VĚSTNÍK
ÚŘADU PRO OCHRANU OSOBNÍCH ÚDAJŮ
2004

Částka 35 | **8. prosince 2004** | **Cena 39,- Kč**

OBSAH

ÚVOD

Úřad ještě znovu upozorňuje na skutečnost, že na základě novely zákona o ochraně osobních údajů, která byla vyhlášena ve Sbírce zákonů dne 26. července 2004, budou v obsahu i v periodicitě Věstníku provedeny změny. V souladu s novelizovaným zákonem o ochraně osobních údajů Úřad není povinen zveřejňovat ve svém Věstníku abecední seznam zaregistrovaných subjektů a povolených zpracování osobních údajů zaregistrovaných Úřadem, ale pouze přehled zrušených registrací. Informace o nových registracích je zveřejňována na webových stránkách Úřadu (www.uoou.cz) v rubrice Registrace.

Tato částka Věstníku tedy již obsahuje pouze přehled zrušených registrací – v období 10. 8. 2004 až 16. 11. 2004.

Rubrika Stanoviska Úřadu přináší Stanovisko č. 6/2004, které poskytuje informace o kopírování dokladů z pohledu zákona o ochraně osobních údajů.

Oddíl Sdělení Úřadu se věnuje aplikaci zákona o některých službách informační společnosti. Kromě obecné informace seznamuje s kompetencemi Úřadu pro ochranu osobních údajů ve vztahu k šíření nevyžádaných obchodních sdělení a vzor formuláře k podání stížnosti na šiřitele takových sdělení. Součástí sdělení Úřadu jsou také dvě Stanoviska Pracovní skupiny pro ochranu dat podle článku 29 směrnice 95/46/ES: Stanovisko č. 4/ 2004, ke zpracování osobních údajů prostředky kamerového sledování a Stanovisko č. 8/ 2004, k informacím pro cestující, týkajícím se předávání údajů obsažených v PNR (Passenger Name Record – Záznam o knihování zákazníka), u letů mezi Evropskou unií a Spojenými státy americkými.

Přehled zrušených registrací od 10. 8. 2004 do 16. 11. 2004

Číslo registrace	Subjekt	Datum zrušení
00000240/001	RYCHVALDSKÉ AUTODRUŽSTVO, VÝROBNÍ DRUŽSTVO	28.9.2004
00001188/018	UNILEVER ČR SPOL. S R.O.	27.8.2004
00001188/024	UNILEVER ČR SPOL. S R.O.	27.8.2004
00001188/029	UNILEVER ČR SPOL. S R.O.	27.8.2004
00005817/001	ESSOX LEASING A.S.	8.9.2004
00005928/001	MICROSOFT S. R. O.	23.9.2004
00005928/003	MICROSOFT S. R. O.	23.9.2004
00021209/001	N&N SECURITY S.R.O.	23.9.2004
00021807/001	DESBOCADO S.R.O.	27.8.2004
00022204/001	ŠIMKOVÁ LENKA	1.10.2004

II. STANOVISKA ÚŘADU

Stanovisko č. 6/2004

listopad 2004

Kopírování dokladů z pohledu zákona o ochraně osobních údajů

Pořizování a uchovávání kopií nejrůznějších druhů osobních dokladů a jiných listin v držení fyzických osob je velmi častým výsledkem zjištění Úřadu pro ochranu osobních údajů v souvislosti s výkonem dozoru podle 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"). Ačkoliv kopie sama o sobě jistě není svým významem adekvátní originálnímu dokladu nebo dokumentu, je uchovávání kopie osobního dokladu či veřejné listiny považováno za zpracování osobních údajů podle zákona o ochraně osobních údajů, které by mělo stejně jako jiné druhy zpracování probíhat pouze v jeho mezích a v souladu s platným zvláštním právním předpisem.

Častým argumentem osob, které si kopie osobních dokladů nebo veřejných listin uchovávají pro úřední potřebu, je skutečnost, že se tímto jednáním brání tlaku kontrolních orgánů nejrůznějších typů, kterým jako důkaz, že tvrzené skutečnosti byly ověřeny podle platného osobního dokladu nebo veřejné listiny, již nepostačuje „pouhý" záznam do příslušné dokumentace, ale vyžadují předložení alespoň kopie dokumentu nebo dokladu. Současně se lze často setkat s tvrzením, že se jedná spíše o ochranu osoby, jejíž kopie dokladu je zakládána, neboť se pak vykonávající úředník může více spolehnout na již existující fotokopie dokladů a porovnat tyto kopie vždy v případě předložení dokladů; což může pomoci odhalit případně možné falzifikáty těchto dokladů předkládané jinými osobami. Nicméně, mj. také s ohledem na dnešní technické možnosti pořízení dokonalých kopií osobních listin a dokladů, s ohledem na nárůst trestné činnosti páchané pomocí padělků osobních dokladů, je nutné přijmout pravidla, kterými by se možnosti legitimního pořizování kopií osobních listin a dokladů minimalizovaly.

