# VĚSTNÍK
## ÚŘADU PRO OCHRANU OSOBNÍCH ÚDAJŮ
## 2006

**Částka 42** | **25. září 2006** | **Cena 26,– Kč**


## OBSAH

# ÚVOD

Částka 42 Věstníku Úřadu pro ochranu osobních údajů obsahuje přehled zrušených registrací za období od 20. 6. 2006 do 10. 9. 2006.

Součástí rubriky Sdělení Úřadu je informace o nové kompetenci, kterou Úřad získal v souvislosti s právní úpravou zákona č. 159/2006 Sb., o střetu zájmů, kterou byly upraveny podmínky týkající se omezení některých činností veřejných funkcionářů a neslučitelnosti výkonu funkce veřejného funkcionáře s jinými funkcemi.

Rubrika Sdělení přináší v oddíle *Úřad pro ochranu osobních údajů k problémům z praxe* příspěvek „K využívání adres z telefonního seznamu pro rozesílání dopisů s výzvou k zasílání příspěvků“. Úřad tímto materiálem informuje občany, jak mohou reagovat, jestliže byli takto osloveni, ale používání svého jména a adresy za účelem výzvy k zaslání příspěvku pociťují jako obtěžující pro svůj soukromý život.

Rubrika Sdělení dále obsahuje dvě stanoviska Pracovní skupiny pro ochranu dat podle článku 29 směrnice 95/46/ES.

# Přehled zrušených registrací

| Číslo registrace | Subjekt | Datum zrušení |
|---|---|---|
| 00000109/009 | DOPRAVNÍ PODNIK HL. M. PRAHY AKCIOVÁ SPOLEČNOST | 11. 8. 2006 |
| 00000109/011 | DOPRAVNÍ PODNIK HL. M. PRAHY AKCIOVÁ SPOLEČNOST | 11. 8. 2006 |
| 00000109/012 | DOPRAVNÍ PODNIK HL. M. PRAHY AKCIOVÁ SPOLEČNOST | 11. 8. 2006 |
| 00000109/023 | DOPRAVNÍ PODNIK HL. M. PRAHY AKCIOVÁ SPOLEČNOST | 11. 8. 2006 |
| 00000109/025 | DOPRAVNÍ PODNIK HL. M. PRAHY AKCIOVÁ SPOLEČNOST | 11. 8. 2006 |
| 00000109/035 | DOPRAVNÍ PODNIK HL. M. PRAHY AKCIOVÁ SPOLEČNOST | 11. 8. 2006 |
| 00000109/036 | DOPRAVNÍ PODNIK HL. M. PRAHY AKCIOVÁ SPOLEČNOST | 11. 8. 2006 |
| 00000109/038 | DOPRAVNÍ PODNIK HL. M. PRAHY AKCIOVÁ SPOLEČNOST | 11. 8. 2006 |
| 00001188/038 | UNILEVER ČR SPOL. S.R.O. | 28. 6. 2006 |
| 00001223/001 | DOPRAVNÍ PODNIK MĚST MOSTU A LITVÍNOVA, A.S. | 10. 8. 2006 |
| 00001302/002 | EUROTEL PRAHA, SPOL. S R.O. | 3. 8. 2006 |
| 00001302/003 | EUROTEL PRAHA, SPOL. S R.O. | 3. 8. 2006 |
| 00001302/004 | EUROTEL PRAHA, SPOL. S R.O. | 3. 8. 2006 |
| 00001302/005 | EUROTEL PRAHA, SPOL. S R.O. | 3. 8. 2006 |
| 00001302/006 | EUROTEL PRAHA, SPOL. S R.O. | 3. 8. 2006 |
| 00001302/007 | EUROTEL PRAHA, SPOL. S R.O. | 3. 8. 2006 |
| 00002562/001 | CEMOS OSTRAVA, A.S. | 20. 8. 2006 |
| 00004091/001 | ČESKOSLOVENSKÁ STÁTNÍ AUTOMOBILOVÁ DOPRAVA STÁTNÍ PODNIK ČESKÉ BUDĚJOVICE | 12. 7. 2006 |
| 00006647/004 | UNIVERZITA PARDUBICE | 11. 7. 2006 |
| 00006647/007 | UNIVERZITA PARDUBICE | 11. 7. 2006 |
| 00006647/008 | UNIVERZITA PARDUBICE | 11. 7. 2006 |
| 00010058/001 | PEGAS A.S. | 6. 7. 2006 |
| 00010235/001 | SEDLÁK JAROMÍR ING. | 23. 8. 2006 |
| 00013749/001 | OKD A.S. | 11. 7. 2006 |
| 00013749/002 | OKD A.S. | 11. 7. 2006 |
| 00013749/003 | OKD A.S. | 11. 7. 2006 |
| 00013749/004 | OKD A.S. | 11. 7. 2006 |
| 00019340/001 | MATEŘSKÁ ŠKOLA OLOMOUC-HOLICE, PŘÍSPĚVKOVÁ ORGANIZACE | 28. 6. 2006 |

# II. SDĚLENÍ ÚŘADU

## Úřad pro ochranu osobních údajů získal nové kompetence v oblasti ochrany soukromí

Parlament České republiky rozhodl, že s účinností od 1. ledna 2007 se do právního řádu začlení nová právní úprava podmínek týkajících se omezení některých činností veřejných funkcionářů a neslučitelnosti výkonu funkce veřejného funkcionáře s jinými funkcemi. Jde o **zákon č. 159/2006 Sb., o střetu zájmů.** V § 13 a 14 tohoto zákona se upravují podmínky pro vedení registru oznámení o činnostech, oznámení o majetku a oznámení o příjmech, darech a závazcích, které zabezpečují orgány zde uvedené a právo každého do registru nahlížet, a to i prostřednictvím veřejné datové sítě, a pořizovat si z něj výpisy a opisy.

Fyzická osoba, která informace z registru použije nebo dále zpracuje k jinému účelu, nežli zjištění případného střetu zájmů při výkonu funkce veřejného funkcionáře [§ 23 písm. a)], nebo poruší povinnost mlčenlivosti podle § 14 odst. 3 tohoto zákona; tj. o skutečnostech, o nichž se dozvěděla z údajů v registru, nebo o osobách, které sdělily skutečnosti nasvědčující nepravdivosti nebo neúplnosti údajů [§ 23 písm. b)], spáchá přestupek, k jehož projednání je kompetentní Úřad pro ochranu osobních údajů a za nějž lze uložit pokutu až do výše 100.000 Kč.

O porušení povinností veřejných funkcionářů, které ze zákona vyplývají, rozhodují soudy ve správním soudnictví.

# ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ K PROBLÉMŮM Z PRAXE

## č. 1/2006

srpen 2006

**K využívání adres z telefonního seznamu pro rozesílání dopisů s výzvou k zasílání příspěvků**

Úřad pro ochranu osobních údajů (dále jen „Úřad“) obdržel již několik žádostí o vyjádření z hlediska zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, v platném znění (dále jen „zákon o ochraně osobních údajů“), k možnosti využívání adres získaných z telefonního seznamu pro rozesílání dopisů s výzvou k zaslání příspěvku na projekty veřejně prospěšné společnosti.

Jestliže jsou údaje o jménu a adrese fyzické osoby získány z telefonního seznamu nebo jiného zpracování osobních údajů, které je veřejně přístupné na základě zvláštního právního předpisu, jde o údaje oprávněně zveřejněné, které lze podle § 5 odst. 2 písm. d) zákona o ochraně osobních údajů zpracovávat bez souhlasu subjektu údajů. Pokud jsou uvedené osobní údaje získány z veřejného seznamu za účelem nabízení obchodu nebo služeb subjektu údajů, řídí se jejich používání pro tento účel ustanoveními § 5 odst. 5 – 10 zákona o ochraně osobních údajů. Tato ustanovení umožňují i vyjádření písemného nesouhlasu se zpracováním adresních údajů pro tento účel.

Pokud se však nejedná o nabízení obchodu nebo služeb, ale o žádost o finanční příspěvek, je nutno vycházet pouze z druhé věty § 5 odst. 2 písm. d) zákona o ochraně osobních údajů, která pro zpracování oprávněně zveřejněných údajů bez souhlasu subjektu údajů stanoví, že tím není dotčeno právo na ochranu soukromého a osobního života subjektu údajů. Bude-li některá z takto oslovených osob používání jména a adresy za účelem výzvy k zaslání příspěvku pociťovat jako obtěžující pro její soukromý život, má možnost postupovat podle § 21 odst. 1 zákona o ochraně osobních údajů, který říká: „Každý subjekt údajů, který zjistí nebo se domnívá, že správce nebo zpracovatel provádí zpracování jeho osobních údajů, které je v rozporu s ochranou soukromého a osobního života subjektu údajů nebo v rozporu se zákonem, zejména jsou-li osobní údaje nepřesné s ohledem na účel jejich zpracování, může

a) požádat správce nebo zpracovatele o vysvětlení,

b) požadovat, aby správce nebo zpracovatel odstranil takto vzniklý stav. Zejména se může jednat o blokování, provedení opravy, doplnění nebo likvidaci osobních údajů.“

Podle výše citovaného ustanovení § 21 zákona o ochraně osobních údajů mohou oslovené osoby písemně požadovat, aby jim tyto žádosti nebyly dále zasílány a jejich údaje nebyly pro tento účel používány. Pokud by jejich žádostem ze strany zasílatele nebylo vyhověno, pak se mohou obrátit se stížností na Úřad, který by posoudil, zda je praktikovaným způsobem zpracování osobních údajů v konkrétním případě dotčeno právo na ochranu soukromého a osobního života subjektu údajů.

PRACOVNÍ SKUPINA PRO OCHRANU DAT PODLE ČLÁNKU 29

2130/05/CS
WP 115

# Stanovisko č. 5/2005 k používání lokalizačních údajů v souvislosti s poskytováním služeb s přidanou hodnotou

Přijato dne 25. listopadu 2005

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

Sekretariát poskytuje Evropská komise, Generální ředitelství pro spravedlnost, svobodu a bezpečnost, Ředitelství C (Občanská spravedlnost, práva a občanství), B-1049 Brusel, Belgie, Úřadovna č. LX-46 01/43.

