VĚSTNÍK
ÚŘADU PRO OCHRANU OSOBNÍCH ÚDAJŮ
2009

Částka 52 **25. června 2009** **Cena 60 Kč**

OBSAH

ÚVOD

Padesátá druhá částka Věstníku Úřadu pro ochranu osobních údajů přináší přehled zrušených registrací za období od 21. 2. 2009 do 10. 6. 2009.

Rubriku Stanoviska Úřadu naplňuje stanovisko č. 3/2009 „Biometrická identifikace nebo autentizace zaměstnanců". Záměrem stanoviska je vyjádřit základní přístupy Úřadu pro použití systémů umožňujících spolehlivé určení fyzické osoby na základě unikátních biometrických znaků.

V rubrice Sdělení Úřadu je publikován dokument Pracovní skupiny pro ochranu dat podle článku 29 (WP29), kterým je „Stanovisko č. 1/2009 k návrhům, kterými se mění směrnice 2002/58/ES o ochraně soukromí v elektronických komunikacích (směrnice o soukromí a elektronických komunikacích)". O závažnosti a aktuálnosti dokumentu vypovídá skutečnost, že v jeho závěru WP29 vyzývá evropské zákonodárce, aby mezi ostatními otázkami zdůrazněnými v tomto stanovisku zvážili také zpřísnění povinnosti oznámit, že došlo k narušení zabezpečení osobních údajů, vzhledem k zásadnímu dopadu takto vzniklé situace na ochranu osobních údajů všech evropských občanů. 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 materiál „Doporučení Komise ze dne 12. května 2009 o zavedení zásad ochrany soukromí a údajů v aplikacích podporovaných identifikací na základě rádiové frekvence". Identifikace na základě rádiové frekvence (RFID) předznamenává nový vývoj v informační společnosti, kdy se předměty vybavené mikroelektronikou, která může automaticky zpracovávat osobní údaje, budou stále více stávat nedílnou součástí každodenního života. Cílem tohoto doporučení je zejména zajistit respektování soukromého a rodinného života a ochrany osobních údajů. Jedná se také o překlad pořízený Evropskou komisí, o přetisk v původní podobě.

Přehled zrušených registrací

Číslo registrace	Subjekt	Datum zrušení
00000383/001	RENTEX AUTOPŮJČOVNA S.R.O.	24.2.2009
00001188/007	UNILEVER ČR, SPOL. S R.O.	19.5.2009
00001188/009	UNILEVER ČR, SPOL. S R.O.	19.5.2009
00001188/011	UNILEVER ČR, SPOL. S R.O.	19.5.2009
00001188/012	UNILEVER ČR, SPOL. S R.O.	19.5.2009
00001188/013	UNILEVER ČR, SPOL. S R.O.	19.5.2009
00001188/027	UNILEVER ČR, SPOL. S R.O.	19.5.2009
00001188/028	UNILEVER ČR, SPOL. S R.O.	19.5.2009
00001188/031	UNILEVER ČR, SPOL. S R.O.	19.5.2009
00001188/032	UNILEVER ČR, SPOL. S R.O.	24.3.2009
00001188/033	UNILEVER ČR, SPOL. S R.O.	24.3.2009
00001188/034	UNILEVER ČR, SPOL. S R.O.	24.3.2009
00001188/035	UNILEVER ČR, SPOL. S R.O.	19.5.2009
00001188/036	UNILEVER ČR, SPOL. S R.O.	19.5.2009
00001188/037	UNILEVER ČR, SPOL. S R.O.	19.5.2009
00001188/039	UNILEVER ČR, SPOL. S R.O.	19.5.2009
00001188/040	UNILEVER ČR, SPOL. S R.O.	19.5.2009
00001188/043	UNILEVER ČR, SPOL. S R.O.	19.5.2009
00004840/001	PIVOVARY STAROPRAMEN A.S.	27.2.2009
00004991/006	JIHOMORAVSKÁ PLYNÁRENSKÁ A.S.	11.4.2009
00004991/007	JIHOMORAVSKÁ PLYNÁRENSKÁ A.S.	11.4.2009
00004991/008	JIHOMORAVSKÁ PLYNÁRENSKÁ A.S.	11.4.2009
00004991/009	JIHOMORAVSKÁ PLYNÁRENSKÁ A.S.	11.4.2009
00004991/010	JIHOMORAVSKÁ PLYNÁRENSKÁ A.S.	11.4.2009
00004991/011	JIHOMORAVSKÁ PLYNÁRENSKÁ A.S.	11.4.2009
00004991/012	JIHOMORAVSKÁ PLYNÁRENSKÁ A.S.	11.4.2009
00004991/013	JIHOMORAVSKÁ PLYNÁRENSKÁ A.S.	11.4.2009
00005009/008	STATUTÁRNÍ MĚSTO HAVÍŘOV	6.5.2009
00018031/001	MĚSTO BLANSKO	12.3.2009
00021608/001	PLZEŇSKÝ HOLDING A.S.	3.3.2009
00030385/001	KVĚTINOVÁ ZAHRADA S.R.O.	11.4.2009
00031317/001	BYTOVÉ DRUŽSTVO RENNESKÁ 29 A 31	2.6.2009
00032123/001	RADKA RACHOTOVÁ	29.5.2009
00033016/001	BIOFAKTORY PRAHA S.R.O.	5.6.2009

II. STANOVISKA ÚŘADU

Stanovisko č. 3/2009

květen 2009

Biometrická identifikace nebo autentizace zaměstnanců

Úvod

Záměrem stanoviska je vyjádřit základní přístupy Úřadu pro ochranu osobních údajů (dále jen „Úřad“) pro použití systémů umožňujících spolehlivé určení fyzické osoby na základě unikátních biometrických znaků, které se v poslední době velmi rozšířilo i v pracovněprávních vztazích. Nejčastěji je ze strany zaměstnavatele vznášen požadavek na poskytnutí otisků prstů (případně otisku dlaně) zaměstnanců pro použití v přístupových a docházkových systémech. Použití biometrických znaků má vyloučit možnosti klamání zaměstnavatele při použití jiných prostředků, např. identifikačních karet, v docházkových systémech. V přístupových systémech má otisk prstu zajistit spolehlivé určení osoby oprávněné pro přístup do chráněných prostor nebo k chráněným informacím.

Otiskem prstu se rozumí obraz papilárních linií prstu včetně charakteristických změn (markantů) zaznamenaný na vhodném nosiči a určený pro další použití. V systémech biometrické identifikace nebo autentizace se markanty digitálně vyhodnocují. Systémy se mohou lišit počtem případně i druhem používaných markantů. Otisk prstu je považován za prakticky unikátní. To zakládá možnost přímého ztotožnění nositele zobrazované biometrické charakteristiky. Tím otisk prstu naplňuje znaky citlivého biometrického údaje jako údaje umožňujícího přímou identifikaci nebo autentizaci subjektu údajů podle § 4 písm. b) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „zákon o ochraně osobních údajů“).

Jakkoliv Úřadu přísluší posuzovat pouze operace prováděné s osobními údaji ve smyslu definice zpracování osobních údajů podle § 4 písm. e) zákona o ochraně osobních údajů, je třeba konstatovat, že i jiný požadavek na poskytnutí otisku prstu, než je shromažďování osobních údajů ve smyslu § 4 písm. f) citovaného zákona, představuje zásah do osobní integrity fyzické osoby, o jehož oprávněnosti by v případě sporu musel rozhodovat soud.

Odůvodnění

Záměr zaměstnavatele na trvalé ukládání biometrických údajů, například samotných scanů či snímků otisků prstů, často zpracovávaných společně s dalšími identifikačními údaji zaměstnanců v informačním systému zaměstnavatele v podobě, která umožňuje tyto informace dále zpracovávat, je zpracováním citlivých údajů, které je možné **jen za podmínek stanovených § 9 zákona o ochraně osobních údajů**, tedy buď s výslovným souhlasem subjektu údajů podle § 9 písm. a), nebo bez tohoto souhlasu za podmínek dále tímto ustanovením stanovených.

Přístupové systémy

Pokud se jedná o možnosti využití výjimky v § 9 písm. b) až i) zákona o ochraně osobních údajů pro zpracovávání biometrických údajů zaměstnanců, dá se využít toto ustanovení jen velmi omezeně. Z hlediska zákona o ochraně osobních údajů jde v tomto případě zejména o zpracování citlivých údajů, které je nezbytné pro dodržení povinností a práv správce odpovědného za zpracování v oblasti pracovního práva a zaměstnanosti, stanovené zvláštním zákonem ve smyslu § 9 písm. d), a dále se může jednat o zpracování nezbytné pro zajištění a uplatnění právních nároků ve smyslu § 9 písm. h), když tato možnost vyplývá ze zvláštních právních předpisů.

