými státy, aby tak bylo dosaženo rozumné úrovně ochrany údajů ([1]). Doporučil, aby byl tento prvek uveden rovněž v současném návrhu, konkrétněji v 17. bodě odůvodnění, ve kterém je zmíněno ustanovení směrnice 95/46/ES o bezpečnosti zpracování.

Zavedení systému sledovatelnosti

40. V tomto konkrétním případě je významným parametrem pro zajištění bezpečnosti přeshraniční výměny údajů mechanismus sledovatelnosti, který má být zaveden. Za tímto účelem je třeba kromě bezpečnostních opatření uplatňovaných na úrovni členských států věnovat zvláštní pozornost možnostem používání pseudonymů k identifikaci dárců a příjemců (např. typu kodifikace, možnosti dvojí kodifikace atd.) a zachování interoperability se systémy identifikace tkáně a buněk.

41. Evropský inspektor ochrany údajů doporučuje, aby byl k tomuto bodu uveden konkrétní odkaz v článku 25 navrhované směrnice věnovaném prováděcím opatřením, tím že by se změnil odst. 1 písm. b) takto: „postupy pro zajištění plné sledovatelnosti orgánů, včetně požadavků na označování, při současném zajištění důvěrného charakteru dárců a příjemců v průběhu celého procesu sledovatelnosti a zachování interoperability se systémem identifikace tkání a buněk."

Výměna orgánů se třetími zeměmi

42. Ještě důležitější jsou potřeby v oblasti bezpečnosti při výměně údajů se třetími zeměmi, kde není pokaždé možné zaručit odpovídající úroveň ochrany údajů. Zvláštní režim pro předávání osobních údajů třetím zemím je stanoven v článcích 25 a 26 směrnice 95/46/ES. Evropský inspektor ochrany údajů si je vědom skutečnosti, že požadavky na ochranu údajů by neměly bránit rychlému a účelnému předávání orgánů, což je v rámci systému dárcovství orgánů nutné a někdy to může být dokonce otázka života a smrti. Měly by se tedy prověřit možnosti předávání navzdory nedostatečnému zajištění odpovídající úrovně ochrany údajů ve třetích zemích obecně. Je třeba mít na paměti, že vzhledem k nepřímé povaze identifikace jednotlivců na přeshraniční úrovni a vzhledem ke skutečnosti, že nad systémem vykonávají celkový dohled příslušné vnitrostátní orgány, hrozí s největší pravděpodobností menší rizika než na vnitrostátní úrovni ([2]).

43. Proto je evropský inspektor ochrany údajů toho názoru, že příslušný orgán, který je odpovědný za povolení těchto předávání, by měl konzultovat vnitrostátní orgán pro ochranu údajů, aby s ohledem na možná omezení uvedená v článku 26 směrnice 95/46/ES vypracoval potřebný rámec pro bezpečné, ale zároveň i rychlé a účelné předávání údajů o orgánech do třetích zemí a ze třetích zemí. Evropský inspektor ochrany údajů doporučuje, aby byl odkaz na tento bod uveden v článku 21 věnovaném výměně orgánů se třetími zeměmi nebo v příslušném 15. bodě odůvodnění.

Prováděcí opatření

44. Na závěr evropský inspektor ochrany údajů naléhavě vyzývá zákonodárce, aby s ohledem na článek 25 ve všech případech, kdy se jedná o prováděcí opatření mající vliv na ochranu a bezpečnost údajů, zajistil, aby byly konzultovány všechny příslušné zúčastněné strany včetně evropského inspektora ochrany údajů a pracovní skupiny podle článku 29.

V. **ZÁVĚRY**

45. Evropský inspektor ochrany údajů vzal na vědomí iniciativu v oblasti zajištění vysokých jakostních a bezpečnostních norem pro lidské orgány určené k transplantaci, kterou je možné považovat za součást celkového přístupu ES ke stanovení společných norem na podporu přeshraniční dostupnosti služeb zdravotní péče v Evropě.

46. Tento návrh již uvážil potřeby dárců a příjemců orgánů v oblasti ochrany údajů, zejména požadavek na zachování důvěrnosti, pokud jde o jejich totožnost. Evropský inspektor ochrany údajů však vyslovuje politování nad tím, že některé z těchto ustanovení jsou vágní, nejednoznačná nebo obecná, a z toho důvodu doporučuje řadu změn, aby se zlepšil současný obsah návrhu, pokud jde o ochranu údajů.