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

PRACOVNÍ SKUPINA PRO OCHRANU FYZICKÝCH OSOB PŘI ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

ustavená směrnicí Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995, s ohledem na čl. 29, čl. 30 odst. 1 písm. a) a čl. 30 odst. 3) výše uvedené směrnice a čl. 15 odst. 3 směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002,

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

PŘIJALA TOTO STANOVISKO:

Pracovní skupina by ráda upozornila, že otázky týkající se používání lokalizačních údajů jsou velmi aktuální. Tyto údaje jsou definovány jako „jakékoli údaje zpracovávané v síti elektronických komunikací, které určují zeměpisnou polohu koncového zařízení uživatele veřejně dostupné služby elektronických komunikací“ (článek 2 směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací).

## Souvislosti a účel

Za posledních 20 let došlo k výraznému nárůstu v používání lokalizačních údajů, a to díky dvěma hlavním faktorům.

Prvním faktorem je prudký nárůst používání satelitních lokalizačních údajů, které dnes mohou být nesmírně přesné a často velmi cenné, zvláště v případech pomoci jednotlivcům v tísni[1)]. Tyto systémy jsou však dostupné pouze těm, kteří jsou vybaveni odpovídajícími koncovými zařízeními.

Druhým faktorem je nevídané rozšíření mobilních telefonů, kdy každý uživatel s sebou neustále nosí přístroj, prostřednictvím kterého může být potenciálně lokalizován.

Obecně řečeno, existuje mnoho způsobů lokalizace fyzických osob převážně využívajících „stopy“ zanechané po používání nových technologií: Automatů na jízdenky v odvětví dopravy, GPS, bankovních karet či elektronických peněženek nebo v daném případě mobilních telefonů. Zpočátku byly lokalizační údaje považovány za údaje čistě technické, nezbytné pro volání na mobilní telefony nebo z mobilních telefonů, a byly dostupné pouze operátorům elektronických komunikací. V této souvislosti se používá termín „provozní údaje“. Tyto údaje jsou pouze výsledkem používání dané technologie a nijak se neliší od jiných denně zanechávaných „stop“.

Jelikož však lokalizační údaje poskytují klíčové informace o fyzické osobě (stručně řečeno, kdo je kde), začaly být brzy považovány za potenciální zdroj příjmu. Firmy vyvinuly řadu služeb založených na těchto údajích.

První takové služby nabízely jednotlivcům informace například o jim nejblíže položené lékárně nebo restauraci. Následně byly služby založené na jednorázovém použití lokalizačních údajů (poskytující informace v daném časovém okamžiku) doplněny o služby založené na nepřetržitém využívání těchto údajů (navigační pomoc).

První fázi vystřídala fáze druhá, kdy se rozvíjejí služby, které již nejsou založeny na lokalizaci lidí na jejich vlastní žádost (uživatelů, kteří sami chtějí využít nějaké služby), ale na jejich lokalizaci jinými osobami (na žádost třetí strany). Rozvinuly se služby sledování a hledání, díky nimž je možné jednotlivce lokalizovat prostřednictvím jejich mobilních telefonů, i když je zrovna nepoužívají, ovšem za předpokladu, že jsou tyto mobilní telefony zapnuté.

Klíčové téma zpracování lokalizačních údajů se tedy posunulo od otázky uchovávání (v podstatě: Za jakých podmínek by měli operátoři elektronických komunikací lokalizační údaje uchovávat?), k otázce jejich používání (Jak můžeme zajistit, aby byly údaje používány k poskytování služeb s přidanou hodnotou v souladu se zásadami platnými pro zpracování osobních údajů?).

## Právní rámec

Jelikož se lokalizační údaje vždy týkají identifikované nebo identifikovatelné fyzické osoby, podléhají ustanovením o ochraně osobních údajů stanovených směrnicí 95/46/ES ze dne 24. října 1995.

---

[1)] *Satelitní geolokalizaci v současné době nabízí pouze GPS (globální polohový systém) vytvořený armádou USA, jehož výsledky byly dány k dispozici pro civilní účely, především pro námořní navigaci. Lokalizační údaje se vypočítávají pomocí triangulace a jsou odesílány přímo osobě, která má přijímač GPS. Pak mohou být prostřednictvím sítě elektronických komunikací (kombinace GPS/GSM) odesílány třetí straně.*

Vzhledem k tomu, že je zpracování těchto údajů zvláště citlivou záležitostí zahrnující klíčovou otázku svobody anonymního pohybu, přijaly evropské zákonodárné orgány, s ohledem na úvahy evropských orgánů pro ochranu údajů, zvláštní pravidla vyžadující získání souhlasu uživatelů nebo účastníků dříve, než dojde ke zpracování lokalizačních údajů nezbytných k poskytování služby s přidanou hodnotou, a aby byli uživatelé a účastníci informováni o podmínkách takového zpracování (článek 9 směrnice 2002/58/ES ze dne 12. července 2002).

Článek 2 směrnice 2002/58/ES definuje provozní údaje jako *„jakékoli údaje zpracovávané pro účely přenosu sdělení sítí elektronických komunikací nebo pro jeho účtování“* a lokalizační údaje jako *„jakékoli údaje zpracovávané v síti elektronických komunikací, které určují zeměpisnou polohu koncového zařízení uživatele veřejně dostupné služby elektronických komunikací.“*

Výše uvedené dvě směrnice sice stanoví uspokojivý rámec pro zpracování lokalizačních údajů, ale Pracovní skupina by ráda vysvětlila, jak by měla být některá jejich ustanovení používána, a zdůraznila zvláštní aspekty některých nabízených služeb.

Toto stanovisko se nezabývá podmínkami pro zpracování lokalizačních údajů podle článku 13 směrnice 95/46/ES a článku 15 směrnice 2002/58/ES, tzn. kdy se lokalizační údaje zpracovávají způsobem, který představuje výjimku ze zásad stanovených těmito směrnicemi, což je v demokratické společnosti nezbytné, přiměřené a úměrné opatření pro zajištění národní bezpečnosti, obrany, veřejné bezpečnosti a pro prevenci, vyšetřování, odhalování a stíhání trestných činů. Vzhledem k významu této záležitosti vyjádřila Pracovní skupina své názory již při několika příležitostech[2)].

## 1. Všeobecné podmínky, kterými se řídí používání lokalizačních údajů pro poskytování služeb s přidanou hodnotou

Pracovní skupina zdůrazňuje, že při zpracovávání osobních údajů musejí různé strany zainteresované na poskytování služeb s přidanou hodnotou založených na používání lokalizačních údajů, ať se jedná o operátory elektronických komunikací, kteří zpracovávají lokalizační údaje, nebo třetí strany, které poskytují služby s přidanou hodnotou vycházející z lokalizačních údajů, jež jim zasílají operátoři, plnit své povinnosti stanovené právními předpisy na ochranu osobních údajů.

### *1.1 Použitelné vnitrostátní právo*

Pracovní skupina zaznamenala rozvoj služeb s přidanou hodnotou založených na zpracování lokalizačních údajů ze služeb elektronických komunikací, poskytují je ale firmy (např. prostřednictvím internetu), které nejsou usazeny na území dotčeného jednotlivce, tzn. subjektu údajů.

Podle článku 3 směrnice 2002/58/ES se tato směrnice vztahuje na zpracování osobních údajů ve spojení s poskytováním veřejně dostupných služeb elektronických komunikací ve veřejných komunikačních sítích ve Společenství. Podle článku 4 směrnice 95/46/ES je použitelným vnitrostátním právem právo členského státu, kde je správce usazen. Toto ustanovení znamená, že ve Společenství podléhá zpracování lokalizačních údajů vnitrostátnímu právu členského státu, v němž je správce usazen, a nikoli členského státu, jehož je subjekt údajů státním příslušníkem.

Pokud není správce (poskytovatel služby s přidanou hodnotou) usazen v členském státě, mohou operátoři elektronických komunikací lokalizační údaje správci předávat pouze za podmínek stanovených v kapitole IV směrnice 95/46/ES o předávání osobních údajů do třetích zemí. Tyto podmínky zahrnují požadavek, aby zákony na ochranu údajů v dané třetí zemi podle Evropské komise zajišťovaly odpovídající úroveň ochrany, nebo aby předávání údajů bylo založeno na jiném legitimním základě – především na souhlasu subjektu údajů, existenci smlouvy uzavřené v zájmu subjektu údajů, existenci vyššího veřejného zájmu, zjištění nebo obraně právních nároků nebo na nutnosti chránit životně důležité zájmy subjektu údajů.

### *1.2 Informování subjektů údajů*

Pracovní skupina by ráda zdůraznila, že směrnice 95/46/ES (článek 10) a 2002/58/ES (články 6 a 9) vyžadují, aby byly subjektům lokalizačních údajů, které mají být zpracovány, sděleny tyto informace:

- totožnost správce a popřípadě jeho zástupce,
- účely zpracování,
- druh zpracovávaných lokalizačních údajů,
- doba trvání zpracování,
- zda budou údaje předány třetí straně za účelem poskytování služby s přidanou hodnotou,
- právo na přístup k údajům a právo na jejich opravu,
- právo uživatelů vzít svůj souhlas se zpracováním údajů kdykoli zpět nebo zpracování takových údajů dočasně odmítnout a podmínky, za nichž lze toto právo vykonávat,
- právo údaje zrušit.