Z hlediska objektové bezpečnosti stanoví použití biometrické identifikace výslovně pouze vyhláška č. 144/1997 Sb., o fyzické ochraně jaderných materiálů a jaderných zařízení a o jejich zařazování do jednotlivých kategorií, vydaná k provedení zákona č. 18/1997 Sb., o mírovém využívání jaderné energie a ionizujícího záření (atomový zákon) a o změně a doplnění některých zákonů. Tato vyhláška v § 8 odst. 2 stanoví: „Každý, kdo je oprávněn vstupovat do střeženého, chráněného a vnitřního prostoru, je vybaven identifikační kartou umožňující automatickou kontrolu a registraci vstupu. Pro kontrolu vstupu osob se minimálně při vstupu do střeženého prostoru zařízení s jaderně energetickými reaktory použije biometrické identifikace (např. geometrie ruky, otisk prstů). Počet osob vstupujících do těchto prostorů se omezuje na nezbytně nutný počet. Aktuální databáze vstupů je dostupná jeden měsíc a zajišťuje se její archivace jeden rok.“

Použití systémů využívajících biometrických znaků, které však nemusejí být založeny na vyhledávání biometrických údajů v databázi za tímto účelem vytvořené, tedy zpracování citlivých údajů ve smyslu zákona o ochraně osobních údajů, může být důvodné i v jiných případech souvisejících s pracovněprávními vztahy. Může jít zejména o přístupové systémy používané z hlediska fyzické bezpečnosti podle § 24 – 33 zákona č. 412/2005 Sb., o ochraně

utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, jako technického prostředku pro kontrolu vstupu ve smyslu § 30 odst. 1 písm. b) tohoto zákona. Podrobnosti upravují vyhlášky Národního bezpečnostního úřadu (NBÚ).

V praxi však u přístupových systémů, kde zajištění bezpečnosti zpracováním citlivých biometrických údajů není stanoveno zvláštním zákonem nebo spojeno se zvláštním zákonem předvídanou prováděcí vyhláškou, **lze biometrické identifikace s vyhledáváním biometrických údajů v databázi použít jen s výslovným souhlasem jejich nositele** podle § 9 písm. a) zákona o ochraně osobních údajů. Současně musejí být dodrženy všechny ostatní povinnosti správce podle zákona o ochraně osobních údajů, zejména § 10. V přístupových systémech by v návaznosti na uvedené mělo vždy platit pravidlo, že jde o mimořádné opatření kdy, kromě ze zvláštního zákona vyplývající povinnosti zajistit bezpečnost přístupu, se zpravidla zpracovávají biometrické údaje omezeného okruhu oprávněných osob, na rozdíl od plošného zpracování biometrických údajů všech zaměstnanců v docházkových systémech.

Docházkové systémy

Podle přístupu Úřadu k této problematice deklarovaného ve výroční zprávě za rok 2007 i v odpovědích na četné dotazy veřejnosti k této problematice nelze použití systémů, v jejichž paměti dochází k uchovávání biometrických údajů v podobě, která umožňuje jejich další zpracování, považovat za nezbytné pro jakoukoliv běžnou evidenci, např. pro evidenci docházky do zaměstnání. Zpracování biometrických údajů zejména v docházkových systémech lze proto posuzovat jako nepřiměřené ve vztahu k rozsahu a účelu zpracovávání, který je povinen stanovit každý správce. V důsledku toho může docházet k porušení povinnosti podle § 5 odst. 1 písm. d) zákona o ochraně osobních údajů, tedy shromažďování osobních údajů neodpovídajících stanovenému účelu a v rozsahu nikoli nezbytném pro naplnění stanoveného účelu, a to i v případě existence výslovného souhlasu subjektu údajů. Na takový postup zaměstnavatele lze podat Úřadu stížnost. Ani splnění oznamovací povinnosti správce podle § 16 problém zaměstnavatele neřeší, protože takové zpracování by nemohlo být ve smyslu § 17 odst. 2 povoleno. Obdobný přístup zaujímá většina úřadů na ochranu dat států Evropské unie.

Problematice zpracování biometrických dat se věnuje Pracovní dokument o biometrii, který 1. srpna 2003 přijala Pracovní skupina pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů zřízená v rámci Evropské komise podle článku 29 směrnice 95/46/ES Evropského parlamentu a Rady (Working Party – WP29).

Prvním podstatným hlediskem je, zda dochází k uchovávání úplných biometrických údajů, nebo zda systém vybírá z úplných biometrických údajů některé rysy specifické pro jednotlivce tak, aby vytvořil biometrickou šablonu, která je redukcí úplného biometrického obrazu.

Je žádoucí, aby šablony byly před uložením v systému zpracovávány matematickými operacemi (kódování, algoritmy nebo hash funkce) tak, aby nebyly volně čitelné nebo zpětně rekonstruovatelné.

Důležité přitom je, že různé systémy mají různé způsoby bezpečného převodu šablony otisku prstů do číselného vyjádření, které je uloženo v systému. Nelze proto říci, že určité takto získané číselné vyjádření je pro subjekt údajů ve všech systémech jednoznačné. Zpracování takovýchto číselných vyjádření šablon tedy nelze posuzovat jako zpracování biometrických údajů.

Jiná situace by ovšem nastala v případě, kdy by existoval pouze jediný způsob převodu, a tudíž by každý subjekt měl ve všech těchto systémech jedinou hodnotu.

Jestliže dojde např. při použití jednosměrného hashování k vytvoření číselného údaje, jehož zpětná rekonstrukce na biometrický údaj není možná, nelze již tento údaj považovat za biometrický a využití takového systému může být v určitých případech přípustné, a to při naplnění povinností správce podle § 5 odst. 1 a dále některé z podmínek § 5 odst. 2 písm. a), b) nebo e) zákona o ochraně osobních údajů i bez souhlasu subjektu údajů, protože nedochází k uchovávání citlivého údaje.

Pro další zpracování údajů o docházce do zaměstnání za účelem plnění práv a povinností vyplývajících z pracovněprávních vztahů je v tom případě **aplikovatelná i výjimka z oznamovací povinnosti podle § 18 odst. 1 písm. b) zákona o ochraně osobních údajů**. Další zpracování osobních údajů zaměstnance např. na základě osobního čísla zaměstnance již není zpracováním citlivých údajů. Podléhá proto ostatním povinnostem stanoveným zákonem o ochraně osobních údajů, se zákonem stanovenými výjimkami, ne však režimu § 9.

Dalším důležitým hlediskem je, zda je použitý systém založen na autentizaci (verifikaci) fyzické osoby, nebo na identifikaci subjektu údajů v databázi, v níž jsou uchovávány osobní údaje i dalších subjektů údajů. Autentizační (verifikační) systém pouze ověřuje totožnost fyzické osoby porovnáním údajů 1:1. Při identifikaci systém rozpoznává jednotlivce odlišením od ostatních osob, tedy výběrem jednoho z *n* možných případů.

Plné biometrické údaje nebo biometrické šablony tedy mohou být uchovávány buď pouze v paměti biometrického zařízení, nebo v centrální databázi, případně u některých systémů na optických nebo čipových kartách, které uživatelům umožňují nosit je při sobě jako identifikační prostředek.

Aplikace pro autentizaci (verifikaci) se často používají pro různé úkoly ve zcela odlišných oblastech a v odpověd-

nosti celé řady různých subjektů. Pro účely autentizace/verifikace není nezbytné uchovávat osobní údaje v databázi, postačuje je uchovávat decentralizovaně. Z hlediska zásady proporcionality jsou jednoznačně upřednostňovány biometrické aplikace, které nezpracovávají data získaná z tělesných stop nevědomě zanechaných jednotlivci a u kterých nejsou data uchovávána v centralizovaném systému.

Povinnostem stanoveným zákonem o ochraně osobních údajů pro zpracování citlivých údajů proto nemusí podléhat systém, který pracuje pouze na principech autentizace, tedy metody kontroly příchodu a odchodu zaměstnance, kdy čtecí zařízení, do kterého otisk prstu vkládá na základě požadavku zaměstnavatele na kontrolu docházky sám zaměstnanec, porovnává údaje 1:1.

Při příchodu na pracoviště nebo odchodu z něj je po zvolení osobního čísla zaměstnance vložený otisk s přiložením příslušného prstu použit pouze pro ověření totožnosti subjektu údajů. Do dalšího zpracování osobních údajů snímek otisku prstu nebo dlaně však již nevstupuje a systém jeho další zpracování ani neumožňuje. Osobní číslo zaměstnance je v takovémto docházkovém systému druhým identifikátorem, který však může být zaměstnavatelem zpracováván v souladu se zákonem o ochraně osobních údajů i bez souhlasu subjektu údajů ve smyslu § 5 odst. 2 písm. e).