Jisté světlo do současného stavu vnáší novelizace zákona č. 328/1999 Sb., o občanských průkazech, ve znění pozdějších předpisů, a zákona č. 329/1999 Sb., o cestovních dokladech a o změně zákona č. 283/1991 Sb., o Policii České republiky, ve znění pozdějších předpisů, (zákon o cestovních dokladech), publikovaná ve Sbírce zákonů pod číslem **559/2004** Sb. jako zákon, kterým se mění zákon č. 328/1999 Sb., o občanských průkazech, ve znění pozdějších předpisů, zákon č. 329/1999 Sb., o cestovních dokladech a o změně zákona č. 283/1991 Sb., o Policii České republiky, ve znění pozdějších předpisů, (zákon o cestovních dokladech), ve znění pozdějších předpisů, zákon č. 200/1990 Sb., o přestupcích, ve znění pozdějších předpisů, a zákon č. 326/1999 Sb., o pobytu cizinců na území České republiky a o změně některých zákonů, ve znění pozdějších předpisů, která obsahuje doplnění příslušných ustanovení tohoto zákona **o zákaz pořizovat jakýmikoliv prostředky kopie občanského průkazu nebo cestovního dokladu bez souhlasu občana, kterému byl občanský průkaz nebo cestovní doklad vydán, pokud zvláštní právní předpis nebo mezinárodní smlouva, kterou je Česká republika vázána, nestanoví jinak.**

Toto ustanovení současně odkazuje v případě pochybnosti k obsahu pojmu souhlas na příslušné ustanovení § 5 zákona o ochraně osobních údajů, které po novele provedené zákonem č. 439/2004 Sb., s účinností od 26. července 2004 společně s novou definicí pojmu souhlas subjektu údajů vychází z principů svobodného, vědomého a informovaného projevu vůle fyzické osoby, jak ostatně již tradičně vyjadřují příslušná ustanovení občanského zákoníku týkající se problematiky právních úkonů obecně.

Tato právní úprava současně odstraňuje vedlejší problém, který musel Úřad pro ochranu osobních údajů řešit při posuzování této otázky, a to, zda v případě, že docházelo ke kopírování osobního dokladu se souhlasem jeho držitele, měl být současně získán také souhlas třetích osob, v případě, že jejich osobní údaje jsou na osobním dokladu také uvedeny. Jde o tzv. nepovinné údaje, kterými jsou jméno, příjmení a rodné číslo manžela, případně jméno, příjmení a rodné číslo dítěte. Při snaze dostát povinnostem podle zákona o ochraně osobních údajů často docházelo k vymazávání těchto údajů z uchovávaných kopií osobních dokladů. To do budoucna již nebude nutné, neboť nová právní úprava podmínek pro pořizování kopií osobních dokladů opravňuje jeho držitele, aby vyjádřil souhlas s pořízením kopie svého osobního dokladu, tedy ke zpracování v něm obsažených osobních údajů.

Nabytím účinnosti dnem 1. ledna 2005 novelizovaných ustanovení zákona o občanských průkazech a zákona o cestovních dokladech bude tedy obecně platit zásada, že pořizování kopie občanského průkazu nebo cestovního dokladu je zakázáno.

Z této zásady budou platit v principu **dvě výjimky,** a to pouze

a) v případě, že **občan – držitel tohoto osobního dokladu vyjádří souhlas** s pořízením kopie,
b) v případě, že pořizování kopií **je stanoveno zvláštním právním předpisem nebo mezinárodní smlouvou**, kterou je Česká republika vázána,

bude možné takovou kopii pořídit a uchovávat.