---

2) *Viz doporučení 2/99 o respektování soukromí v kontextu zachycování telekomunikací; Stanovisko 7/2000 k návrhu Evropské komise směrnice Evropského parlamentu a Rady o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací ze dne 12. července 2000, KOM(2000) 385; Stanovisko 4/2001 k návrhu Rady Evropy Úmluvy o kyberkriminalitě; Stanovisko 10/2001 k potřebě vyváženého přístupu v boji proti terorismu; Stanovisko 5/2002 k Prohlášení evropských komisařů pro ochranu údajů na Mezinárodní konferenci v Cardiffu (9. - 11. září 2002) o povinném systematickém uchovávání telekomunikačních provozních údajů; Stanovisko 1/2003 k uchovávání provozních údajů pro účely účtování a Stanovisko 9/2004 k návrhu rámcového rozhodnutí o ukládání údajů zpracovávaných a uchovávaných pro účely poskytování veřejně dostupných služeb elektronických komunikací nebo údajů dostupných v sítích veřejných komunikací s ohledem na prevenci, vyšetřování, odhalování a stíhání trestných činů, včetně terorismu. [Návrh předložila Francie, Irsko, Švédsko a Velká Británie (dokument Rady 8958/04 ze dne 28. dubna 2004)].*

Pracovní skupina zastává názor, že tyto informace by měla poskytovat strana shromažďující lokalizační údaje ke zpracování, tzn. poskytovatel služby s přidanou hodnotou, nebo, pokud není poskytovatel v přímém kontaktu se subjektem údajů, operátor elektronických komunikací.

Informace by mohly být poskytovány buď v rámci všeobecných podmínek služby s přidanou hodnotou, nebo přímo pokaždé, když je služba využívána. S ohledem na velmi citlivou povahu zpracování lokalizačních údajů by Pracovní skupina poskytovatele služeb ráda upozornila na potřebu poskytovat jasné, úplné a komplexní informace o vlastnostech navrhované služby.

Pokud jsou informace poskytovány v rámci všeobecných podmínek dané služby, Pracovní skupina doporučuje, aby poskytovatel služby dotčeným jednotlivcům nabízel možnost si informace znovu prostudovat kdykoli a snadným způsobem, např. prostřednictvím internetových stránek nebo při využívání služby (např. zavoláním na určené číslo).

*1.3 Souhlas*

Získání souhlasu

V souladu s běžnou praxí při provádění ochrany osobních údajů, když se zpracovávají citlivé údaje, evropské právní předpisy vyžadují, aby byl souhlas se zpracováním lokalizačních údajů odlišných od provozních údajů získán předem.

Pracovní skupina by proto ráda objasnila podmínky získání souhlasu.

Čl. 2 písm. h) směrnice 95/46/ES definuje souhlas jako „jakýkoli výslovný, svobodný a vědomý projev vůle, kterým subjekt údajů dává své svolení k tomu, aby osobní údaje, které se jej týkají, byly předmětem zpracování".

Tato definice výslovně vylučuje, aby byl dáván souhlas jako součást přijetí všeobecných podmínek nabízené služby elektronických komunikací. V tomto ohledu je možné odkázat na vysvětlení, které poskytla Pracovní skupina zřízená podle článku 29 ve svém stanovisku č. 5/2004 k nevyžádaným sdělením pro účely přímého marketingu, což je v tomto kontextu zvláště důležité.

V závislosti na typu nabízené služby se však může souhlas vztahovat na určité činnosti nebo může představovat dohodu o průběžné lokalizaci.

Nabízení služby, která vyžaduje automatickou lokalizaci jednotlivce (např. možnost zavolání na konkrétní číslo pro získání informací o povětrnostních podmínkách v místě, kde se dotčená osoba nachází), je přijatelné za předpokladu, že jsou uživatelé v plném rozsahu předem informováni o zpracování jejich lokalizačních údajů. V tomto případě by se zavolání na příslušné číslo považovalo za souhlas s lokalizací.

Poskytovatelé, kteří musejí získat souhlas subjektu údajů

Služba s přidanou hodnotou založená na lokalizačních údajích může být poskytována buď přímo operátorem elektronických komunikací (dotčená fyzická osoba kontaktuje operátora, který pak službu poskytne na základě lokalizačních údajů získaných ze svého systému), nebo prostřednictvím třetí strany (dotčená fyzická osoba kontaktuje třetí stranu, která pak službu poskytne na základě lokalizačních údajů získaných od operátora). V tomto druhém případě je to poskytovatel služby, kdo musí získat souhlas subjektu údajů. S výjimkou případů, kdy jsou lokalizační údaje generovány samotným koncovým zařízením, je nutné, aby operátoři třetí straně na její žádost systematicky zasílali lokalizační údaje o identifikované fyzické osobě (osobě, která kontaktovala třetí stranu, aby mohla využít dané služby).

S ohledem na zvýšení počtu poskytovatelů služeb Pracovní skupina konstatuje, že vysokého stupně ochrany zpracování osobních lokalizačních údajů by mohlo být dosaženo, pokud by operátoři požadavky při využívání služby s přidanou hodnotou založené na lokalizačních údajích (zákazníků volajících na číslo spravované operátorem) shromažďovali centrálně a předávali je třetím stranám odpovědným za poskytování dotčené služby tak, aby poskytovatel služby nemohl určit totožnost zákazníka (např. používáním falešných jmen[3]). Tímto způsobem by mohl poskytovatel služby požadovanou službu poskytnout (např. jméno nejbližší restaurace) prostřednictvím operátora, aniž by byl schopen určit totožnost osoby, která si službu vyžádala.

Pracovní skupina rovněž konstatuje, že také zařízení koncového uživatele by mohlo poskytovat vysoký stupeň ochrany díky vlastní vestavěné funkci lokalizace. Lokalizační údaje pak mohou být zpracovány systémem řízení identity tak, že jsou četným poskytovatelům služeb předávány pouze pseudonymy. Alternativně by s ohledem na stále se rozvíjející šířku pásma a paměti mobilních telefonů mohly přístroje koncových uživatelů např. stáhnout kompletní seznam restaurací ve městě a lokálně v tomto seznamu vyhledávat s využitím nejen lokalizačních údajů, ale také preferencí uživatele (francouzská kuchyně, vegetariánské menu atd.). Těmito příklady Pracovní skupina zdůrazňuje potřebu uvažovat o technologiích na podporu soukromí jako o účinných a doplňujících prvcích při poskytování vysokého a uspokojivého stupně ochrany pro uživatele geolokalizačních služeb.

V každém případě by Pracovní skupina operátory ráda upozornila na potřebu zavádět efektivní opatření k ověřování a potvrzování žádostí o přístup k lokalizačním údajům třetích stran, které nabízejí službu s přidanou hodnotou.

Opatření k zajištění platnosti souhlasu

Pracovní skupina zastává názor, že poskytovatelé služby s přidanou hodnotou musejí při získávání souhlasu přijmout vhodná opatření, aby bylo zajištěno, že osoba, jíž se lokalizační údaje týkají, je totožná s osobou, která poskytla souhlas. Pokud jsou lokalizační údaje zpracovávány průběžně (např. služby jako *seznamka*), musí poskytovatel služby:

- potvrdit objednání služby odesláním zprávy na koncové zařízení uživatele, jakmile obdrží souhlas, a
- v případě potřeby požadovat potvrzení objednávky.

[3] *„Falešným jménem" se rozumí technické údaje umožňující poskytovateli služby poskytnout službu odpovídající lokalizačním údajům fyzické osoby, aniž by byl schopen danou osobu identifikovat podle jména; pouze operátor je schopen propojit falešné jméno s dotčenou fyzickou osobou.*

Tento postup má pomoci zabránit podvodnému objednání služby bez vědomí fyzické osoby (dočasné odebrání koncového zařízení osoby, aby mohlo dojít k objednání služby).

Osoba, jejíž souhlas je vyžadován

Článek 6 a článek 9 směrnice 2002/58/ES odkazuje na souhlas uživatelů nebo účastníků. Pracovní skupina zastává názor, že pokud je služba poskytována soukromým fyzickým osobám, je nutné získat souhlas osoby, které se údaje týkají, tzn. uživatele koncového zařízení.

*1.4 Uplatnění práva vzít souhlas zpět*

Podle článku 9 směrnice 2002/58/ES mohou lidé, kteří poskytli souhlas se zpracováním lokalizačních údajů odlišných od provozních údajů, svůj souhlas vzít kdykoli zpět a musejí mít možnost jednoduchým způsobem a zdarma dočasně odmítnout zpracování těchto údajů.

Pracovní skupina považuje tato práva, která lze považovat za provádění práva vznést námitku proti zpracování lokalizačních údajů, za zásadní vzhledem k citlivé povaze lokalizačních údajů.

Pracovní skupina se domnívá, že základním předpokladem uplatňování těchto práv je, aby byli jednotlivci informováni, a to nejen ve chvíli, když si službu objednávají, ale také když službu využívají. Pokud služba vyžaduje průběžné zpracování lokalizačních údajů, zastává Pracovní skupina názor, že poskytovatel služby by měl dotčenému jednotlivci pravidelně připomínat, že jeho koncové zařízení bylo, bude nebo může být lokalizováno. To takové osobě umožní uplatnit právo vzít svůj souhlas zpět podle článku 9 směrnice 2002/58/ES, pokud tak bude chtít učinit.

*1.5 Doba uchovávání údajů*

Lokalizační údaje mohou být zpracovávány pouze „po dobu nezbytnou pro poskytování služeb s přidanou hodnotou“ (čl. 9 odst. 1 směrnice 2002/58/ES).

To znamená, že jakmile je jednou služba poskytnuta, nesmí poskytovatel v zásadě dále uchovávat lokalizační údaje jednotlivců, pokud nejsou nezbytné pro účely účtování a platby za propojení[4)].

Pokud chtějí poskytovatelé služby uchovávat záznamy o poloze uživatelů své služby, musejí být údaje nejdříve anonymizovány.

*1.6 Bezpečnostní opatření a předávání třetím stranám*

Pracovní skupina by operátory elektronických komunikací a poskytovatele služeb s přidanou hodnotou založených na zpracování lokalizačních údajů ráda upozornila na požadavek zavést bezpečnostní opatření k zajištění důvěrnosti a neporušenosti zpracovávaných lokalizačních údajů.