Rozhodné pro posouzení, zda jde o z hlediska zásad ochrany přípustnou autentizaci, nebo o identifikaci, kterou je třeba podrobit přísné regulaci, je, zda účelem použití otisku prstu je pouze ověření totožnosti porovnáním s přiloženým prstem ruky, nebo v systému dochází v návaznosti na přiložení ruky nebo její části (případně karty s RFID čipem, který již tyto informace obsahuje) k vyhledávání a porovnávání informací s údajem uchovávaným v databázi biometrických údajů, která musí být vždy považována za zpracování citlivých údajů, podléhající režimu § 9 zákona o ochraně osobních údajů.

I zde však platí, že pro další zpracování osobních údajů zaměstnanců mohou být uplatněny výjimky pro zpracování bez souhlasu subjektu údajů podle § 5 odst. 2 písm. a), b) nebo e) a výjimka z oznamovací povinnosti podle § 18 odst. 1 písm. b), ale je třeba upozornit, že Úřad bude aplikaci těchto výjimek u všech systémů založených na použití biometrických znaků posuzovat nadále velmi obezřetně.

Zaměstnavatel musí důsledně splnit nejen shora uvedené povinnosti podle § 5, 9 a 16, ale dále také informační povinnost podle § 11 a povinnosti při zabezpečení osobních údajů podle § 13 – 15 zákona o ochraně osobních údajů, jestliže by šlo o shromažďování citlivých údajů umožňující jejich další zpracování v databázi, ale v případě jakéhokoliv systému založeného na použití biometrických znaků i informační povinnost o základních pracovních podmínkách a jejich změnách podle § 279 zákoníku práce, neboť může nastat situace, kdy zaměstnanec výlučně vstupní otisk prstu pro ověření totožnosti neposkytne z obavy z jeho možného zneužití.

Závěr

Je třeba zdůraznit, že zejména **biometriku založenou na zpracování citlivých údajů v centrální databázi lze v pracovněprávních vztazích využívat jen ve výjimečných situacích.** Připomenout je třeba i povinnosti zaměstnavatele podle § 316 zákoníku práce, týkající se zákazu otevřeného i skrytého sledování zaměstnance. Toho by se zaměstnavatel mohl dopustit, pokud by pro kontrolu docházky přípustný systém biometrické autentizace využíval pro kontrolu pohybu zaměstnance na pracovišti nad rámec evidence přítomnosti zaměstnance na pracovišti podle § 96 odst. 1 písm. a) zákoníku práce.

Zaměstnancům, kteří mají pochybnosti o oprávněnosti požadavku zaměstnavatele na poskytnutí otisku prstu, Úřad doporučuje využít práva, které dává zákon o ochraně osobních údajů v § 21: Požádat zaměstnavatele o vysvětlení na jakém základě systém funguje. V případě, že by šlo o systém založený na zpracování biometrických údajů jejich vyhledáváním v databázi, nemusejí k tomu dávat souhlas a mohou se na Úřad obrátit s podnětem podle § 21 odst. 4 zákona o ochraně osobních údajů.

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

III. SDĚLENÍ ÚŘADU

PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29

00350/09/CS
WP 159

Stanovisko 1/2009 k návrhům, kterými se mění směrnice 2002/58/ES o ochraně soukromí v elektronických komunikacích (směrnice o soukromí a elektronických komunikacích)

Přijaté dne 10. února 2009

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

Sekretariát skupiny zajišťuje Ředitelství C (Občanská spravedlnost, práva a státní občanství) Evropské komise, generální ředitelství pro spravedlnost, svobodu a bezpečnost, 1049 Brusel, Belgie, kancelář LX-46 01/06.

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

Obsah

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

s ohledem na článek 255 Smlouvy o ES a na 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 její jednací řád,

PŘIJALA TENTO DOKUMENT:

1. SOUVISLOSTI

Dne 13. listopadu 2007 přijala Komise návrh směrnice („návrh"), kterou se mění směrnice 2002/58/ES (směrnice o soukromí a elektronických komunikacích) o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací, a směrnice 2002/21/ES (rámcová směrnice).

Při jeho prvním čtení dne 24. září 2008 Evropský parlament přijal změny návrhu („změny Parlamentu"), ke kterým se vyjádřila dne 6. listopadu 2008 Evropská komise v dokumentu KOM(2008) 723 v konečném znění („vyjádření Komise").

Dne 27. listopadu 2008 pak Rada Evropské unie dosáhla politické dohody („dohoda Rady").

Pracovní skupina zřízená podle článku 29 si přeje vyjádřit své připomínky ke změnám Parlamentu, vyjádřením Komise a dohodě Rady.

Pracovní skupina připomíná, že již přijala dvě stanoviska k návrhům, kterými se mění předpisový rámec EU pro elektronické komunikační sítě a služby (stanovisko 8/2006 přijaté dne 26. září 2006[2] a stanovisko 2/2008 přijaté dne 15. května 2008[3]).

Ačkoli pracovní skupina vítá, že některá z jejích předchozích doporučení byla vzata v úvahu, přeje si zdůraznit některé zásadní obavy týkající se otázek vzešlých po prvním čtení v Parlamentu a v Radě; pracovní skupina neopakuje všechny body zmíněné ve svých předchozích stanoviscích, které stále zůstávají platné.

2. OZNÁMENÍ O NARUŠENÍ BEZPEČNOSTI OSOBNÍCH ÚDAJŮ

2.1. Připomínky

Pracovní skupina plně podporuje navrhované posílení článku 4 směrnice o soukromí a elektronických komunikacích požadavkem, aby poskytovatelé veřejně dostupných komunikačních služeb oznamovali případy narušení bezpečnosti. Oznámení o narušení

[1] Úř. věst. L281, 23.11.1995, s. 31, http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm
[2] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp126_cs.pdf
[3] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp150_cs.pdf

bezpečnosti se mohou stát důležitým nástrojem pro orgány pro ochranu údajů, který pomůže zvýšit soustředění a účinnost při prosazování povinnosti poskytovatelů služeb přijmout vhodná bezpečnostní opatření.

Obecně pracovní skupina doporučuje tento přístup k otázce oznámení o narušení bezpečnosti osobních údajů:

– příslušný vnitrostátní regulační orgán je informován vždy, existuje-li riziko nepříznivých vlivů[4] na soukromí a ochranu údajů fyzické osoby,

– je zásadní, aby byli postižení uživatelé bezodkladně informováni poskytovateli služeb v těch případech, kdy je pravděpodobné, že by narušení bezpečnosti mohlo vést k nepříznivým vlivům[5] na soukromí a ochranu údajů fyzických osob, aniž by byla dotčena možnost příslušného vnitrostátního regulačního orgánu zveřejnit informace o narušení a přinutit poskytovatele služby, aby odhalil informace o tomto narušení,

– každý poskytovatel služby by měl vést záznamy[6] o všech narušeních bezpečnosti osobních údajů.

Pracovní skupina také podotýká, že tři návrhy (Parlamentu, Komise a Rady) přijímají k otázce bezpečnosti a narušení bezpečnosti osobních údajů významně odlišné přístupy, zejména pokud jde o:

– působnost povinnosti (která se rozšiřuje na služby informační společnosti ve změnách Parlamentu a je omezena na veřejně dostupné služby elektronických komunikací pro Radu a Komisi); pracovní skupina důrazně podporuje rozšíření působnosti dané povinnosti na služby informační společnosti,

– subjekt, kterému přísluší rozhodnutí o oznamování fyzickým osobám (je jím příslušný orgán pro Parlament a Komisi a je jím poskytovatel služby pro Radu),

– typy narušení, které se mají oznamovat (všechna narušení v návrhu Parlamentu a ve vyjádřeních Komise a pouze vážné případy narušení v dohodě Rady),

– a osoby, kterým je možno případy narušení oznamovat (účastníci nebo fyzické osoby pro Parlament a Komisi, ale pouze účastníci pro Radu).

Působnost oznámení: služby informační společnosti

Pracovní skupina důrazně podporuje pozměňovací návrhy 187/rev a 184 změn Parlamentu. **Rozšíření oznamování případů narušení bezpečnosti osobních údajů na služby informační společnosti je nezbytné, vezmeme-li v úvahu stále se zvyšující úlohu, kterou tyto služby hrají v každodenním životě evropských občanů,** stejně jako zvyšující se

[4] Riziko nepříznivých vlivů by mělo být posouzeno při zohlednění prvků jako množství údajů postižených narušením bezpečnosti, jejich povaha, dopad tohoto narušení na fyzickou osobu, například krádež identity, finanční ztráta, ztráta obchodních příležitostí nebo příležitostí zaměstnání či kombinace těchto nebo jiných podobných okolností. Kvalitativní a kvantitativní kritéria pro posouzení dopadu nepříznivých vlivů budou muset být při postupu projednávání přesně definována při zohlednění toho, že je důležité nepřetěžovat orgány nevýznamnými případy a zbytečně neburcovat fyzické osoby.