Pokud jde o **podmínky souhlasu** držitele osobního dokladu, jak je již výše uvedeno, bude muset ten subjekt, který hodlá kopírovat předložený osobní doklad, přesvědčit držitele dokladu o svém záměru zejména v tom směru, zda je pořízení kopie pro něj natolik potřebné a nezbytné, aby prováděný způsob zpracování osobních údajů uchováním kopie osobního dokladu nesnižoval dosavadní úroveň ochrany soukromí subjektu údajů – jeho držitele, případně dalších osob, jejichž osobní údaje jsou tímto způsobem současně

zpracovány. V této souvislosti je dále třeba upozornit na rozsah povinně zapisovaných údajů, který se v porovnání s minulostí již při předcházejících novelizacích těchto ustanovení rozšířil o podpis držitele osobního dokladu. Za této situace se přitom bude jednat o přímou aplikaci několika ustanovení novelizovaného zákona o ochraně osobních údajů, které se této problematiky dotýkají. Jde především o ustanovení § 4 písm. n), které obsahuje definici pojmu souhlas subjektu údajů, podle kterého se má jednat o „svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů“, vedle toho se bude aplikovat nové znění § 5 odst. 4 (dříve odst. 5), obsahující podmínky, které musejí být při udělování souhlasu subjektu údajů dodrženy: Jde o to, že „Subjekt údajů musí být při udělení souhlasu informován o tom, pro jaký účel zpracování a k jakým osobním údajům je souhlas dáván, jakému správci a na jaké období. Souhlas subjektu údajů se zpracováním osobních údajů musí být správce schopen prokázat po celou dobu zpracování.“ I když jsou nové právní podmínky pro pořizování kopií osobních dokladů jistě žádoucí, je nutné je chápat a vykládat pouze v celém kontextu souboru práv a povinností správce podle zákona o ochraně osobních údajů a dbát na to, že i přes udělený souhlas je nutno, aby správce dodržoval další principy ochrany dat – legitimitu, přiměřenost a účelovost zpracovávaných osobních údajů.

Rozhodne-li se tedy odpovědný subjekt uchovávat kopie dokladů, stává se z pohledu zákona o ochraně osobních údajů vždy správcem, který musí dodržovat veškeré povinnosti, které od něj tento zákon očekává. Samotné uchovávání kopií dokladů je jen jednou z operací, kterou správce při zpracování osobních údajů provádí. Stejně důležité z pohledu zákona o ochraně osobních údajů jsou však také

a) splnění oznamovací povinnosti správce vůči Úřadu pro ochranu osobních údajů podle § 16 zákona o ochraně osobních údajů,
b) vlastní informační kampaň správce vůči subjektům údajů, jejíž rámec je vymezen § 5 odst. 4 zákona o ochraně osobních údajů, prováděná ještě před tím, nežli k souhlasu subjektu údajů dochází,
c) schopnost správce prokázat, že souhlas subjektu údajů existuje.

V případě zákonem o občanských průkazech a zákonem o cestovních dokladech vyjmenované druhé možnosti pro pořizování kopií těchto dokladů za situace, kdy je tak **stanoveno zvláštním právním předpisem** nebo mezinárodní smlouvou závaznou pro Českou republiku, lze již dnes v právním řádu České republiky nalézt příklad, kdy se jako součást povinné dokumentace, dokladování apod. očekává také uchovávání kopií osobních dokladů. Jde o **zákon č. 61/1996 Sb.,** o některých opatřeních proti legalizaci výnosů z trestné činnosti a o změně a doplnění souvisejících zákonů, ve znění pozdějších předpisů, který upravuje speciální podmínky pro provádění identifikace fyzických osob (§ 2 odst. 6 až 8) a uchovávání stanovených údajů také prostřednictvím kopií dokladů (§ 3 odst. 2). Podle ustanovení § 2 odst. 7 ten, kdo provedl identifikaci podle odstavce 6 (Identifikace na žádost povinné osoby), připojí k veřejné listině o identifikaci kopie příslušných dokladů nebo jejich částí, z nichž provedl identifikaci. Podle ustanovení § 2 odst. 8 byla-li provedena identifikace a další úkony podle odstavců 6 a 7, doklady tam uvedené musejí být uloženy u povinné osoby. Do té doby neprovede povinná osoba s takto identifikovanou osobou žádný obchod podle tohoto zákona.Vzhledem k tomu, že se tato úprava dotýká poměrně vymezeného okruhu subjektů (Notářský řád. Zákon č. 41/1993 Sb., o ověřování shody opisů nebo kopie s listinou a o ověřování pravosti podpisu okresními a obecními úřady a o vydávání potvrzení orgány obcí a okresními úřady, ve znění pozdějších předpisů. Vyhláška č. 272/2000 Sb., o ověřování pravosti podpisu nebo shody opisu nebo kopie s listinou velitelem lodě.) a jejich činností, dá se očekávat také úměrný nárůst požadavků ze strany kontrolních orgánů na podmínky pro uchování dokumentace, obsahující kopie těchto dokladů.