Podle čl. 9 odst. 3 směrnice 2002/58/ES nesmějí být lokalizační údaje, které mají být zpracovány k poskytnutí služby s přidanou hodnotou, předávány jiným třetím stranám než těm, které službu s přidanou hodnotou poskytují. Pouze osoby jednající z pověření třetí strany poskytující službu s přidanou hodnotou smějí zpracovávat tyto údaje, v rozsahu a po dobu nezbytnou k poskytnutí služby. Přístupy takových osob k lokalizačním údajům by rovněž měly být logovány.

**2. Podmínky zavedení určitých lokalizačních služeb s ohledem na jejich účel**

Kromě dodržení konkrétních ustanovení uvedených ve směrnici 2002/58/ES musejí lokalizační služby, protože využívají osobní údaje, splňovat požadavky článku 6 směrnice 95/46/ES, který stanoví, že osobní údaje mohou být použity pouze „pro stanovené účely, výslovně vyjádřené a legitimní“. Pracovní skupina by proto ráda probrala podmínky, za kterých mohou být zavedeny určité lokalizační služby, zvláště s ohledem na jejich účel.

*2.1 Lokalizace nezletilých*

Pracovní skupina zaznamenala rozvoj lokalizačních služeb určených pro rodiče, které rodičům například umožní připojit se na internetové stránky a ověřit si polohu svých dětí, které vybavili mobilním telefonem. Tento typ služby vyvolává řadu problémů spojených především s potřebou dosáhnout rovnováhy mezi různými zájmy a příslušnými právy s tím spojenými.

Služba, pomocí níž lze děti lokalizovat prostřednictvím mobilního telefonu, by mohla splnit přání některých rodičů.

Mediální zpravodajství o trestných činech týkajících se dětí, potřeba monitorovat děti postižené určitými nemocemi nebo stále „kočovnější“ životní styl mohou některé rodiče vést ke snaze se „uklidňovat“ tím, že mají možnost lokalizovat své děti, aniž by jim museli přímo volat. Tento nový způsob používání mobilního telefonu ve prospěch rodičů, a na jejich vlastní náklady, může být považován za jistý druh rodinné „smlouvy“: Větší nezávislost komunikace pro dítě výměnou za možnost být rodičem lokalizován.

V tomto ohledu mohou tyto služby uspokojit zjištěnou moderní „potřebu“ a odrazit touhu poskytovatelů služeb prosadit se na trhu, který se bude pravděpodobně rozšiřovat a který představuje nový příklad toho, jak lze možnosti, jež nabízejí lokalizační údaje, prodat.

Stejně tak však můžeme na tuto službu nahlížet i z druhé strany: Nikoli z pohledu rodiče, ať už je tento pohled jakkoli pochopitelný, ale z pohledu dítěte.

Pracovní skupina by ráda připomněla, že články 3 a 18 Mezinárodní úmluvy o právech dítěte uvádí, že při jakémkoli rozhodování týkajícím se dětí „musejí být nejlepší zájmy dítěte předním hlediskem“. V uvedeném případě je zapotřebí vzít v potaz, že článek 16 Úmluvy stanoví, že „žádné dítě nesmí být vystaveno svévolnému nebo nezákonnému zasahování do svého soukromého života, rodiny, domova nebo korespondence“.

Řada otázek vyvstává v souvislosti s využíváním tohoto druhu služby, která by mohla narušit normální vztahy důvěry mezi rodiči a jejich dětmi a bránit dětem získat si od rodičů nezbytný odstup, jak se postupně stávají nezávislejšími.

---

4) *V této souvislosti Pracovní skupina odkazuje na své doporučení o uchovávání provozních údajů pro účely účtování (Stanovisko 1/2003 ze dne 29. ledna 2003).*

Nemohl by navíc takový systém zcela zvráceně způsobit, že někteří rodiče se vzdají své zodpovědnosti a budou žít v iluzi, že mají nad činnostmi svých dětí kontrolu, nebo je alespoň sledují? Nepřispěje ze společenského hlediska vývoj tohoto typu k tomu, že si jednotlivci od velmi mladého věku budou zvykat na téměř trvalou formu sledování, kterou již nebudou ani vnímat jako dotěrnou?

A konečně existuje riziko, že rodiče budou zaměňovat informaci o tom, kde se nachází mobilní telefon jejich dítěte, s informací o tom, co jejich dítě ve skutečnosti dělá.

Pracovní skupina proto alespoň vyzývá k opatrnosti při používání tohoto typu služby a zdůrazňuje, že musejí být prováděny v souladu s pravidly pro zpracování lokalizačních údajů a v souladu se zvláštními vnitrostátními právními předpisy s ohledem na věk dotčených nezletilých.

Poskytovatelé služeb tedy musejí zavést vhodné postupy k identifikaci osob, které se registrují jako rodiče, a k omezení přístupu těchto osob ke službě.

Navíc vyvstává otázka souhlasu nezletilého s tím, aby byl subjektem požadavku na lokalizaci.

V této souvislosti Pracovní skupina upozorňuje, že v okamžiku, kdy je vznesen požadavek na lokalizaci, není možné ověřit, zda osoba, která telefon používá, je dotčený nezletilý a nikoli jiná osoba, např. dospělý, kterému účastník služby příslušný telefon svěřil. Proto doporučuje, aby byl získán souhlas uživatele telefonu, a to alespoň v okamžiku objednání služby. Aby se zamezilo podvodné registraci telefonů, měli by poskytovatelé služeb například posílat na příslušný telefon zprávy uvádějící, že je subjektem požadavku na lokalizaci tak, aby uživatel mohl uplatnit právo vzít svůj souhlas zpět v souladu s článkem 9 směrnice 2002/58/ES.

*2.2 Lokalizace zaměstnanců*

Pracovní skupina se již zabývala otázkou zpracování osobních údajů v pracovněprávním kontextu[5)]. Zdůraznila, že dohled nad pracovníky musí probíhat co nejméně dotěrným způsobem.

Zpracování údajů, které zaměstnavateli umožní shromažďovat údaje o poloze zaměstnance, buď přímo (poloha samotného zaměstnance) nebo nepřímo (poloha vozidla, které zaměstnanec používá, nebo výrobku či majetku, který mu byl svěřen), zahrnuje používání osobních údajů a podléhá ustanovením směrnice 95/46/ES.

Pracovní skupina zaznamenala vývoj systémů, které firmám umožňují určit zeměpisnou polohu svých zaměstnanců v určitém časovém okamžiku nebo nepřetržitě lokalizací objektů v jejich držení (jmenovka, mobilní telefon atd.) či užívání (vozidla).

Tyto informace mohou být založeny na zpracování údajů ze satelitů (GPS), ze sítí elektronických komunikací (mobilní telefony, síť WiFi) nebo z jakéhokoli jiného zařízení (např. RFID etiketa lokalizovaná čtečkou). Stále častěji jsou doplňovány údaji z různých snímačů, které nejsou lokalizační údaje v užším smyslu, např. údaje o době používání stroje nebo vozidla, počtu ujetých kilometrů nebo rychlosti, kterou se vozidlo pohybuje.

Toto zpracování vyvolává dvě otázky: Kde je dělící čára mezi pracovním a soukromým životem a jaký stupeň sledování a trvalého dohledu je vůči zaměstnanci přijatelný?

Z hlediska ochrany údajů by Pracovní skupina ráda připomněla, že zákonnost těchto operací zpracování údajů by se neměla opírat pouze o souhlas zaměstnance, který musí být v souladu se směrnicí „svobodný". Jak již Pracovní skupina upozornila ve svém pracovním dokumentu o ochraně údajů v pracovněprávním kontextu, měla by být otázka souhlasu řešena v širším zorném úhlu; zvláště zapojení všech příslušných zainteresovaných stran (jak předpokládají právní předpisy několika členských států) prostřednictvím kolektivních smluv by mohlo být vhodným způsobem regulace získávání souhlasu za těchto okolností.

Vzhledem k požadavku, aby údaje byly zpracovávány jen pro stanovené účely, je Pracovní skupina toho názoru, že zpracování lokalizačních údajů o zaměstnancích musí odpovídat určité potřebě příslušné části firmy, která je spojena s její činností. Zpracování lokalizačních údajů může být odůvodněné v případech, kdy slouží pro monitorování přepravy osob či zboží nebo k lepší distribuci zdrojů u služeb v rozptýlených lokalitách (např. pro plánování operací v reálném čase), nebo v případech, kdy je účelem bezpečnost samotného zaměstnance nebo jemu svěřeného zboží či vozidel.

Pracovní skupina naopak považuje zpracování údajů za nadbytečné v případech, kdy si mohou zaměstnanci své cesty volně organizovat dle vlastního uvážení, nebo v případech, kdy je účelem zpracování údajů pouze sledování práce zaměstnance, která by mohla být sledována jiným způsobem. V těchto dvou případech daným účelem nelze odůvodnit zpracování údajů nesporně zasahující do soukromí vzhledem k typu shromažďovaných údajů. To je ještě umocněno existencí vnitrostátních právních předpisů výslovně zakazujících sledování zaměstnanců na dálku z důvodu hodnocení jejich výkonu.

V každém případě požadavek účelu znamená, že by zaměstnavatel neměl shromažďovat lokalizační údaje týkající se zaměstnance mimo jeho pracovní dobu. Pracovní skupina proto doporučuje, aby bylo vybavení, které mají zaměstnanci k dispozici, zvláště firemní vozidla, a které může být využíváno i k soukromým účelům, opatřeno systémem umožňujícím zaměstnancům funkci lokalizace vypnout.

Lokalizační údaje týkající se zaměstnance musejí být uloženy po dobu nezbytnou z hlediska předem uvedeného účelu odůvodňujícího zpracovaní těchto údajů. Vzhledem k možným stanoveným účelům odůvodňujícím zpracování lokalizačních údajů bude zpracování v podstatě probíhat v reálném čase. V každém případě Pracovní skupina doporučuje, aby byla doba uchovávání lokalizačních údajů přiměřená, tzn. maximálně dva měsíce.