[5] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp126_cs.pdf

[6] Formát těchto záznamů by měl být standardizován, aby se zajistilo, že jsou záznamy kontrolovatelné příslušným vnitrostátním regulačním orgánem.

množství osobních údajů zpracovávaných těmito službami. On-line transakce včetně přístupu k službám elektronického bankovnictví a k zdravotní dokumentaci soukromého sektoru stejně jako on-line nákupy představují několik příkladů služeb, které mohou být předmětem narušení bezpečnosti osobních údajů, jež představují významné riziko pro velký počet evropských občanů. Omezení působnosti těchto povinností na veřejně dostupné služby elektronických komunikací by postihlo pouze velmi omezený počet zúčastněných stran, a významně by tak snížilo dopad oznámení o narušení bezpečnosti osobních údajů jako prostředku ochrany fyzických osob před riziky, jako je krádež totožnosti, finanční ztráta, ztráta obchodních příležitostí nebo příležitostí zaměstnání a fyzická újma.

Proto pracovní skupina hluboce lituje, že tento návrh Komise a Rada nepodpořily, a připomíná, že některá ustanovení směrnice o soukromí a elektronických komunikacích se již uplatňují nad rámec přísného rozsahu služeb elektronických komunikací[7].

Odpovědnost a kritéria pro oznámení

Za posouzení rizik způsobených narušením bezpečnosti osobních údajů by měli být odpovědní příslušní poskytovatelé služeb; ti jsou nejlépe schopni bezodkladně stanovit na základě pravidel pro posouzení stanovených orgány, zda by měly být postižené osoby vyrozuměny. **Aniž by byla dotčena jejich povinnost oznamovat příslušným vnitrostátním regulačním orgánům všechna narušení, kdykoliv hrozí riziko nepříznivých vlivů, poskytovatelé služeb by měli stanovit, zda je potřebné vyrozumět účastníky nebo fyzické osoby. Aby se zajistilo poskytnutí přesných a relevantních informací veřejnosti, mohou se příslušné regulační orgány rozhodnout zveřejnit narušení bezpečnosti vždy, je-li to považováno za nezbytné, a mohou přinutit poskytovatele služby, aby odhalil informace o tomto narušení.**

Protože oznámení provede poskytovatel služby, **je důležité, aby směrnice poskytovala záruky k zajištění, že narušení bezpečnosti nebylo zatajeno**, že bylo provedeno jeho správné posouzení a že fyzické osoby byly vyrozuměny, kdykoli o to bylo požádáno.

Orgány budou vyrozuměny ve větším počtu případů, aby mohly vykonávat dozor nad procesem oznamování fyzickým osobám poskytovateli služeb. Formát oznámení by měl být harmonizován na evropské úrovni a měl by zahrnovat objektivní a srozumitelná kritéria, která napomohou při posuzování dopadu nepříznivých vlivů způsobených narušením bezpečnosti. Kromě toho by měl příslušný vnitrostátní regulační orgán zkontrolovat, zda poskytovatel služby správně provedl posouzení daného narušení a zda byla po narušení bezpečnosti osobních údajů přijata vhodná opatření. **Proto, aby se zamezilo zatajování případů narušení bezpečnosti, je nutné, aby směrnice poskytovala příslušnému vnitrostátnímu regulačnímu orgánu pravomoc ukládat finanční trestní sankce (pokuty)[8] v případech, kdy poskytovatel služby narušení bezpečnosti osobních údajů fyzickým osobám a/nebo vnitrostátnímu regulačnímu orgánu neoznámí, případně není-li toto oznámení učiněno správně.**

---

[7] Určitá ustanovení směrnice o soukromí a elektronických komunikacích, jako je čl. 5 odst. 3 (*cookies* a *spyware*) a článek 13 (nevyžádaná sdělení) jsou již obecnými ustanoveními, která jsou použitelná nejen na služby elektronických komunikací.
S tímto možným rozšířením nad rámec přísného rozsahu dostupných služeb elektronických komunikací se také počítá v jiných situacích, protože Komise navrhla rozšířit působnost použití čl. 5 odst. 3 na případy, kdy jsou *cookies* a *spyware* dodány prostřednictvím takových médií, jako jsou CD-ROM nebo klíče USB, které nejsou veřejně dostupnými službami elektronických komunikací.

[8] Pracovní skupina poznamenává, že tato ustanovení navrhl Parlament, Komise a Rada v novém čl. 15a odst. 1.

Typy narušení, které se mají oznamovat fyzickým osobám: pojem nepříznivých vlivů

Pracovní skupina vítá zavedení nové definice „narušení bezpečnosti osobních údajů“ v článku 2[9], jak je navržena ve vyjádřeních Komise[10].

Pracovní skupina však zaznamenává, že tři návrhy používají různou formulaci pro stanovení, kdy by měla být narušení oznámena subjektům údajů. Proto **pracovní skupina doporučuje, že by se případy narušení bezpečnosti měly oznamovat subjektům údajů, jestliže by mohly mít nepříznivý vliv na soukromí a ochranu údajů fyzických osob.** V tomto ohledu poskytuje dohoda Rady užitečné příklady v bodu odůvodnění 29.

Osoby, které mohou být vyrozuměny

Pracovní skupina vítá odkazy na „účastníky nebo fyzické osoby“, na „postižené uživatele“ a na „příslušný vnitrostátní orgán“ zahrnuté do bodu odůvodnění 29 změn Parlamentu[11]. Dohoda Rady omezuje oznámení na „účastníky“, a proto některé případy narušení bezpečnosti osobních údajů, které byly popsány ve stanovisku 2/2008, nebudou postiženým osobám oznámeny.

2.2. Výjimky z oznamování

Pracovní skupina uznává, že oznámení o narušení bezpečnosti by měla zahrnovat informace o okolnostech narušení, včetně toho, zda byly osobní údaje chráněny šifrováním; tyto informace jsou zásadní proto, aby příslušný vnitrostátní regulační orgán v případě narušení určil podle potřeby vhodné opatření, které se má učinit s poskytovatelem služby.

Pracovní skupina je však proti vytváření výjimek z oznamování[12], jestliže poskytovatelé služby přijali „vhodná technická ochranná opatření“ a tato opatření byla použita ve vztahu k údajům, jež byly předmětem daného narušení bezpečnosti“. Toto ustanovení by významně snížilo kvalitu a užitečnost informací poskytnutých postiženým osobám. Postižení uživatelé budou schopni učinit vhodná opatření ke zmírnění rizik, kterým čelí, pouze pokud byli vhodně informováni. Proto **pracovní skupina zdůrazňuje důležitost formátu oznámení a posouzení rizika při určení, zda by měly být fyzické osoby vyrozuměny bez ohledu na technická opatření, která byla skutečně přijata pro ochranu jejich údajů.**

3. PROVOZNÍ ÚDAJE

3.1. Zpracování provozních údajů pro účely bezpečnosti

V čl. 6 novém odst. 6a navrhuje Parlament, Rada a Komise vytvořit novou výjimku ve směrnici o soukromí a elektronických komunikacích umožňující zpracování provozních údajů pro účely bezpečnosti.

Pracovní skupina si je vědoma toho, že „poskytovatelé bezpečnostních služeb“ zavádějí bezpečnostní řešení[13] (antivirové a antispamové programové vybavení, firewall nebo systémy

---

9 Viz vyjádření Komise k pozměňovacím návrhům 187/rev a 184 změn Parlamentu.

10 Přesto je tento pojem „narušení bezpečnosti osobních údajů“ obecný a neměl by být omezen na údaje zpracovávané v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací; měl by také zahrnovat alespoň služby informační společnosti.

11 Viz pozměňovací návrh 183.

12 Viz bod odůvodnění 29 ve změnách Parlamentu (pozměňovací návrh 122) a body odůvodnění 29 a 32 v dohodě Rady.

13 Buď v koncovém zařízení uživatele, nebo v síti.

detekce průniků), která mohou vyžadovat zpracování provozních údajů pro účely zabezpečení osobních údajů uživatelů a ochrany vlastní služby. Přesto vyjadřuje obavu, že současná formulace by mohla znamenat oprávněnost rozsáhlého zavedení hloubkové kontroly paketů[14], a to v síti i ve vybavení uživatele, jako jsou sady ADSL, zatímco současný právní rámec již uvádí případy, kdy mohou být provozní údaje zpracovány pro bezpečnostní účely.

Právní základ umožňující zpracování provozních údajů veřejně dostupnými službami elektronických komunikací a zpracování osobních údajů správci dat je skutečně stanoven v článku 6 směrnice o soukromí a elektronických komunikacích i v článcích 7 a 17 směrnice o ochraně údajů. Rozsah, do kterého mohou být zpracovány osobní údaje pro uskutečnění oprávněných zájmů správce, je uveden v čl. 7 písm. f) směrnice o ochraně údajů; zpracování nesmí převýšit zájem nebo základní práva a svobody subjektu údajů. Článek 17 směrnice o ochraně údajů také ukládá správci údajů povinnost „*přijmout vhodná technická a organizační opatření na ochranu osobních údajů proti náhodnému nebo nedovolenému zničení, náhodné ztrátě, úpravám, neoprávněnému sdělování nebo přístupu... jakož i proti jakékoli jiné podobě nedovoleného zpracování*“. Přijatá opatření musí být také úměrná rizikům, která představují zpracování a povaha údajů, které se mají chránit.