V této souvislosti je nezbytné odkázat opět na příslušná ustanovení zákona o ochraně osobních údajů, a to zejména na § 13 a následující ustanovení, týkající se povinností správce při zabezpečení zpracování osobních údajů. Již dříve zákonem o ochraně osobních údajů vymezený rámec podmínek je doplněn o nový odstavec 2 v § 13, podle něhož je „správce nebo zpracovatel povinen zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů v souladu se zákonem o ochraně osobních údajů a jinými právními předpisy“.

Na rozdíl od obecné právní úpravy podmínek pro pořizování kopií osobních dokladů se zatím neobjevují v právním řádu náznaky, že by podobně jako v případech občanských průkazů a cestovních dokladů měl zákonodárce vůli řešit obdobným způsobem i podmínky pro kopírování jiných druhů listin nebo dokumentů osobního charakteru, jako jsou například rodné listy, oddací listy, úmrtní listy apod. Zatím se pouze v několika případech zakotvila v právních předpisech oprávnění pro pořizování kopií dokladů o dosaženém vzdělání, o čemž svědčí například zákon č. 18/2004 Sb., o uznávání odborné kvalifikace, nebo vyhláška č. 333/2004 Sb., o odborné způsobilosti na úseku rostlinolékařské péče. V ostatních případech je naopak nezbytné požadavek na pořízení kopie osobního dokladu nebo dokumentu odmítnout jako nezákonný. Pouze v těch případech, kdy správce držiteli tohoto dokladu prokáže oprávněnost svého požadavku, je možné per analogiam uchovávat kopii se souhlasem držitele tohoto dokladu.

III. SDĚLENÍ ÚŘADU

Aplikace zákona o některých službách informační společnosti vzhledem k ochraně osobních údajů

1. Obecně k zákonu č. 480/2004 Sb., o některých službách informační společnosti

Zákonem se transponuje do právního řádu České republiky směrnice Evropského parlamentu a Rady o elektronickém obchodu č. 2000/31/ES, s ohledem na směrnici o soukromí v elektronických komunikacích (2002/58/ES), která v článku 5 zdůrazňuje povinnost členských států EU zajistit **důvěrný charakter sdělení** přenášených pomocí veřejné komunikační sítě a veřejně dostupných elektronických služeb.

Proto i základní myšlenkou zákona č. 480/2004 Sb. je **posílení ochrany soukromí uživatele služby informační společnosti,** kterým může být každá fyzická nebo právnická osoba /viz definice uživatele obsažená v § 2 písm. e) zákona/. Zřejmá je snaha zákonodárce docílit, aby uživatel nemusel vydávat žádné náklady na jemu doručená obchodní sdělení zasílaná elektronickou poštou /viz definice elektronické pošty obsažená v § 2 písm. b) zákona/, která si nevyžádal, a která jej ve svém důsledku obtěžují. V této souvislosti není důležitá forma elektronické komunikace.

Pojem **šíření obchodních sdělení** se podle směrnice č. 2000/31/ES, stejně jako podle zákona č. 480/2004 Sb., vztahuje na všechny formy sdělení určené k přímé či nepřímé podpoře zboží nebo služeb (i školení, placené informace apod.) konkrétního subjektu, tedy i na nabídky bezplatných služeb, pokud tento subjekt je tzv. ekonomickým subjektem, tedy subjektem vykonávajícím podnikatelskou činnost (tímto se sice ze zákona vylučují všechny nepodnikatelské aktivity ekonomických subjektů, jako je podpůrná nadační nebo charitativní činnost), ale přitom se zákon č. 480/2004 Sb. vztahuje na telemarketing realizovaný například přímým hovorem se zákazníkem bez ukládání zprávy v koncovém zařízení uživatele. Zákon se nevztahuje na uskutečňování přímých kontaktů mezi uživateli elektronické pošty navzájem, ať již formou zprávy textové, hlasové, zvukové nebo obrazové, pokud je uskutečňována mimo rámec jejich obchodní nebo profesní činnosti. Stejně tak se zákon nevztahuje na šíření televizního ani rozhlasového vysílání, ale naopak se zákon vztahuje na službu, kterou je například video na přání.

Zákon č. 480/2004 Sb., upravuje také **podmínky výkonu tzv. regulované činnosti,** ale to spíše s ohledem na formu této činnosti – nabídky zboží nebo služby, která je součástí služby informační společnosti s očekáváním jistých samoregulačních vlivů jednotlivých profesních sdružení nebo profesních komor zřízených zákonem, kterým je také současně svěřena kompetence dozorového subjektu.