Pokud zaměstnavatel chce lokalizační údaje zpracovávat po dobu delší než dva měsíce (např. za účelem získání historických záznamů o cestách s cílem optimalizovat trasy), Pra-

---

5) *Stanovisko 8/2001 ze dne 13. září 2001 ke zpracování osobních údajů v pracovněprávním kontextu.*

covní skupina doporučuje, aby byly údaje nejdříve anonymizovány.

Přístup k lokalizačním údajům musí být omezen na osoby, které do nich smějí při plnění svých povinností s ohledem na jejich účel legitimně nahlížet. Zaměstnavatelé proto musejí podniknout veškeré nezbytné kroky k zabezpečení těchto údajů a k zabránění neoprávněnému přístupu k nim, zvláště zavedením opatření k ověřování a identifikaci.

Na závěr Pracovní skupina zdůrazňuje povinnost informovat dotčené zaměstnance a upozorňuje firmy na nutnost zavádět lokalizační systémy tak, aby si zaměstnanci byli vědomi jejich existence.

V Bruselu, dne 25. listopadu 2005

Za Pracovní skupinu
předseda
Peter SCHAAR

Poznámka: Dokument je také k dispozici na internetové adrese http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_cs.pdf .

PRACOVNÍ SKUPINA PRO OCHRANU DAT PODLE ČLÁNKU 29

00451/06/CZ
WP 118

# Stanovisko č. 2/2006 k problematice ochrany soukromí v kontextu poskytování služeb spočívajících ve screeningu elektronické pošty

Přijato dne 21. února 2006

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

Služby sekretariátu poskytuje ředitelství C (Občanská spravedlnost, práva a občanství) Evropské komise, Generální ředitelství pro spravedlnost, svobodu a bezpečnost, B-1049 Brusel, Belgie, kancelář č. LX-46 01/43.

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

PRACOVNÍ SKUPINA PRO OCHRANU FYZICKÝCH OSOB PŘI ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ,

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

s ohledem na článek 29, čl. 30 odst. 1 písm. c) a čl. 30 odst. 3 uvedené směrnice,

s ohledem na svůj jednací řád, a zejména na jeho články 12 a 14,

PŘIJALA TOTO STANOVISKO:

## I. ÚVOD

Pracovní skupina zřízená podle článku 29 směrnice 95/46/ES si je vědoma mimořádného rozvoje různých komunikačních služeb poskytovaných on-line, k nimž patří i bezplatné služby elektronické pošty dostupné na internetu a další související služby. Rozvoj elektronických komunikačních služeb nastoluje řadu otázek souvisejících s ochranou práva na soukromí při komunikaci, především co se týče skutečně používaných metod a postupů kontroly komunikací, jejichž cílem je odstraňovat případnou nežádoucí poštu (tzv. „spamy“) a viry a zjišťovat určitý předem určený obsah.

Pracovní skupina si je vědoma skutečnosti, že většina poskytovatelů internetových služeb („ISP“) a poskytovatelů služeb elektronické pošty („ESP“) používá tzv. filtry k ochraně sítí a zařízení, a (v menším počtu případů) ke kontrole komunikací prováděné z komerčních důvodů. Pracovní skupina však zastává názor, že by použití těchto filtrů mohlo být v určitých případech v rozporu s platnými právními předpisy o ochraně údajů, jejichž přehled je podán v dalším textu. Tento rozpor by mohl být způsoben mimo jiné tím, že v některých případech není jasné, jak se zmíněné právní předpisy uplatní v souvislosti s těmito novými formami služeb.

Toto stanovisko má především poskytnout určité pokyny týkající se důvěrnosti komunikace prostřednictvím elektronické pošty a zejména otázek filtrování komunikací uskutečňovaných on-line.V této souvislosti vyvstává především otázka, zda skenování komunikací prováděné poskytovateli ISP a/nebo ESP k dosažení nejrůznějších cílů představuje zachycování těchto komunikací, a pokud na tuto otázku odpovíme kladně, související otázka, zda a jak lze takové jednání zdůvodnit.

Předmětem toho stanoviska je proto mimo jiné analýza ustanovení o důvěrnosti zpráv definovaných v čl. 5 odst. 1 směrnice 2002/58/ES o soukromí a elektronických komunikacích, jakož i analýza dalších relevantních ustanovení, které tvoří součást *acquis communautaire* a vnitrostátních právních předpisů k provedení *acquis*.

[1] *Úř. věst. ES L 281, 23.11.1995, s. 31, k nahlédnutí na adrese http://europa.eu.int/comm/internal_market/privacy/law_fr.htm .*

## II. PRÁVNÍ RÁMEC OCHRANY ÚDAJŮ A SOUKROMÍ PŘI KOMUNIKACI PROSTŘEDNICTVÍM ELEKTRONICKÉ POŠTY

### A) Evropská úmluva o ochraně lidských práv a základních svobod

Důvěrnost komunikací je zaručena v souladu s mezinárodními právními předpisy upravujícími oblast lidských práv, zejména Evropské úmluvy o ochraně lidských práv a základních svobod („EÚLP“) a ústavních pořádků členských států. Je zaručena i dvěma dále uvedenými směrnicemi EU.

Ustanovení článku 8 EÚLP poskytuje každému právo na respektování soukromého života a korespondence a současně stanoví podmínky, za nichž lze toto právo omezit. Evropský soud pro lidská práva („ESLP“) nejednou užil předmětný článek 8 v oblasti běžné komunikace uskutečňované prostřednictvím konvenčních poštovních služeb.

Jednání spočívající v zachycování, otevírání a čtení dopisů, zdržování jejich doručení, anebo vytváření překážek pro jejich odesílání byla považována za porušení článku 8 EÚLP[2]. Na základě rozhodovací praxe Komise a ESLP lze dospět k závěru, že se článek 8 bude zřejmě vztahovat i na komunikaci uskutečňovanou prostřednictvím elektronické pošty, přičemž se uplatní kombinace konceptů „soukromého života“ a „korespondence“[3]. Osoby komunikující prostřednictvím elektronické pošty mohou plným právem očekávat, že jejich komunikaci nebude kontrolovat žádný třetí subjekt (ať již veřejný nebo soukromý).

Právo na respektování „korespondence“ znamená nejen právo na respektování její důvěrnosti, ale i právo ji odesílat a přijímat[4]. Proto lze dospět k závěru, že z tohoto důvodu je jakékoliv obecné bránění v odesílání nebo přijímání elektronické pošty v rozporu s článkem 8 EÚLP.

Právo na respektování soukromého života a korespondence má každá osoba v jurisdikci některého ze smluvních států EÚLP. To se týká všech osob zúčastněných na komunikaci. V případě A. v. Francie (1993) soud rozhodl, že zaznamenávání telefonického rozhovoru na základě souhlasu pouze jednoho z účastníků rozhovoru je zásahem do práva na respektování korespondence druhé osoby zúčastněné na komunikaci.

Podle EÚLP mohou státy, které jsou stranami této úmluvy, legálně zachycovat korespondenci, jakož i elektronické zprávy, nebo přijímat jiná opatření, jestliže je to nutné z kteréhokoli z uvedených důvodů a v souladu s EÚLP a jejím výkladem obsaženým v rozhodnutích Evropského soudu pro lidská práva. Zachycování komunikací je možné definovat jako situaci, kdy třetí osoba získá přístup k obsahu a/nebo provozním údajům týkajícím se komunikace soukromého charakteru mezi dvěma nebo více účastníky, popř. k provozním údajům týkajícím se využití služeb elektronické komunikace, což představuje porušení práva určité osoby na ochranu soukromí a důvěrnosti korespondence. Toto zachycování je přípustné jen tehdy, jestliže splňuje tři základní kritéria vyplývající z ustanovení čl. 8 odst. 2 EÚLP a výkladu tohoto ustanovení Evropským soudem pro lidská práva:

„...[jestliže má] základ v právu, [jestliže je] v demokratické společnosti zapotřebí přijmout taková opatření a [jestliže] je v souladu s některým ze zákonných cílů uvedených v Úmluvě...“ .

V rámci vztahů mezi soukromými osobami je však nejvýznamnějším aplikačním mechanismem Úmluvy tzv. doktrína pozitivních povinností smluvních států. Smluvní státy mají totiž nejen povinnost zdržet se jakéhokoliv zásahu, ale i povinnost přijmout opatření pozitivního charakteru k zajištění skutečného výkonu těchto práv, a to nejen ve vztahu k veřejné moci, ale i ve sféře vzájemných vztahů mezi jednotlivci. Sem patří i povinnost vytvořit odpovídající právní rámec pro výkon těchto práv.

Ustanovení čl. 6 odst. 2 Smlouvy o EU jednoznačně stanoví, že Evropská unie respektuje základní práva, která jsou zaručena v EÚLP a vyplývají ze společných ústavních tradic členských států, jako základní zásady práva Společenství. Podle článku 52 odst. 3 Listiny EU je obsah a rozsah práv obsažených v Listině stejný jako obsah a rozsah práv zaručených EÚLP. Toto ustanovení nebrání tomu, aby právo Unie přiznávalo předmětným právům ochranu ve větším rozsahu.

### B) Zvláštní ustanovení o důvěrnosti komunikace uskutečňované prostřednictvím elektronické pošty

Jak již bylo uvedeno, je dále důvěrnost komunikace zaručena dvěma směrnicemi EU. Při posuzování otázky důvěrnosti komunikace musejí být ustanovení těchto směrnic vykládána v kontextu s EÚLP a citovanou judikaturou Soudu pro lidská práva.