Pracovní skupina také zdůrazňuje, že rozsah pozměňovacího návrhu 180 změn Parlamentu byl objasněn ve vyjádřeních Komise. **Pracovní skupina poznamenává, že formulace navržená Komisí nepochybně stanoví, že zpracování provozních údajů patří do působnosti směrnice o ochraně údajů.** Proto musí poskytovatelé bezpečnostních služeb vyrozumět orgány pro ochranu údajů, kdykoli je to potřebné, a zajistit, aby mohla být uplatňována práva jednotlivců.

Dále pracovní skupina připomíná, že zpracování provozních údajů pro bezpečnostní účely se již provádí v členských státech, kde byla přijata specifická opatření podle čl. 15 odst. 1 směrnice o soukromí a elektronických komunikacích, který umožňuje členským státům přijmout legislativní opatření upouštějící od zásady anonymizování nebo vymazání provozních údajů[15], jakmile již nejsou potřebné pro přenos sdělení, aby se zabránilo neoprávněnému použití elektronického komunikačního systému.

Z výše uvedených důvodů **není návrh čl. 6 nového odst. 6a nutný.**

4. IP ADRESY

Parlament a Komise navrhují zavést nový bod odůvodnění 27a o IP adresách[16].

Pracovní skupina vítá formulaci navrženou ve vyjádřeních Komise, kde uvádí zvláštní odkaz na její činnost. Pracovní skupina však nepodporuje návrh zavést výslovný odkaz na tuto otázku do směrnice.

V tomto ohledu **znovu zdůrazňuje své dřívější stanovisko[17], že pokud není poskytovatel služby** „*schopen s naprostou jistotou odlišit údaje odpovídající uživatelům, kteří nemohou být identifikováni, bude muset pro jistotu nakládat se všemi informacemi o IP adresách jako s osobními údaji*“.

---

[14] Hloubková kontrola paketů umožňuje velmi agresivní kontrolu a sledování chování uživatele.

[15] Stanovené v čl. 6 odst. 1.

[16] Pozměňovací návrh 185 Parlamentu.

[17] Stanovisko 4/2007 k pojmu osobní údaje a stanovisko k otázkám ochrany údajů v souvislosti s vyhledávači.

IP adresy souvisí ve většině případů s identifikovatelnými osobami. Schopnost identifikace znamená možnost identifikace poskytovatelem přístupu nebo jinými prostředky za pomoci dalších identifikátorů, jako jsou *cookies*, nebo při interakcích s internetovými službami, u kterých je subjekt údajů explicitně nebo implicitně identifikován.

Bod odůvodnění 26 směrnice o ochraně údajů jasně uvádí, že pro určení, zda je osoba identifikovatelná, *„je třeba přihlédnout ke všem prostředkům, které mohou být rozumně použity jak správcem, tak jakoukoli jinou osobou pro identifikaci dané osoby“*.

Definice osobních údajů ve směrnici o ochraně osobních údajů odkazuje na údaje „o“ určité osobě a IP adresy se běžně používají pro rozlišení mezi uživateli, u kterých by mělo být uplatněno rozdílné zacházení, například v souvislosti s účely cílené inzerce nebo tvorby profilu.

I když je pracovní skupina připravena napomáhat Komisi při vyvíjení činnosti týkající se IP adres navržené Parlamentem[18], souhlasí s Komisí, že hmotněprávní ustanovení směrnice není nejvhodnější způsob, jak tuto otázku řešit, a že povinnost předkládání zpráv odkazující „na účely neuvedené v této směrnici“ není vhodná.

5. INFORMACE ORGÁNŮ PRO OCHRANU ÚDAJŮ

Ve svém prvním čtení Parlament přijal pozměňovací návrh 136 článku 15 směrnice o soukromí a elektronických komunikacích, který pak byl změněn vyjádřeními Komise. Tento návrh by zřídil povinnost pro všechny poskytovatele telekomunikačních služeb a sítí a všechny poskytovatele služeb informační společnosti informovat příslušný orgán pro ochranu údajů o každé žádosti „obdržené podle odstavce 1“[19] a povinnost pro tento orgán vyšetřit každou žádost a zpětně „uvědomit příslušné soudní orgány, že nebyla dodržena platná ustanovení vnitrostátního práva“.

Navržená informační povinnost je užitečným přídavkem v zájmu větší transparentnosti a kontroly regulačními orgány. Zatímco by toto ustanovení výrazně zvýšilo schopnost dozoru a prosazování ze strany orgánů pro ochranu údajů, a přispělo tak k lepšímu uplatňování zákonného přístupu k informacím, vytvořilo by však také správní zatížení pro zapojené společnosti i pro orgány pro ochranu údajů. V tomto ohledu pracovní skupina vyjadřuje obavy s ohledem na potřebu sledovat rostoucí počet požadavků soudních orgánů[20] a na novou odpovědnost pro orgány pro ochranu údajů kontrolovat každé soudní šetření, což vyžaduje významný nárůst finančních a personálních zdrojů těchto orgánů.

Proto **pracovní skupina navrhuje, aby mohla být taková informační povinnost prováděna pouze jednou ročně. Mohla by obsahovat údaje o vnitřních postupech používaných pro odpovědi na žádosti o přístup k osobním údajům uživatelů, počtu obdržených žádostí, uplatněném právním odůvodnění a podle potřeby o problémech, ke kterým došlo.** Je také zásadní, aby byla taková informační povinnost harmonizována a podrobně popsána na úrovni EU.

---

[18] V pozměňovacích návrzích 139 a 186/rev.

[19] Který popisuje povinnosti uchovávání údajů formalizované ve směrnici o uchovávání údajů (2006/24/ES).

[20] Mnoho provozovatelů telekomunikačních služeb dostává několik stovek požadavků za den.

6. NEVYŽÁDANÁ SDĚLENÍ

Pozměňovací návrh 131 Parlamentu poskytuje upřesnění, že MMS a podobné technologie spadají pod definici „elektronická pošta“ uvedenou v čl. 2 písm. h).

Zaprvé pracovní skupina podotýká, že bod odůvodnění 40 směrnice o soukromí a elektronických komunikacích již upřesňuje, že SMS spadá do definice elektronické pošty[21].

Zadruhé je nezbytné přizpůsobit čl. 13 odst. 1 nově vznikajícím technologiím podle zásady stanovené v bodu odůvodnění 4[22]. Současná formulace čl. 13 odst. 1 předpokládá, že osoba je již připojena k síti, ve které je sdělení přenášeno (například volání nebo elektronická pošta). Nevztahuje se na případy, kdy by byl uživatel žádán, aby se připojil k síti, která slouží výhradně k inzerci. To by obvykle mohl být případ marketinkových aplikací Bluetooth.

Proto pracovní skupina vítá upřesnění poskytnutá ve vyjádřeních Komise k působnosti čl. 13 týkající se hlavně použití slova „sdělení“ a nový bod odůvodnění odkazující na „podobné technologie“. To zajišťuje, že je nutný předchozí souhlas u marketingových aplikací Bluetooth, a bere tedy v úvahu poznámky pracovní skupiny v jejím stanovisku 2/2008 týkající se potřeby „chránit uživatele bezdrátových médií s krátkým dosahem proti nevyžádaným sdělením definovaným v článku 13“. Výslovný odkaz na Bluetooth by mohl také být součástí bodu odůvodnění 40.

Zatřetí pracovní skupina připomíná svoji poznámku v stanovisku 2/2008 o používání výrazu „účastník“ v článku 13 a s uspokojením bere na vědomí formulaci navrhovanou v dohodě Rady.

Návrh Rady změnit čl. 13 odst. 2 přidáním obratu „v okamžiku shromažďování těchto podrobností“ je konečně také velmi užitečný, protože poskytuje jednoznačné informace o okamžiku, kdy budou uživatelé schopni odmítnout využití jejich elektronických kontaktních údajů pro účely přímého marketingu.

7. NASTAVENÍ PROHLÍŽEČE

Pracovní skupina důrazně odmítá pozměňovací návrh 128 přijatý Parlamentem, který uvádí, že standardní nastavení prohlížeče by bylo prostředkem poskytnutí předchozího souhlasu. I když byl tento pozměňovací návrh zahrnut do vyjádření Komise a dohody Rady, pracovní skupina se chce k tomuto pozměňovacímu návrhu vyjádřit.

Kromě formálního problému s vytvořením tak technologicky specifického jazyka ve směrnici se pracovní skupina obává, že by mohlo dojít k rozkladu definice souhlasu a následné absenci transparentnosti.