Pokud jde o **institut souhlasu zákazníka,** v návaznosti na nové znění příslušných ustanovení zákona o ochraně osobních údajů, která jednoznačně deklarují, že souhlas subjektu údajů je projevem jeho vůle, tedy právním úkonem, dá se ze strany ÚOOÚ očekávat i stejný přístup k podstatě „prokazatelnosti souhlasu“ zákazníka s využitím svého elektronického kontaktu pro potřeby šíření obchodních sdělení, ve smyslu příslušných ustanovení zákona č. 480/2004 Sb. Skutečnost, že i když byl souhlas podle § 7 odst. 1 zákona č. 480/2004 Sb. udělen, musí být podle téhož ustanovení zákazníkovi při zaslání každé zprávy vytvořena možnost jednoduše a bez vynaložení nákladů souhlas odvolat (v zákoně uvedeno slovo „odmítnout“), lze považovat za základní pravidlo pro komunikaci se zákazníkem, kterou tento zákon označuje jako šíření obchodních sdělení.

Obecně lze konstatovat, že i když je zákon o některých službách informační společnosti svou jednoznačnou preferencí metody „opt-in“ pro komunikaci se zákazníkem poněkud přísnější v porovnání s vymezením tohoto rámce v právu ES, zákonodárce tím dal všem subjektům působícím v této oblasti jednoznačně najevo svou vůli, kterou Úřad pro ochranu osobních údajů hodlá prosazovat.

2. Kompetence Úřadu pro ochranu osobních údajů ve vztahu k šíření obchodních sdělení

Působnost Úřadu pro ochranu osobních údajů (dále jen „Úřad“) podle zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), spočívá ve výkonu dozoru nad šířením obchodních sdělení prováděným v rámci podnikatelské činnosti; součástí výkonu dozoru je i prověřování podání týkajících se této činnosti.

Podání adresovaná Úřadu musejí směřovat proti obchodním sdělením za následujících předpokladů:

1. Obchodní sdělení bylo učiněno zejména elektronickou poštou, telefonem anebo faxem.
2. Z obsahu obchodního sdělení vyplývá, že podporuje, ať přímo či nepřímo, zboží či služby nebo image podnikatelského subjektu. Pokud uvedená podmínka není splněna, nelze za obchodní sdělení považovat uvedení pouhé e-mailové či webové adresy jako kontaktních údajů v elektronické korespondenci.
   Do působnosti Úřadu nenáleží šíření obchodního sdělení podporujícího zboží, služby anebo image osob vykonávajících regulované činnosti (např. lékaři, advokáti apod.), neboť tato náleží příslušné profesní samosprávné komoře zřízené zvláštním zákonem.
3. Subjekt, který šíří obchodní sdělení, musí podléhat právnímu řádu České republiky.

Pro rychlé a účinné přezkoumání podání lze doporučit:

1. Uvést všechny požadované informace v připraveném formuláři.

2. Přiložit, pokud je to možné, všechny dostupné, ve věci důležité doklady, případně uvést, kde lze získat důkazní materiály. Pro předání informací o obchodním sdělení, které bylo zasláno elektronickou poštou a jehož šíření je předmětem podání, tak, aby byly zaslány všechny potřebné údaje, jsou nezbytné následující kroky: *ve formuláři v bodě 3. vložit kopii hlavičky e-mailové zprávy, která obsahovala předmětné obchodní sdělení a v bodě 5. vložit kopii obchodního sdělení a případnou přílohu zprávy*
3. Uvést, zda, a případně jaké, kroky již byly osobou zasílající podání (případně jinou osobou) ve věci učiněny.
4. V případě telefonického podání je nezbytná následná komunikace (zaslání důkazních materiálů, příp. osobní projednání a sepsání úředního záznamu).

Úřad je povinen podání posoudit dle obsahu a v návaznosti na to učinit další kroky vedoucí k dozorovým, nápravným a sankčním opatřením. Ten, kdo učinil podání, bude písemně informován o výsledku prověření podnětu, a to na jím uvedenou kontaktní adresu.

Pokud osoba, která obdržela nevyžádané obchodní sdělení, požaduje omluvu či finanční úhradu, je nutno upozornit, že v takovém případě je třeba se obrátit na soud, neboť Úřad není oprávněn rozhodovat o nárocích satisfakční povahy. Úřad není ani orgánem činným v trestním řízení. Osoba, která učinila podání, ani osoba, která pociťuje šíření obchodních sdělení jako újmu, nemají v průběhu kontrolních a sankčních řízení prováděných Úřadem postavení účastníků těchto řízení, nejsou proto oprávněny podávat opravné prostředky, když Úřad svým postupem neuspokojí jejich požadavky a očekávání. Ovšem v případě, že sdělí nové závažné a podstatné skutečnosti, je Úřad připraven se věcí znovu zabývat.