Ve směrnici Evropského parlamentu a Rady 95/46/ES o ochraně fyzických osob při zpracovávání osobních údajů a volném pohybu těchto údajů („směrnice o ochraně údajů“) byl stanoven horizontální právní režim zajištění práva fyzických osob na ochranu údajů. Pokud jde o zpracovávání osob-

---

[2] *Soud ve svém rozhodnutí ve věci Niemitz z roku 1992 rozhodl, že se článek 8 EÚLP vztahuje i na dopisy, jež již byly doručeny adresátovi. V tomto rozhodnutí soud rovněž konstatoval, že ochranu požívá nejen soukromá, ale i obchodní korespondence. V rozhodnutích ve věcech Klass (1978), Malone (1984) a Huvig (1990) soud vyslovil, že se článek 8 vztahuje i na telefonické rozhovory. V souvislosti s jinými formami komunikace je významná věc Mersch (1958), v němž dospěla Komise k závěru, že odposlouchávání komunikací, bez ohledu na jejich formu, je porušením článku 8 EÚLP.*

[3] *Tento závěr podporuje i skutečnost, že ve většině členských států platí zákaz kontroly e-mailů a že na zachycování komunikací uskutečňovaných prostřednictvím elektronické pošty bylo nutno udělit konkrétní zmocnění jak na mezinárodní, tak i na vnitrostátní úrovni.*

[4] *Rozhodnutí ve věci Golder (1975), bod 43: „Bránit jinému dokonce již v zahájení korespondence představuje tu nejzávažnější formu zasahování (čl. 8 odst. 2 EÚLP) do výkonu práva na respektování korespondence. Je nemyslitelné, aby se článek 8 vztahoval na uskutečnění pouze samotné korespondence a zároveň se nevztahoval na takovéto jednání.“ Zasahováním by bylo rovněž zadržování již přijaté pošty (Schöneberger&Durmaz, 1988).*

ních údajů, odkazuje uvedená směrnice na právo na soukromí v rozsahu, v němž je uznáno článkem 8 EÚLP[5]. Rovněž bylo uznáno, že svoboda informací zaručená článkem 10 EÚLP zahrnuje právo přejímat a sdělovat informace[6]. Dále se podle odůvodnění č. 47 za správce osobních údajů obsažených v e-mailové zprávě považuje osoba, od níž tento e-mail pochází, přičemž poskytovatel služby elektronické pošty se obvykle považuje za správce, pokud jde o zpracovávání dalších údajů potřebných pro fungování služby.

Směrnice Evropského parlamentu a Rady 2002/58/ES týkající se zpracovávání osobních údajů a ochrany soukromí v odvětví elektronických komunikací („směrnice o ochraně soukromí v elektronické sféře“) se vztahuje na zpracovávání osobních údajů uskutečňované v souvislosti s poskytováním veřejně dostupných elektronických komunikačních sítí ve Společenství. Ustanovení této směrnice dále rozvíjejí a doplňují směrnici o ochraně údajů. Ochrana důvěrnosti komunikace je stanovena především v článku 5 směrnice o ochraně soukromí v elektronické sféře, jenž zní takto:

*„…Členské státy zajistí prostřednictvím vnitrostátních právních předpisů důvěrný charakter sdělení přenášených pomocí veřejné komunikační sítě. Zejména zakáží příposlech, odposlech, uchovávání nebo jiné druhy zachycování či sledování sdělení a s nimi souvisejících provozních údajů osobami jinými než uživateli bez souhlasu dotčených uživatelů, pokud k takovému jednání nejsou zákonem oprávněny v souladu s čl. 15 odst. 1…“ .*

Článek 4 směrnice o ochraně soukromí v elektronické sféře dále stanoví, že *„Poskytovatel veřejně dostupných služeb elektronických komunikací musí přijmout vhodná technická a organizační opatření, aby zajistil bezpečnost svých služeb, v případě nutnosti i v součinnosti s provozovatelem veřejné komunikační sítě, s ohledem na bezpečnost sítě“.*

V této souvislosti se uplatní i směrnice o elektronickém obchodu a zejména její ustanovení týkající se odpovědnosti poskytovatelů internetových služeb, resp. služeb elektronické pošty, podle nichž členské státy nemohou uložit poskytovatelům ISP a ESP obecnou povinnost monitorování. Tato povinnost by představovala zásah do svobody informací i do práva na ochranu důvěrnosti korespondence (článek 15 směrnice o elektronickém obchodu[7]).

## III. SKENOVÁNÍ OBSAHU E-MAILŮ

Ve světle tohoto právního základu vyvstává otázka, zda je skenování komunikací často prováděné poskytovateli ISP resp. ESP k dosažení různých cílů, slučitelné s právem EU.

E-maily skenuje většina poskytovatelů ISP a ESP. Tito poskytovatelé je skenují např. za účelem odfiltrování spamů a detekce virů, anebo je provádějí v souvislosti s funkcemi, jako je například vyhledávání, kontrola pravopisu, přeposílání pošty, automatické odpovídání, zvýrazňování přednostních zpráv, konverze e-mailů do podoby textových zpráv pro mobilní telefony, automatické ukládání nebo uchovávání v složkách a konverze URL vyjádřených textovou formou do podoby funkčního hyperlinkového odkazu.

V následujících částech tohoto dokumentu se budeme zabývat screeningem, který je prováděn z těchto důvodů: (A) detekce virů (B) odfiltrování spamů (C) detekce předem určeného obsahu.

### A) Screening elektronické pošty za účelem detekce virů

Antivirové skenování je postup spočívající v kontrole souborů s cílem zjistit, zda obsahují některý z již známých virů. V některých případech se po antivirovém skenovaní přistoupí k odvirování, postupu, který spočívá v odstranění detekovaného viru z napadnutého souboru, aby bylo možno soubor bezpečně použít. Obecně lze konstatovat, že k tomuto skenování dochází již při přijetí e-mailu některým ze serverů poskytovatele služby elektronické pošty. Většina poskytovatelů poskytuje antivirové skenování jako součást služby elektronické pošty s cílem ochránit sebe i uživatele před nebezpečím škodlivých virů. Ve většině případů nemají uživatelé možnost deaktivovat toto automatické skenování, které je přednastavenou součástí služby.

V souvislosti s posouzením právních důvodů, které by tvořily právní základ tohoto postupu, zastává Pracovní skupina názor, že zřizování a používání filtrovacích systémů poskytovateli služeb elektronické pošty, které se uskutečňuje za účelem detekce virů, lze právně zdůvodnit tím, že poskytovatelé mají povinnost provádět vhodné technické a organizační opatření k zaručení bezpečnosti svých služeb. Tato povinnost vyplývá z citovaného článku 4 směrnice o ochraně soukromí v elektronické sféře.

Vzhledem k tomu, že doručení e-mailu obsahujícího virus by mohlo (mimo poškození jiných dokumentů nebo softwaru uchovávaného v koncovém zařízení koncového uživatele) způsobit výpadek systému poskytovatele služby elektronické pošty a tak narušit přenos další e-mailové komunikace, je Pracovní skupina toho názoru, že provádění screeningu představuje bezpečnostní opatření zaměřené na ochranu systému správce údajů (v našem případě systému poskytovatele služby elektronické pošty), a proto (jak již bylo uvedeno výše) je plněním závazné povinnosti poskytovatele elektronických komunikačních služeb uložené článkem 4 směrnice o ochraně soukromí v elektronické sféře.

Pracovní skupina se dále domnívá, že používání filtru pro účely článku 4 může být slučitelné s článkem 5 směrnice o ochraně soukromí v elektronické sféře.

---

5) *Odůvodnění č. 10 „jelikož cílem vnitrostátních právních předpisů o zpracovávání osobních údajů je chránit základní práva a svobody, zejména právo na soukromí, což je respektováno jak v článku 8 Evropské úmluvy o ochraně lidských práv a základních svobod, tak i v obecných zásadách práva Společenství“.*

6) *Odůvodnění č. 37 „Jelikož zpracování osobních údajů pro účely žurnalistiky anebo literárního či uměleckého ztvárnění, zejména v audiovizuální oblasti, by mělo opravňovat k výjimkám z požadavků vyplývajících z určitých ustanovení této směrnice do té míry, jak je to nutné pro sladění základních práv jednotlivců se svobodou informací, zejména s právem získávat a předávat informace, jak to zaručuje zejména článek 10 Evropské úmluvy o ochraně lidských práv a základních svobod“.*

7) *Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu.*

Pracovní skupina chce především zdůraznit, že by uvedená opatření měla být v souladu s obecnými zásadami práva Společenství.

Pracovní skupina dále zastává názor, že zřizování filtrovacích systémů poskytovateli e-mailových služeb je možné rovněž považovat i za jednání v zájmu plnění smlouvy o poskytování služby uzavřené se zákazníky, kteří očekávají, že přijímání a odesílání e-mailů bude prováděno s určitým stupněm zabezpečení. Proto lze právně zdůvodnit zpracovávání údajů prováděné poskytovateli služeb elektronické pošty, k němuž dochází při zřizování filtrovacích systémů rovněž podle článku 7 písm. b) směrnice o ochraně údajů, podle nějž je upravené zpracovávání údajů *„nutné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů“*.

Vzhledem k tomu, že v souladu s výše uvedenými skutečnostmi lze antivirové filtrování zdůvodnit potřebou zajistit bezpečnost služby podle článku 4 směrnice o ochraně soukromí v elektronické sféře a/nebo prostým plněním smlouvy podle článku 7 odst. písm. b) směrnice o ochraně údajů, aniž by tím byla dotčena důvěrnost komunikace, Pracovní skupina připomíná, že poskytovatelé služeb elektronické pošty musejí zajistit dodržení těchto podmínek:

a) obsah e-mailů a příloh musí být uchován v tajnosti a nesmí se s ním seznámit žádná jiná osoba kromě příjemce popř. příjemců,

b) v případě nalezení viru musí nainstalovaný software poskytovat dostatečné záruky zachování důvěrnosti korespondence,

c) jestliže se antivirové skenování uskutečňuje formou skenování obsahu, mělo by se spouštět automaticky a pouze za tímto účelem, t.j. nesmí docházet k analýze obsahu ze žádného jiného důvodu.

Rovněž by měly být poskytnuty informace o screeningu (viz zvláštní oddíl).

### B) Screening elektronické pošty k odfiltrování spamů[8)]

Poskytovatelé ISP a ESP používají řadu metod, aby zabránili doručování nevyžádané elektronické pošty (která nemívá pouze komerční charakter) cílovému příjemci.

Jedna z těchto metod spočívá ve vytvoření a využívaní tzv. indexu, jakési „černé listiny“ IP adres serverů a registrů dynamických IP adres přidělovaných poskytovatelem ISP[9)]. V tomto stanovisku se však sestavováním a využíváním černé listiny dále nezabýváme.