Většina prohlížečů používá standardní nastavení, která nedovolují uživatelům, aby byli informováni o jakémkoli prozatímním ukládání nebo přístupu k jejich koncovému vybavení. Proto by standardní nastavení prohlížeče měla být „přívětivá z hlediska soukromí“, ale

---

[21] Která je definována v čl. 2 písm. h) směrnice o soukromí a elektronických službách.

[22] Který stanoví, že směrnici o soukromí a elektronických službách je „nutno přizpůsobit vývoji trhů a technologií v oblasti služeb elektronických komunikací, aby uživatelům veřejně dostupných služeb elektronických komunikací zajistila stejnou úroveň ochrany osobních údajů a soukromí bez ohledu na použité technologie“.

nemohou být prostředkem shromažďování svobodného, výslovného a vědomého souhlasu uživatelů, jak vyžaduje čl. 2 písm. h) směrnice o ochraně údajů.

Pokud se jedná o *cookies*, pracovní skupina zastává stanovisko, že správce *cookies* by měl informovat své uživatele v prohlášení o ochraně soukromí a nesměl by se spoléhat na (standardní) nastavení prohlížeče. Zvolená formulace také není omezena na současné vydání *cookies*, ale předpokládá jakoukoli další novou technologii, která by se mohla používat pro sledování chování uživatelů, kteří používají svůj prohlížeč.

8. PRÁVNÍ KROKY FYZICKÝCH A PRÁVNICKÝCH OSOB

Pracovní skupina podporuje návrh Parlamentu[23] zavést v čl. 13 odst. 6 možnost, aby „každá fyzická nebo právnická osoba mohla učinit právní kroky v případě, že byla nepříznivě ovlivněná porušováním vnitrostátních předpisů přijatých podle směrnice o soukromí a elektronických komunikacích".

Toto ustanovení bezpochyby posílí práva uživatele a přispěje k rozvoji lepších bezpečnostních postupů mezi účastníky daného odvětví.

9. DALŠÍ OTÁZKY

Na závěr pracovní skupina s uspokojením poznamenává:

– že zákonodárce má v úmyslu potrestat postupy *phishing*[24],

– že Komise a Rada vzaly v úvahu[25] požadavek pracovní skupiny, aby byla konzultována v průběhu postupu projednávání stanoveného v čl. 4 odst. 4,

– že byla zahrnuta do konzultačního procesu stanoveného v čl. 15a odst. 4,

– že bude konzultována při přípravě zprávy o uplatňování pozměněné směrnice o soukromí a elektronických komunikacích[26],

– že Komise, Rada a Parlament si přejí upřesnit, že směrnice o soukromí a elektronických komunikacích se vztahuje na nově vznikající technologie, jako je RFID[27] nebo NFC, které jsou založeny na bezkontaktních identifikačních zařízeních využívajících rádiové frekvence.

---

23 V pozměňovacím návrhu 133.
24 Viz pozměňovací návrh 132 Parlamentu.
25 Ve svém vyjádření k pozměňovacímu návrhu 127 Parlamentu.
26 Viz pozměňovací návrh 139 a 186/rev Parlamentu.
27 V článku 3 a bodu odůvodnění 28.

10. ZÁVĚR

Pracovní skupina zřízená podle článku 29 vyzývá evropské zákonodárce, aby mezi ostatními otázkami zdůrazněnými v tomto stanovisku v co nejvyšší míře zvážili rozšíření působnosti oznamovacích povinností o narušení bezpečnosti osobních údajů na služby informační společnosti, vzhledem k jeho zásadnímu dopadu na ochranu osobních údajů všech evropských občanů.

V Bruselu dne 10. února 2009.

Za pracovní skupinu
předseda
Alex TÜRK

IV. MATERIÁLY Z ÚŘEDNÍHO VĚSTNÍKU EVROPSKÉ UNIE

Příloha Věstníku Úřadu pro ochranu osobních údajů (s. 3046 – 3051)

DOPORUČENÍ

KOMISE

DOPORUČENÍ KOMISE

ze dne 12. května 2009

o zavedení zásad ochrany soukromí a údajů v aplikacích podporovaných identifikací na základě rádiové frekvence

(oznámeno pod číslem K(2009) 3200)

(2009/387/ES)

KOMISE EVROPSKÝCH SPOLEČENSTVÍ,

s ohledem na Smlouvu o založení Evropského společenství, a zejména na článek 211 této smlouvy,

po konzultaci s evropským inspektorem ochrany údajů,

vzhledem k těmto důvodům:

(1) Identifikace na základě rádiové frekvence (RFID) předznamenává nový vývoj v informační společnosti, kdy se předměty vybavené mikroelektronikou, která může automaticky zpracovávat údaje, budou stále více stávat nedílnou součástí každodenního života.

(2) RFID je postupně stále běžnější, stává se tudíž součástí života jednotlivců v různých oblastech, jako je logistika ([1]), zdravotnictví, veřejná doprava, maloobchod, zejména v zájmu větší bezpečnosti výrobků a rychlejšího stažení výrobků z trhu, zábava, práce, správa mýtného, odbavování zavazadel a cestovní doklady.

(3) Technologie RFID se může stát novou hnací silou růstu a tvorby pracovních příležitostí, a tak významně přispět k Lisabonské strategii, jelikož je velmi slibná z hospodářského hlediska, kde může zajistit nové obchodní příležitosti, snížení nákladů a vyšší účinnost, zejména v boji proti padělání a při nakládání s elektronickým odpadem, nebezpečným materiálem a při recyklaci výrobků na konci jejich životnosti.

([1]) KOM(2007) 607 v konečném znění.

(4) Technologie RFID umožňuje zpracovávat údaje, včetně osobních údajů, na krátké vzdálenosti bez fyzického kontaktu či viditelné interakce mezi čtecím nebo zapisovacím zařízením a etiketou, takže k této interakci může dojít, aniž by si toho byl dotyčný jednotlivec vědom.

(5) Aplikace RFID mohou zpracovávat údaje týkající se fyzické osoby, jejíž totožnost je zjištěna nebo se má zjistit, a to přímo či nepřímo. Mohou zpracovávat osobní údaje uložené na etiketě, například jméno dotyčné osoby, její datum narození nebo adresu či biometrické údaje nebo údaje spojující určité číslo výrobku RFID s osobními údaji uloženými jinde v systému. Tuto technologii lze využít ke sledování jednotlivců, pokud tito vlastní jeden či více výrobků, které obsahují číslo výrobku RFID.

(6) Vzhledem k potenciálu této technologie být všudypřítomná a prakticky neviditelná je při zavádění RFID nutno věnovat zvláštní pozornost otázkám ochrany soukromí a údajů. Do aplikací by proto měly být před jejich rozšířeným používáním zabudovány bezpečnostní prvky s ohledem na soukromí a informace (zásada „konstrukčního návrhu nenarušujícího bezpečnost a soukromí“).

(7) RFID může přinést četné hospodářské a společenské výhody pouze tehdy, budou-li zavedena účinná opatření k zajištění ochrany osobních údajů, soukromí a souvisejících etických zásad, jež jsou ústředním bodem diskuse o přijetí RFID ze strany veřejnosti.

(8) Členské státy a zúčastněné osoby by měly zejména v této počáteční fázi zavádění RFID vynaložit další úsilí s cílem zajistit, aby aplikace RFID byly sledovány a aby byla respektována práva a svobody jednotlivců.

(9) Sdělení Komise ze dne 15. března 2007 „Identifikace na základě rádiové frekvence (RFID) v Evropě: kroky k rámci politiky“ ([1]) oznámilo, že budou poskytnuta objasnění a pokyny k aspektům ochrany údajů a soukromí v souvislosti s aplikacemi RFID prostřednictvím jednoho či více doporučení Komise.

(10) Práva a povinnosti týkající se ochrany osobních údajů a volného pohybu těchto údajů, jak jsou stanoveny ve 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 ([2]) a směrnici Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích) ([3]), jsou plně použitelné na aplikace RFID, které zpracovávají osobní údaje.

(11) Při vývoji aplikací RFID je nutno uplatňovat zásady stanovené ve směrnici Evropského parlamentu a Rady 1999/5/ES ze dne 9. března 1999 o rádiových zařízeních a telekomunikačních koncových zařízeních a vzájemném uznávání jejich shody ([4]).

(12) Stanovisko evropského inspektora ochrany údajů ([5]) poskytuje vodítko pro nakládání s výrobky obsahujícími etikety, které jsou poskytovány jednotlivcům a vyžaduje posouzení dopadů na soukromí a bezpečnost k určení a vypracování „nejlepších dostupných technologií“ v zájmu zajištění soukromí a bezpečnosti systémů RFID.