Stížnosti na šíření obchodních sdělení v oblasti regulovaných činností, které nejsou ve věcné působnosti Úřadu, budou předány příslušným profesním komorám zřízeným na základě zákona. Stížnosti na šíření obchodních sdělení subjekty, které nesídlí na území České republiky a jsou umístěny v zemích Evropské unie, budou předány orgánům v členských státech Evropské unie.

3. Vzor formuláře k podání stížnosti

Podávám stížnost týkající se šíření obchodního sdělení podle zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), dále jen „zákon“, a v této souvislosti uvádím(e) následující:

1. Obchodní sdělení jsem (jsme) obdržel(i) prostřednictvím následujícího elektronického kanálu:
(alespoň jeden údaj povinný)
☐ e-mail
☐ SMS
☐ MMS
☐ telefonické volání
☐ fax
Jiný (popis): ☐

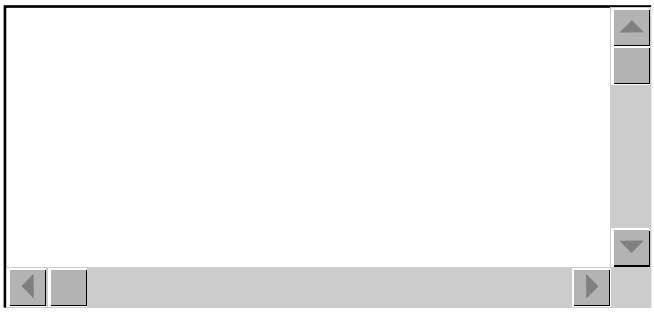
2. Obchodní sdělení nesplňuje podle mého(našeho) názoru tyto požadavky zákona:
☐ nikdy jsem (jsme) nedal(i) souhlas odesilateli k zaslání obchodního sdělení
☐ odesílatel nereagoval na dřívější odmítnutí zasílání sdělení
☐ není zřetelně a jasně označeno, že se jedná o obchodní sdělení
☐ sdělení skrývá nebo utajuje totožnost odesilatele, jehož jménem se komunikace uskutečňuje
☐ sdělení neobsahuje platnou adresu pro odmítnutí dalších sdělení
Další: ☐

3. Údaje o odesilateli obchodního sdělení:
(alespoň jeden údaj povinný)
kopie hlavičky e-mailu

☐ telefonní číslo
☐ faxové číslo
☐ jiné

4. Obdobné obchodní sdělení od tohoto odesílatele jsem(jsme) dostal(i) již dříve:
(pouze jeden údaj povinný)
ano – ojediněle
ano – často
ne
nevím

5. Kopie (nebo obsah) sdělení v případě e-mailu, v ostatních případech popis sdělení:
(povinný údaj, nevztahuje se na přílohu)



Příloha (maximálně 500 kB):
*(z technologických a bezpečnostních důvodů nebude tato položka při **chybném** odeslání formuláře zapamatována a je nutné ji zadat znovu)*

6. Kontakt na stěžovatele:

- Příjmení, jméno, (Název)
- Adresa
- Tel.číslo
- e-mail

7. Doplňující informace:

8. Kontrolní kód:

(povinný údaj, přepište kód do políčka pod obrázkem)

Poznámka: Výše uvedený formulář je k dispozici na internetové adrese Úřadu www.uoou.cz/spam.php3. Úřad ovšem přijímá stížnosti občanů i v klasické písemné podobě (poštou či faxem – viz tiráž).

PRACOVNÍ SKUPINA PRO OCHRANU DAT PODLE ČLÁNKU 29

11750/02/EN
WP 89

Stanovisko č. 4/2004
ke zpracování osobních údajů prostředky kamerového sledování

Přijato dne 11. února 2004

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 14 směrnice 97/66/ES.

Sekretariát poskytuje Evropská komise, Generální ředitelství pro vnitřní trh, Ředitelství E (Služby, duševní a průmyslové vlastnictví, média a ochrana dat), B-049 Brusel, Belgie, Úřadovna č. C100-6/136.

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

PRACOVNÍ SKUPINA PRO OCHRANU FYZICKÝCH OSOB PŘI ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

ustavená směrnicí 95/46/ES Evropského parlamentu a Rady z 24. října 1995,[1)]

s ohledem na články 29 a 30 odst. 1 písm. a) a odst. 3 uvedené směrnice,

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

PŘIJALA TOTO STANOVISKO:

1. ÚVOD

Soukromé a veřejné orgány v Evropě začaly v posledních letech v rostoucí míře využívat systémů k pořizování obrazových záběrů. Tato skutečnost vedla k živé diskusi jak na úrovni Společenství, tak v jednotlivých členských státech. Cílem diskuse bylo stanovit předpoklady a omezení týkající se instalace zařízení pro kamerové sledování a také nezbytná ochranná opatření pro subjekty údajů.