([1]) Stanovisko evropského inspektora ochrany údajů ze dne 2. prosince 2008 k návrhu směrnice o uplatňování práv pacientů v přeshraniční zdravotní péči.

([2]) Viz stanovisko 7/2007 Pracovní skupiny pro ochranu údajů zřízené podle článku 29, s. 18, o pseudonymizovaných a kódovaných údajích.

47. Evropský inspektor ochrany údajů v prvé řadě upozorňuje na stávající rozpor mezi pojmy sledovatelnost a anonymita používanými v uvedeném návrhu. S ohledem na to doporučuje konkrétní změny formulací určitých částí návrhu (zejména v 16. bodě odůvodnění, čl. 10 odst. 2 a v článku 17) s cílem vyhnout se nejednoznačnosti a výslovně zohlednit skutečnost, že údaje nejsou anonymní, ale že by se při jejich zpracování měla uplatňovat přísná pravidla důvěrnosti a bezpečnosti.

48. Navíc doporučuje, aby se více zdůraznila potřeba přijmout výrazná bezpečnostní opatření na vnitrostátní úrovni. Za tímto účelem by bylo možné doplnit v článku 16 druhý odstavec, v němž by byly popsány základní zásady pro zajištění bezpečnosti na úrovni členských států, a dále upřesnit tyto zásady jako součást prováděcích opatření čl. 25 odst. 1. K navrhovaným zásadám bezpečnosti patří:

a) přijetí politiky v oblasti bezpečnosti s cílem zajistit důvěrnost, integritu, vymezení odpovědnosti a dostupnost osobních údajů o dárcích a příjemcích;

b) definování konkrétní politiky v oblasti důvěrnosti a kontroly přístupu spolu se zárukami důvěrnosti údajů u osob zapojených do zpracování údajů;

c) zaměření se na bezpečnostní mechanismy ve vnitrostátních databázích na základě zásady „soukromí coby aspektu návrhu“;

d) stanovení postupů, s jejichž pomocí by dárcům a příjemcům byla zaručena práva v oblasti ochrany údajů, zejména právo na přístup a opravu a právo na informace, přičemž by se zvláštní pozornost věnovala případům dárců, kteří by svůj souhlas chtěli zrušit, nebo nebyli jako dárci přijati;

e) stanovení opatření, s jejichž pomocí by byla zajištěna integrita a nepřetržitá dostupnost údajů;

f) zajištění pravidelného monitorování a nezávislých auditů bezpečnostních politik přímo na místě.

49. Pokud jde o přeshraniční výměnu orgánů, evropský inspektor ochrany údajů doporučuje, aby byla v 17. bodě odůvodnění uvedena potřeba harmonizace politik členských států v oblasti bezpečnosti informací. Navíc by se měla zvláštní pozornost věnovat možnostem používání pseudonymů pro identifikaci dárců a příjemců a zachování interoperability se systémem identifikace tkání a buněk. Evropský inspektor ochrany údajů doporučuje, aby byl na tento bod zvláštní odkaz v čl. 25 odst. 1 písm. b) návrhu.

50. Ohledně výměny orgánů se třetími zeměmi evropský inspektor ochrany údajů doporučuje, aby bylo v článku 21 nebo v příslušném 15. bodě odůvodnění návrhu uvedeno, že příslušný orgán bude konzultovat vnitrostátní orgán pro ochranu údajů za účelem vytvoření nezbytného rámce pro bezpečné, ale i rychlé a účelné předávání údajů o orgánech třetím zemím a ze třetích zemí.

51. V neposlední řadě evropský inspektor ochrany údajů doporučuje, aby ve všech případech, kdy se provádějí opatření mající vliv na ochranu a bezpečnost údajů, byly konzultovány všechny příslušné zúčastněné strany včetně evropského inspektora ochrany údajů a pracovní skupiny podle článku 29.

V Bruselu dne 5. března 2009.

Peter HUSTINX

evropský inspektor na ochranu údajů

Věstník Úřadu pro ochranu osobních údajů

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

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

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

ISSN 1213-3442