Odfiltrovávání spamů je nyní nutné. Pokud by poskytovatelé služeb elektronické pošty nepoužívali systémy filtrování e-mailů k ochraně před spamy, nevyžádané e-maily by tvořily stále větší část příchozí pošty. Systémy elektronické pošty by byly velmi pomalé a nevýkonné, a staly by se pro uživatele téměř nepoužitelnými. To by bezpochyby vedlo k nespokojenosti zákazníků a zároveň omezilo možnost poskytovaní důvěryhodných a spolehlivých služeb elektronické pošty.

Třebaže spam sám o sobě neohrožuje bezpečnost služeb poskytovatele ESP, snižuje celkovou výkonnost sítě i služeb elektronické pošty a může vést až k tomu, že poskytovatel ESP zcela ztratí schopnost poskytovat službu elektronické pošty. Pracovní skupina se domnívá, že článek 4 směrnice o ochraně soukromí v elektronické sféře, který ukládá poskytovatelům služeb elektronické pošty povinnost přijmout vhodná technická a organizační opatření k zajištění bezpečnosti svých služeb, pojednává nejen o bezpečnosti poskytovatele ESP a síťových služeb jako takových, ale i o zajištění celkové výkonnosti síťových služeb a elektronické pošty. Bezpečnost poskytovatele ESP je proto problémem do té míry, v níž má vliv na služby elektronické pošty. Pracovní skupina proto zastává názor, že by se článek 4 mohl vztahovat i na tuto situaci. Jinak řečeno ohrožení celkové výkonnosti síťových služeb a služeb elektronické pošty může být důvodem pro jednání poskytovatelů ISP a ESP, které spočívá ve filtrování elektronické pošty za účelem ochrany před nevyžádanou korespondencí. Argumentaci pro uplatnění článku 4 směrnice o ochraně soukromí v elektronické sféře na předmětnou situaci posiluje i zvážení důsledků, které nevyžádaná pošta má, a to i v případě, kdy odesílatel této pošty rozešle e-mailem jen několik informací denně, ale velkému počtu adresátů. Již v takové situaci může odeslání malého počtu e-mailů zablokovat provoz internetu a vážně narušit celkovou spolehlivost, bezpečnost a výkonnost služeb elektronické pošty. Pracovní skupina dále zastává názor, že filtrování by bylo možné právně zdůvodnit i na základě článku 7 písm. b) směrnice o ochraně údajů, s poukazem na to, že toto odfiltrování spamů je nutné k zajištění schopnosti poskytovatele služby elektronické pošty řádně plnit smlouvu o poskytnutí služby, jejíž smluvní stranou je subjekt údajů, t. j. příjemce.

Na druhé straně se však Pracovní skupina obává případných „nesprávných pozitivních nálezů“, do nichž někdy ústí odfiltrovávání spamů, to znamená situace, kdy dojde k nedoručení legální a „vyžádané“ pošty, protože ji systém považoval za spam. Pracovní skupina zastává názor, že jednání spočívající ve filtrování a zadržování přijaté pošty, o níž se předpokládá, že je nevyžádaná, může znamenat nejenom zásah do

---

8) *V dokumentu OECD s názvem „Regulační opatření zaměřená proti nevyžádané korespondenci“ („Anti Spam Regulations“), který byl vypracován pracovní skupinou pro oblast spamů v březnu 2005 (DSTI/CP/ICCP/SPAM(2005)1), je pojem „spam“ definován takto: Pojem „spam“ se běžně používá ve světových médiích i při oznamování politických iniciativ různých zemí, jeho obecně uznávaná definice však neexistuje. Třebaže se různé státy většinou odvolávají na týž fenomén, definují spam způsobem, který má největší význam pro jejich místní poměry. Při vytváření politik zaměřených na potírání spamů je především nutné přesně pochopit a vymezit povahu spamu a zároveň jasně rozlišovat mezi šířením spamů a metodami, které jsou v souladu s právem.*

9) *Poskytovatel služby elektronické pošty v rámci této metody neprovádí filtraci e-mailů. Místo toho bez jakéhokoliv screeningu obsahu pouze prostě blokuje (tzn. nepřijímá) e-maily, které přicházejí ze serverů nebo registru dynamických IP adres, které jsou na černé listině. Třebaže metoda vytváření a využívání černých listin v zásadě představuje v porovnání s metodou filtrace elektronické pošty založené na zkoumání obsahu e-mailu méně výrazný zásah do práva na ochranu soukromí, může nastolit otázku svobody slova a svobody projevu a práva na neomezené provádění a příjem korespondence ve smyslu článku 8 EÚLP a jejího výkladu Evropským soudem pro lidská práva.*

svobody slova, ale i porušení článku 10 EÚLP a zasahování do soukromé komunikace[10)].

Vzhledem k uvedené skutečnosti, bez ohledu na uplatňování článku 4 směrnice o ochraně soukromí v elektronické sféře a v zájmu dodržení zásady svobody komunikace uznané článkem 10 EÚLP a důvěrnosti komunikace stanovené v článku 5 směrnice o ochraně soukromí v elektronické sféře a uznané v článku 8 EÚLP, Pracovní skupina naléhavě doporučuje poskytovatelům služeb elektronické pošty zohlednit tato doporučení, jejichž cílem je zejména umožnit příjemcům e-mailů kontrolu nad komunikacemi, které jsou jim v zásadě adresované:

a) Pracovní skupina vyjadřuje svou podporu takovým postupům, které účastníkům umožní vyjmout své e-maily ze skenování prováděného za účelem ochrany před spamy, a dále možnost prověřit e-maily, které jsou považované za spam, s cílem zjistit, zda tomu tak skutečně je, a konečně možnost rozhodnout o tom, který „druh" spamů by měl být odfiltrován. Pracovní skupina dále vítá iniciativu některých poskytovatelů ESP, kteří účastníkům nabízejí jednoduchý způsob zpětného přihlášení e-mailů do skenování za účelem odfiltrování spamů,

b) Pracovní skupina současně vyzývá k tomu, aby byly vytvořeny takové filtry, které by si mohli nainstalovat nebo zkonfigurovat sami uživatelé, a to buď přímo do svých koncových zařízení, anebo na servery třetích osob, popřípadě na servery poskytovatele služby elektronické pošty a které by jim poskytly možnost kontroly nad tím, co chtějí nebo nechtějí přijmout. To by zároveň vedlo ke snížení nákladů, jež vznikají stahováním nevyžádané elektronické pošty, jak se připomíná v odůvodnění č. 44 směrnice 2002/58/ES. Pracovní skupina vítá i výzkum v oblasti prostředků boje proti spamům, které by mohly představovat méně výrazné zasahování do práva na soukromí.

Pracovní skupina chce kromě výše uvedených skutečností připomenout poskytovatelům služeb elektronické pošty, kteří uskutečňují skenování e-mailů za účelem ochrany před spamy, jejich povinnost vyplývající z článku 10 směrnice o ochraně údajů, v jehož smyslu jsou povinni jasným a jednoznačným způsobem informovat účastníky o svých politikách ochrany proti spamům, jak se uvádí dále v části IV tohoto stanoviska. Poskytovatel služby musí rovněž zajistit důvěrnost filtrovaných e-mailů. Tyto e-maily by se neměly použít k žádnému jinému účelu.

### C) Screening elektronické pošty za účelem detekce předem určeného obsahu.

Pracovní skupina konstatuje, že si někteří poskytovatelé služeb elektronické pošty vyhrazují právo prověřit nebo dokonce odstranit předem určený obsah[11)]. Tímto obsahem by mohl být například materiál, o němž existuje podezření, že má protiprávní charakter, nebo materiál, který si příjemce, čili uživatel této konkrétní služby, nepřeje. Při tomto druhu screeningu se používá velmi podobná metoda jako při detekci virů a spamů.

Na rozdíl od screeningu za účelem detekce virů nelze screening elektronické pošty za účelem detekce předem určeného obsahu (a to i v případě, že by se tento obsah mohl považovat za materiál, o němž existuje podezření z protizákonného charakteru) považovat za vhodné technické a organizační opatření k zaručení bezpečnosti služeb elektronické pošty ve smyslu článku 4 směrnice o ochraně soukromí v elektronické sféře. Poskytovateli služby elektronické pošty nehrozí v důsledku předmětných materiálů obsažených v e-mailech nebezpečí vzniku újmy nebo výpadku komunikace. Z tohoto důvodu nelze skenování za účelem detekce takového obsahu právně zdůvodnit potřebou poskytovatele zaručit bezpečnost služby.

Pracovní skupina se rovněž obává, že při uskutečňování tohoto typu filtrování se poskytovatelé služeb elektronické pošty stávají cenzory soukromé e-mailové komunikace (např. tím, že blokují komunikace, jejichž obsah je zcela v souladu se zákonem), což nastoluje zásadní otázky svobody slova, projevu a informací. Pracovní skupina zdůrazňuje, že poskytovatelé služeb nemají povinnost monitorovat předem určený obsah nebo obsah údajně škodlivého charakteru, že však mohou tento typ služby nabízet (jak uvádíme v následujících částech tohoto stanoviska) formou služby s přidanou hodnotou.