Poznatky získané v posledních letech, včetně období po zavedení směrnice 95/46/ES do vnitrostátních předpisů, ukazují, že došlo k velkému využívání uzavřených okruhů, kamer a jiných ještě důmyslnějších zařízení, která se používají v různých oblastech.

Rozvoj dostupné technologie, digitalizace a miniaturizace navíc značně rozšiřuje možnosti obrazových a zvukových záznamových systémů také v souvislosti s jejich využitím v interních sítích a na Internetu.

Kromě zpracování údajů v rámci pracovního poměru, které již řešila Pracovní skupina ve svém podrobném dokumentu (Stanovisko č. 8/2001 ke zpracování osobních údajů v oblasti zaměstnávání[2)])*, si občané jistě povšimli, že dochází ke stále častějšímu používání různých forem kamerového sledování. Roste také vzájemné propojení systémů kamerového sledování.

Z namátkové analýzy hlavních aplikací vyplývá, že kamerové sledování může sloužit řadě různých účelů,[3)] které lze seskupit do několika hlavních kategorií:

1) ochrana jednotlivců,
2) ochrana majetku,
3) veřejný zájem,
4) odhalování, prevence a stíhání trestné činnosti,
5) získávání důkazů,
6) jiné legitimní zájmy.

Pro instalaci videokamer a podobných zařízení také platí různé podmínky.

V ojedinělých případech může být používání obrazového záznamového systému dokonce povinné, a to na základě zvláštních ustanovení členských států – tak je tomu např. v některých kasinech – nebo může sloužit zvláště důležitým účelům z hlediska osob příbuzných subjektům údajů – např. v souvislosti s pátráním po pohřešovaných dětech a dospě-

---

1) *Úřední věstník č. L 281 z 23.11.1995, str. 31, k dispozici na: http://europa.eu.int/comm/internal_market/en/dataprot/index.htm stránce Evropské komise „Europa“.*

2) *WP 48, přijato dne 13. září 2001, k dispozici na: http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm*

3) *Různé systémy kamerového sledování jsou instalovány:*
a) uvnitř nebo v blízkosti veřejných a/nebo veřejně dostupných budov, jako jsou muzea, modlitebny, památníky a v jejich blízkosti, s cílem předejít trestným činům a/nebo drobnějším formám vandalismu,
b) na stadionech a ve sportovních objektech, zejména v souvislosti s konkrétními akcemi,
c) v sektoru dopravy a v souvislosti se silniční dopravou, s cílem sledovat provoz na silnicích a dálnicích, nebo případně s cílem odhalit případy překročení povolené rychlosti a/nebo porušení dopravních předpisů v centrech měst, či ke kontrole podzemních prostor metra, sledování benzínových čerpacích stanic a vnitřních prostor vozů taxi,
d) s cílem předcházet protiprávnímu jednání v okolí škol a také obtěžování nezletilých a/nebo takové jednání odhalit,
e) v zdravotnických zařízeních v průběhu operací a/nebo s cílem např. poskytovat vzdálenou péči nebo monitorovat pacienty na jednotkách intenzivní péče a/nebo v prostorách, kde jsou hospitalizováni vážně nemocní pacienti a/nebo pacienti v karanténě,
f) na letištích, trajektech a v blízkosti hraničních oblastí, s cílem sledovat pašování a usnadnit pátrání po nezletilých a jiných pohřešovaných osobách,
g) soukromými detektivy,
h) v supermarketech a obchodech a v jejich blízkosti, zejména v případě prodeje luxusního zboží, s cílem zajistit důkazy v případě spáchání trestného činu a také za účelem prodeje zboží a/nebo získání profilu zákazníků,
i) v soukromých bytech a jejich sousedství z bezpečnostních důvodů a s cílem zajistit důkazy v případě spáchání trestného činu,
j) k novinářským a reklamním činnostem, které se uskutečňují on-line, prostřednictvím webových kamer nebo on-line kamer používaných k propagaci turistiky a reklamním účelům, mj. například v pobřežních hotelech a tančírnách; dochází zde k natáčení zákazníků a návštěvníků v pravidelných intervalech, a to bez jakéhokoli upozornění.

lých. Na druhé straně lze uvést i neobvyklé případy použití takovýchto systémů, zejména ve třetích zemích, kde byly zřízeny systémy rozpoznávání obličeje k prevenci bigamie, anebo v případech, kdy se místní policejní orgány rozhodly zveřejnit, bez souhlasu odsouzených, obrázky dokumentující tvrdý život ve věznicích.