(13) Provozovatelé aplikací RFID by měli přijmout veškerá přiměřená opatření s cílem zajistit, aby se údaje nevztahovaly na fyzickou osobu, jejíž totožnost je zjištěna nebo se má zjistit, prostřednictvím jakýchkoli prostředků, jež budou pravděpodobně použity provozovatelem aplikace RFID či jinou osobou, nejsou-li tyto údaje zpracovávány v souladu s platnými zásadami a právními předpisy o ochraně údajů.

(14) Sdělení Komise ze dne 2. května 2007 o „podpoře ochrany osobních údajů prostřednictvím technologií zvyšujících ochranu soukromí (PETs)“ ([6]) stanoví jasná opatření k dosažení cíle týkajícího se minimalizace zpracování osobních údajů a tam, kde je to možné, využívání anonymních nebo pseudonymních údajů podporou vývoje PETs a jejich využívání správci údajů a jednotlivci.

(15) Sdělení Komise ze dne 31. května 2006 Strategie pro bezpečnou informační společnost – „Dialog, partnerství a posílení účasti“ ([7]) uznává, že rozmanitost, otevřenost, interoperabilita, použitelnost a hospodářská soutěž jsou hlavními hnacími silami pro bezpečnou informační společnost, vyzdvihuje úlohu členských států a orgánů veřejné správy při zvyšování informovanosti a prosazování dobrých bezpečnostních postupů a vyzývá zúčastněné strany ze soukromého sektoru, aby přijaly iniciativy s cílem pracovat na cenově dostupných programech osvědčování bezpečnosti pro produkty, procesy a služby, které budou zohledňovat specifické potřeby EU zejména s ohledem na ochranu soukromí.

(16) Usnesení Rady ze dne 22. března 2007 ([8]) o strategii pro bezpečnou informační společnost v Evropě členské státy vyzývá, aby věnovaly náležitou pozornost potřebě zamezit novým a stávajícím bezpečnostním hrozbám pro elektronické komunikační sítě.

(17) Rámec vypracovaný na úrovni Společenství pro posuzování dopadů na soukromí a ochranu údajů zajistí, aby ustanovení tohoto doporučení byla jednotně dodržována ve všech členských státech. Vypracování takovéhoto rámce by mělo navazovat na stávající postupy a zkušenosti získané v členských státech, ve třetích zemích a při práci Evropské agentury pro bezpečnost sítí a informací (ENISA) ([9]).

(18) Komise zajistí vypracování pokynů na úrovni Společenství k řízení bezpečnosti informací pro aplikace RFID, které navazují na stávající postupy a zkušenosti získané v členských státech a třetích zemích. Členské státy by měly přispět k tomuto procesu a vybízet soukromé subjekty a orgány veřejné správy k účasti.

(19) Posouzení dopadů na soukromí a ochranu údajů provedené provozovatelem před zavedením aplikace RFID poskytne informace potřebné pro náležitá ochranná opatření. Tato opatření je nutno sledovat a přezkoumávat po celou dobu používání aplikace RFID.

(20) V odvětví maloobchodu by mělo posouzení dopadů výrobků obsahujících etikety, které jsou prodávány spotřebitelům, na soukromí a ochranu údajů poskytnout potřebné informace s cílem určit, zda existuje pravděpodobná hrozba pro soukromí nebo ochranu osobních údajů.

([1]) KOM(2007) 96 v konečném znění.
([2]) Úř. věst. L 281, 23.11.1995, s. 31.
([3]) Úř. věst. L 201, 31.7.2002, s. 37.
([4]) Úř. věst. L 91, 7.4.1999, s. 10.
([5]) Úř. věst. C 101, 23.4.2008, s. 1.
([6]) KOM(2007) 228 v konečném znění.
([7]) KOM(2006) 251 v konečném znění.
([8]) Úř. věst. C 68, 24.3.2007, s. 1.
([9]) Čl. 2 odst. 1 nařízení (ES) č. 460/2004 Evropského parlamentu a Rady (Úř. věst. L 77, 13.3.2004, s. 1).

(21) Řízení bezpečnosti informací a opatření na ochranu soukromí v celém obchodním procesu umožněném RFID může napomoci používání mezinárodních norem, například norem vypracovaných Mezinárodní organizací pro normalizaci (ISO), kodexů chování a osvědčených postupů, jež jsou v souladu s právním rámcem EU.

(22) Aplikace RFID s důsledky pro širokou veřejnost, například elektronické jízdenky ve veřejné dopravě, vyžadují vhodná ochranná opatření. Aplikace RFID, které se dotýkají jednotlivce například zpracováváním biometrických identifikačních údajů nebo údajů souvisejících se zdravím, jsou obzvláště kritické, pokud jde o bezpečnost informací a soukromí, a vyžadují proto zvláštní pozornost.

(23) Celá společnost musí být informována o povinnostech a právech, jež jsou platné s ohledem na používání aplikací RFID. Strany, které zavádějí tuto technologii, proto odpovídají za informování jednotlivců o používání těchto aplikací.

(24) Zvyšování informovanosti veřejnosti a malých a středních podniků o charakteristikách a schopnostech RFID pomůže této technologii naplnit hospodářská očekávání a současně zmírnit rizika toho, že bude použita na úkor veřejného zájmu, zvýšit tudíž její přijatelnost.

(25) Komise přispěje k provádění tohoto doporučení přímo a nepřímo usnadněním dialogu a spolupráce mezi zúčastněnými stranami, zejména prostřednictvím rámcového programu pro konkurenceschopnost a inovace zřízeného rozhodnutím Evropského parlamentu a Rady č. 1639/2006/ES [1] a sedmého rámcového programu pro výzkum (7. RP) zřízeného rozhodnutím Evropského parlamentu a Rady č. 1982/2006/ES [2].

(26) Na úrovni Společenství je nezbytný výzkum a vývoj nízkonákladových technologií na podporu ochrany soukromí a technologií pro bezpečnost informací k prosazování širšího přijetí těchto technologií za přijatelných podmínek.

(27) Toto doporučení dodržuje základní práva a ctí zásady uznávané zejména Listinou základních práv Evropské unie. Cílem tohoto doporučení je zejména zajistit respektování soukromého a rodinného života a ochrany osobních údajů,

[1] Úř. věst. L 310, 9.11.2006, s. 15.
[2] Úř. věst. L 412, 30.12.2006, s. 1.

DOPORUČUJE:

Oblast působnosti

1. Toto doporučení poskytuje členským státům vodítko při navrhování a provozování aplikací RFID zákonným, etickým a sociálně a politicky přijatelným způsobem při současném dodržování práva na soukromí a zajištění ochrany osobních údajů.

2. Toto doporučení poskytuje pokyny k opatřením, jež je nutno přijmout s ohledem na zavádění aplikací RFID s cílem zajistit, aby při používání těchto aplikací byly popřípadě dodržovány vnitrostátní právní předpisy k provedení směrnic 95/46/ES, 1999/5/ES a 2002/58/ES.

Definice

3. Pro účely tohoto doporučení se použijí definice stanovené ve směrnici 95/46/ES. Použijí se rovněž tyto definice:

a) „identifikací na základě rádiové frekvence“ (RFID) se rozumí využívání elektromagnetických vln nebo magnetického pole v části spektra rádiových frekvencí ke komunikaci s etiketou prostřednictvím různých modulačních a kódovacích systémů z účelem jednoznačného přečtení identity etikety nebo jiných údajů, které jsou na ní uloženy;

b) „etiketou RFID“ nebo „etiketou“ se rozumí zařízení RFID, které je schopné vytvářet rádiový signál, nebo zařízení RFID, jež opětovně spojuje, zpětně rozptyluje nebo odráží (podle druhu zařízení) a moduluje nosný signál přijatý ze čtecího nebo zapisovacího zařízení;

c) „čtecím nebo zapisovacím zařízením RFID“ nebo „čtečkou“ se rozumí pevné nebo přenosné zařízení k zachycování a identifikaci údajů pomocí vysokofrekvenčních elektromagnetických vln nebo magnetického pole ke stimulaci a vyvolání odezvy modulovaných dat z etikety nebo skupiny etiket;

d) „aplikací RFID“ nebo „aplikací“ se rozumí aplikace, která zpracovává údaje pomocí etiket a čteček a která je podporována záložním systémem a síťovou komunikační infrastrukturou;

e) „provozovatelem aplikace RFID“ nebo „provozovatelem“ se rozumí fyzická nebo právnická osoba, orgán veřejné správy, úřad nebo jiný subjekt, který sám či společně s ostatními stanoví účel a způsoby provozování aplikace, včetně správců osobních údajů používajících aplikaci RFID;

f) „bezpečností informací“ se rozumí zachování důvěrnosti, integrity a dostupnosti informací;

g) „sledováním“ se rozumí jakákoliv činnost vykonávaná za účelem zjištění, pozorování, reprodukování nebo zaznamenání údajů o místě, na němž se jednotlivec nachází, jeho pohybu, činnosti nebo stavu.