Pracovní skupina se tudíž domnívá, že ve smyslu čl. 5 odst. 1 směrnice o ochraně soukromí v elektronické sféře poskytovatelé služeb elektronické pošty nemohou filtrovat, uchovávat nebo uskutečňovat jiné druhy zachycování komunikace nebo souvisejících provozních údajů za účelem detekce předem určeného obsahu bez souhlasu uživatelů služby,

---

[10)] *Uznáno ESLP v rozhodnutí ve věci Schöneberger a Durmaz z roku 1988.*

[11)] *Viz obchodní podmínky společnosti Yahoo!: Tímto berete na vědomí, že společnost Yahoo! může předem prozkoumat (nebo neprozkoumat) obsah; Yahoo! (případně osoby určené touto společností) mají právo (nikoli však povinnost) podle svého uvážení prozkoumat, odmítnout příjem nebo přesunout jakýkoliv obsah, který je dostupný prostřednictvím této služby. Yahoo! a osoby určené touto společností mají, aniž by bylo dotčeno předchozí ustanovení, právo odstranit jakýkoliv obsah, jenž by byl v rozporu s těmito obchodními podmínkami nebo byl nevhodný z jakýchkoliv jiných důvodů. Dále vyjadřujete souhlas s tím, že jste povinen zvážit a nést jakékoliv riziko, které je spojeno s použitím jakéhokoliv obsahu, včetně nebezpečí, které hrozí při spoléhání na správnost, úplnost nebo užitečnost takového obsahu. V této souvislosti berete na vědomí, že se nemůžete spoléhat na jakýkoliv obsah vytvořený společností Yahoo! nebo na obsah této společnosti poskytnutý. To platí rovněž (nikoli však výhradně) pro informace poskytované v diskusních fórech společnosti Yahoo! na nástěnkách i v jakýchkoliv jiných součástech služby. Tímto berete na vědomí a vyjadřujete svůj souhlas s tím, že společnost Yahoo! má právo přístupu k údajům o vašem účtu i k obsahu, a že tyto údaje anebo obsah může uchovávat a poskytnout, jak jí to ukládá zákon, anebo v dobré víře, že takovýto přístup, uchovávání nebo poskytování lze důvodně považovat za nutné: a) ke splnění povinností uložených zákonem nebo jinými obecně závaznými právními předpisy, b) k vynucení práv a povinností stanovených těmito obchodními podmínkami, c) pro vyjádření se k tvrzení, že obsah představuje porušení práv třetích osob, d) v souvislosti s odpovědí na Vaši žádost o poskytnutí zákaznického servisu, nebo e) za účelem ochrany práv, majetku anebo bezpečnosti pracovníků společnosti Yahoo!, uživatelé jejích služeb nebo veřejnosti.*

nebo musejí být k uskutečňování tohoto screeningu zmocněny zákonem v souladu s článkem 15 směrnice o ochraně soukromí v elektronické sféře, popř. v souladu s právními předpisy členských států, jimiž je tato směrnice provedena.

## IV. INFORMAČNÍ POVINNOST

Kromě čl. 5 směrnice o ochraně soukromí v elektronické sféře musí zpracovávání osobních údajů za účelem získávání poznatků o obsahu soukromé komunikace a/nebo souvisejících provozních údajích splňovat i různé další podmínky stanovené směrnicí o ochraně údajů.

Směrnice o ochraně údajů ukládá mimo jiné povinnost informovat fyzické osoby o tom, že jsou zpracovávány jejich osobní údaje. Zejména článek 10 *„Informace poskytované subjektu údajů“* ukládá správcům údajů povinnost poskytnout subjektům údajů, od nichž jsou osobní údaje získávány, určité informace, k nimž patří informace o totožnosti správce údajů a o účelech zpracování těchto údajů. Ustanovení čl. 6 odst. 1 písm. a) směrnice o ochraně údajů dále stanoví, že údaje musejí být zpracovávány řádně a v souladu se zákonem, což posiluje povinnost správce údajů zajistit plnou transparentnost ohledně podmínek zpracování osobních údajů.

V otázce filtrování pro účely screeningu virů a spamů považuje Pracovní skupina za adekvátní praxi poskytovatelů ESP, která spočívá v tom, že tito poskytovatelé účastníkům poskytují informace jako součást smluvních podmínek služby.

Navíc má poskytovatel ESP povinnost postupovat i v souladu s článkem 4 směrnice o ochraně soukromí v elektronické sféře, podle nějž jsou poskytovatelé veřejně dostupných elektronických komunikačních služeb povinni informovat účastníky o konkrétních rizicích narušení bezpečnosti sítě.V případě, že je bezpečnost mimo rámec, v němž je náprava v možnostech poskytovatelů služeb, poskytovatelé by měli informovat uživatele a účastníky o opatřeních, která mohou přijmout v zájmu ochrany bezpečnosti jejich komunikací.

## V. DALŠÍ SLUŽBY SOUVISEJÍCÍ S ELEKTRONICKOU POŠTOU

Pracovní skupina poznamenává, že dochází k vývoji nových typu softwarových produktů a služeb, například služby nazvané *„Did they read it?“* („Přečetli to ?“), jejímž cílem je sledovat, zda došlo k otevření e-mailu.

Tento typ služby umožňuje každému účastníku služby zjistit, zda byl jím odeslaný e-mail:

a) adresátem popř. více adresáty přečten,

b) kdy byl přečten,

c) kolikrát byl přečten (nebo alespoň otevřen),

d) zda byl přeposlán dalším osobám a

e) na který e-mailový server byl přeposlán a kde se tento server nachází.

Služba dále umožňuje zjistit, jaký druh internetového prohlížeče a operačního systému příjemce e-mailu používá.

Zpracovávání údajů se uskutečňuje skrytou formou, to znamená, že o něm nejsou poskytnuty informace příjemcům e-mailu, od nichž se tyto údaje získávají. Příjemcům e-mailu není poskytnuta ani možnost toto získávání informací schválit nebo odmítnout. Lze tedy uzavřít, že na rozdíl od klasických systémů potvrzování příjmu e-mailu nemá u těchto nových produktů příjemce e-mailu možnost schválit nebo nepovolit uživateli systému zpracovávání informací souvisejících s potvrzením příjmu.

Pracovní skupina zásadně nesouhlasí s tímto zpracovávání údajů, a sice proto, že při něm dochází k zaznamenávání a přenosu osobních údajů o chování adresáta bez jeho výslovného a jednoznačného souhlasu. Toto skryté zpracovávání odporuje zásadám ochrany údajů obsaženým v článku 10 směrnice o ochraně údajů, které při shromažďování osobních údajů vyžadují loajálnost a transparentnost.

K provedení úkonu zpracování údajů spočívajícího v získávání informací od příjemců e-mailu o tom, zda a kdy byl tento e-mail přečten a zda byl přeposlán třetím osobám, je zapotřebí výslovný a jednoznačný souhlas příjemců e-mailu. Neexistují žádné další právní důvody k takovému zpracovávání. Zpracovávání údajů skrytou formou odporuje tudíž zásadám ochrany údajů stanoveným v ustanovení článku 7 směrnice o ochraně údajů, které vyžaduje poskytnutí výslovného a jednoznačného souhlasu.

## VI. ZÁVĚR

Pracovní skupina se domnívá, že vzhledem k trvající nejistotě v otázce slučitelnosti filtrování komunikace uskutečňované prostřednictvím elektronické pošty i v souvislosti s tím, že zainteresované strany vyjádřily zájem o vydání pokynů, by bylo užitečné zveřejnění tohoto stanoviska.

Pracovní skupina vyzývá poskytovatele služeb elektronické pošty, aby v rámci svých služeb zohlednili pokyny a doporučení obsažené v tomto stanovisku. Pracovní skupina by jako výraz obecného přístupu spočívajícího v podpoře technologií, které při budování infrastruktury, informačních systémů a koncových zařízení umožňují zapracování prvků na ochranu údajů a splnění požadavků na ochranu soukromí, chtěla povzbudit softwarové vývojáře v oblasti e-mailových aplikací k tomu, aby navrhli a vytvořili systémy splňující požadavky vyplývající z práva na ochranu soukromí tak, aby se zpracovávání osobních údajů zredukovalo na nutné minimum, aby k jeho uskutečňování docházelo jen ve zcela nutném rozsahu a aby toto zpracovávání bylo přiměřené účelu zpracování.

V Bruselu, dne 21. února 2006

Za Pracovní skupinu
předseda
Peter SCHAAR

Poznámka: Dokument je také k dispozici na internetové adrese http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp118_cs.pdf .

# Věstník Úřadu pro ochranu osobních údajů

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

**Administrace**: Písemné objednávky předplatného, změny adres a počtu odebíraných výtisků – SEVT, a. s., Pekařova 4, 181 06 Praha 8-Bohnice, telefon: 283 090 352, 283 090 354, fax: 233 553 422, www.sevt.cz, e-mail: sevt@sevt.cz. – **Předpokládané roční předplatné** se stanovuje za dodávku kompletního ročníku a je od předplatitelů vybíráno formou záloh ve výši oznámené ve Věstníku a pro tento rok činí 450 Kč – Vychází podle potřeby – **Tiskne**: SPRINT SERVIS, Lovosická 31, Praha 9.

**Distribuce:** Předplatné, jednotlivé částky na objednávku i za hotové – SEVT, a. s., Pekařova 4, 181 06 Praha 8-Bohnice, telefon: 283 090 352, 283 090 354, fax: 233 553 422; drobný prodej v prodejnách SEVT, a. s. – Praha 5, Elišky Peškové 14, tel./fax: 257 320 049, – Praha 4, Jihlavská 405, tel.: 261 260 414 – Brno, Česká 14, tel.: 542 213 962 – Ostrava, roh ul. Nádražní a Denisovy, tel.: 596 120 690 – České Budějovice, Česká 3, tel.: 387 319 045 a ve vybraných knihkupectvích. **Distribuční podmínky předplatného**: Jednotlivé částky jsou expedovány předplatitelům neprodleně po dodání z tiskárny. Objednávky nového předplatného jsou vyřizovány do 15 dnů a pravidelné dodávky jsou zahajovány od nejbližší částky po ověření úhrady předplatného, nebo jeho zálohy. Částky vyšlé v době od zaevidování předplatného do jeho úhrady jsou doposílány jednorázově. Změny adres a počtu odebíraných výtisků jsou prováděny do 15 dnů. Lhůta pro uplatnění reklamací je stanovena na 15 dnů od data rozeslání, po této lhůtě jsou reklamace vyřizovány jako běžné objednávky za úhradu. V písemném styku vždy uvádějte IČ (právnická osoba) a kmenové číslo předplatitele. **Podávání novinových zásilek** povoleno ŘPP Praha.

**ISSN 1213-3442**