Posouzení dopadů na soukromí a ochranu údajů

4. Členské státy by měly zajistit, aby odvětví ve spolupráci s příslušnými zúčastněnými stranami z občanské společnosti vypracovalo rámec pro posuzování dopadů na soukromí a ochranu údajů. Tento rámec by měl být předložen ke schválení pracovní skupině pro ochranu údajů zřízené podle článku 29 do dvanácti měsíců ode dne vyhlášení tohoto doporučení v *Úředním věstníku Evropské unie*.

5. Členské státy by měly zajistit, aby provozovatelé bez ohledu na své povinnosti podle směrnice 95/46/ES:

a) prováděli posuzování důsledků zavedení aplikace pro ochranu osobních údajů a soukromí, včetně toho, zda by bylo možno aplikaci využít ke sledování jednotlivce. Úroveň podrobnosti tohoto posouzení by měla odpovídat hrozbě pro soukromí, jež je případně s aplikací spojena;

b) přijali vhodná technická a organizační opatření s cílem zajistit ochranu soukromých údajů a soukromí;

c) určili osobu nebo skupinu osob odpovědných za přezkum posouzení a další vhodnosti technických a organizačních opatření k zajištění ochrany soukromých údajů a soukromí;

d) zpřístupnili posouzení příslušnému orgánu nejméně šest týdnů před zavedením aplikace;

e) jakmile bude k dispozici rámec pro posuzování dopadů na soukromí a ochranu údajů stanovený v bodě 4, prováděli výše uvedená ustanovení v souladu s tímto rámcem.

Bezpečnost informací

6. Členské státy by měly Komisi podpořit při určování aplikací, které mohou představovat hrozbu pro bezpečnost informací s důsledky pro širokou veřejnost. U těchto aplikací by měly členské státy zajistit, aby provozovatelé spolu s příslušnými vnitrostátními orgány a organizacemi občanské společnosti vyvinuli nové systémy nebo používali stávající systémy, například osvědčování nebo sebehodnocení provozovatele, s cílem prokázat, že s ohledem na posuzovaná rizika je zajištěna přiměřená úroveň bezpečnosti informací a ochrany soukromí.

Informování a transparentnost používání RFID

7. Aniž jsou dotčeny povinnosti správců údajů v souladu se směrnicemi 95/46/ES a 2002/58/ES, členské státy by měly zajistit, aby provozovatelé pro každou ze svých aplikací vypracovali a zveřejnili stručnou, přesnou a srozumitelnou informační politiku. Tato politika by měla zahrnovat přinejmenším:

a) totožnost a adresu provozovatelů;

b) účel aplikace;

c) jaké údaje má aplikace zpracovávat, zejména v případě zpracování osobních údajů, a zda bude sledováno umístění etiket;

d) souhrn posouzení dopadů na soukromí a ochranu údajů;

e) pravděpodobná rizika pro soukromí (pokud existují) v souvislosti s používáním etiket v aplikaci a opatření, jež mohou jednotlivci přijmout ke zmírnění těchto rizik.

8. Členské státy by měly zajistit, aby provozovatelé přijali opatření k informování jednotlivců o přítomnosti čteček na základě společné evropské značky vypracované evropskými normalizačními organizacemi s podporou dotčených zúčastněných stran. Značka by měla udávat totožnost provozovatele a kontaktní místo, kde mohou jednotlivci obdržet informační politiku pro danou aplikaci.

Aplikace RFID používané v maloobchodu

9. Na základě společné evropské značky vypracované normalizačními organizacemi s podporou dotčených zúčastněných stran by provozovatelé měli jednotlivce informovat o přítomnosti etiket, jež jsou umístěny na výrobcích či v nich zabudovány.

10. Při posuzování dopadů na soukromí a ochranu údajů uvedeného v bodech 4 a 5 by provozovatel aplikace měl zejména určit, zda etikety umístěné na výrobcích či zabudované ve výrobcích, jež jsou prodávány spotřebitelům prostřednictvím maloobchodníků, kteří nejsou provozovateli dané aplikace, představují pravděpodobnou hrozbu pro soukromí nebo ochranu osobních údajů.

11. Maloobchodníci by měli v okamžiku prodeje deaktivovat nebo odstranit etikety používané v jejich aplikaci, ledaže spotřebitele poté, co byli informováni o politice uvedené v bodě 7, udělili souhlas se zachováním funkčnosti etiket. Deaktivací etiket se rozumí proces, který zastaví interakce etikety s jejím okolím, jež nevyžadují aktivní účast spotřebitele. Deaktivaci nebo odstranění etiket by měl maloobchodník provést pro spotřebitele neprodleně a zdarma. Spotřebitelé by měli být schopni ověřit, zda je deaktivace nebo odstranění účinné.

12. Bod 11 by se neměl použít v případě, dospěje-li posouzení dopadů na soukromí a ochranu údajů k závěru, že etikety, které jsou používány v maloobchodní aplikaci a které zůstanou po prodeji funkční, nepředstavují pravděpodobnou hrozbu pro soukromí nebo ochranu soukromých údajů. Maloobchodníci by však měli zdarma poskytnout snadné prostředky pro okamžitou či pozdější deaktivaci nebo odstranění těchto etiket.

13. Deaktivace nebo odstranění etiket neznamená omezení či zrušení právních povinností maloobchodníka nebo výrobce vůči spotřebiteli.

14. Body 11 a 12 platí pouze pro maloobchodníky, kteří jsou provozovateli aplikace.

Opatření k zvýšení informovanosti

15. Členské státy by měly ve spolupráci s odvětvím, Komisí a ostatními zúčastněnými stranami přijmout vhodná opatření s cílem informovat orgány veřejné správy a společnosti, zejména malé a střední podniky, a zvýšit jejich povědomí o možných přínosech a rizicích spojených s používáním technologie RFID. Zvláštní pozornost je nutno věnovat aspektům bezpečnosti informací a soukromí.

16. Členské státy by měly ve spolupráci s odvětvím, sdruženími občanské společnosti, Komisí a ostatními zúčastněnými stranami určit a poskytnout příklady osvědčených postupů při zavádění aplikací RFID s cílem informovat širokou veřejnost a zvýšit její povědomí o této záležitosti. Měly by rovněž přijmout vhodná opatření, například rozsáhlé pilotní projekty, ke zvýšení informovanosti veřejnosti o technologii RFID, jejích přínosech, rizicích a o důsledcích jejího používání jako předpoklad pro širší přijetí této technologie.

Výzkum a vývoj

17. Členské státy by měly spolupracovat s odvětvím, příslušnými zúčastněnými stranami z občanské společnosti a s Komisí s cílem podnítit a podpořit zavedení zásady „konstrukčního návrhu nenarušujícího bezpečnost a soukromí“ v počáteční fázi vývoje aplikací RFID.

Následná opatření

18. Členské státy by měly přijmout veškerá nezbytná opatření s cílem upozornit na toto doporučení všechny zúčastněné strany, které se podílejí na navrhování a provozování aplikací RFID ve Společenství.

19. Členské státy by měly nejpozději do 24 měsíců od vyhlášení tohoto doporučení v *Úředním věstníku Evropské unie* Komisi informovat o opatřeních přijatých v reakci na toto doporučení.

20. Do tří let od vyhlášení tohoto doporučení v *Úředním věstníku Evropské unie* Komise předloží zprávu o provádění tohoto doporučení, jeho účinnosti a dopadu na provozovatele a spotřebitele, zejména s ohledem na opatření, jež jsou doporučena v bodech 9 až 14.

Určení

21. Toto doporučení je určeno členským státům.

V Bruselu dne 12. května 2009.

Za Komisi

Viviane REDING

členka Komise

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 5, Elišky Peškové 14, tel./fax: 257 320 049, – Praha 4, Jihlavská 405, tel.: 261 260 414 – Brno, Česká 14, tel.: 542 213 962 – Ostrava, roh ul. Nádražní a Denisovy, tel.: 596 120 690 – České Budějovice, Česká 3, tel.: 387 319 045 a ve vybraných knihkupectvích. Distribuční podmínky předplatného: Jednotlivé částky jsou expedovány předplatitelům neprodleně po dodání z tiskárny. Objednávky nového předplatného jsou vyřizovány do 15 dnů a pravidelné dodávky jsou zahajovány od nejbližší částky po ověření úhrady předplatného, nebo jeho zálohy. Částky vyšlé v době od zaevidování předplatného do jeho úhrady jsou doposílány jednorázově. Změny adres a počtu odebíraných výtisků jsou prováděny do 15 dnů. Lhůta pro uplatnění reklamací je stanovena na 15 dnů od data rozeslání, po této lhůtě jsou reklamace vyřizovány jako běžné objednávky za úhradu. V písemném styku vždy uvádějte IČ (právnická osoba) a kmenové číslo předplatitele. Podávání novinových zásilek povoleno ŘPP Praha.

ISSN 1213-3442