Kamerové sledování může tedy být v některých případech do určité míry odůvodněné, existují však i případy, kdy mají videokamery sloužit k ochraně osob, aniž by však byly dostatečně zváženy potřebné předpoklady a nezbytná opatření. To je v některých případech způsobeno ekonomickými zájmy, jež jsou sledovány ve velkém měřítku veřejnými orgány, a také nabídkou lepších pojistných podmínek v případě použití systémů kamerového sledování.

Kamerové sledování má také psychologický účinek, neboť je v některých případech považováno veřejností, ať už oprávněně či nikoli, za „nedocenitelný nástroj“, který se osvědčil při odhalování trestné činnosti.

Jedná se tedy o rozmanitou a stále se rozvíjející oblast, ve které je již nyní k dispozici řada různých zařízení.

Tento pracovní dokument by měl poskytnout úvodní rozbor, počínaje existencí částečně odlišných předpisů a příliš podrobných ustanovení jednotlivých vnitrostátních zákonů, které vyžadují systematičtější a více sladěný přístup.

Tento pracovní dokument je zaměřen na sledování, jehož cílem je vzdálené monitorování různých akcí, situací a událostí, a nezaměřuje se přímo na jiné případy, kdy jsou určité akce příležitostně a/nebo tendenčně zveřejňovány například v souvislosti s transparentností činnosti místních úřadů a/nebo parlamentních orgánů.

Každý provozovatel bude schopen dále rozvíjet úvahy, které jsou zde uvedeny, a to jak v příslušném sektoru, tak i s ohledem na budoucí technologický rozvoj , který hodlá Pracovní skupina studovat.

Zásady uvedené v tomto dokumentu se týkají i pořizování obrazových záznamů, případně ve spojení se zvukem a/nebo biometrickými údaji, jako jsou například otisky prstů.[4)]

Výše uvedené zásady lze brát v potaz případně také ve spojení se zpracováním osobních údajů, které není uskutečňováno pomocí kamerového zařízení, nýbrž jinými způsoby sledování, tzn. prostřednictvím dálkové kontroly – jako v případě satelitních systémů GPS.

Cílem tohoto pracovního dokumentu je především upozornit na širokou škálu kritérií, jež slouží k hodnocení zákonnosti a oprávněnosti instalace jednotlivých systémů kamerového sledování.

V potaz byly však brány i následující aspekty:

a) příslušné instituce členských států musí hodnotit kamerové sledování z obecného hlediska, také s cílem podporovat globálně selektivní a systematický přístup k této otázce. Přílišné rozšíření systémů pořizování obrazových záznamů ve veřejných a soukromých oblastech by nemělo vést k neoprávněným omezením práv a základních svobod občanů; občané by jinak byli nuceni se podrobit nepřiměřenému shromažďování osobních údajů, jež by umožnilo hromadnou identifikaci občanů v řadě veřejných a soukromých míst.
b) trendy rozvoje metod kamerového sledování by mohly být účelně vyhodnocovány, aby se zabránilo tomu, že vývoj softwarových aplikací, které vycházejí z rozpoznávání obličeje a studia a předpovídání zobrazeného lidského chování povede bezohledně k dynamicko-preventivnímu sledování – oproti běžnému statickému sledování, které je zaměřeno především na dokumentaci konkrétních akcí a jejich původců. Tato nová forma sledování vychází z automatického zjišťování rysů obličeje jednotlivců a jejich „neobvyklého“ chování ve spojení s automatickými varovnými výzvami a příkazy, což by mohlo vést k nebezpečí diskriminace.

2. MEZINÁRODNÍ PRÁVNÍ NÁSTROJE

a) Úmluva o lidských právech a základních svobodách
Ochrana soukromí je zaručena v článku 8 Úmluvy o lidských právech.

b) Úmluva Rady Evropy č. 108/1981 o ochraně jednotlivců se zřetelem na automatizované zpracování osobních dat.
Působnost úmluvy není omezena tak, jako je tomu u směrnice 95/46/ES, na činnosti v oblasti prvního pilíře (viz níže). Kamerové sledování, které zahrnuje zpracování osobních údajů, spadá do působnosti dané úmluvy. Konzultační výbor ustavený touto úmluvou konstatoval, že hlasy a obrazy se považují za osobní údaje, mohou-li poskytnout informace o jednotlivci tím, že umožní, byť i nepřímo, jeho identifikaci.
Rada Evropy v současné době dokončuje soubor orientačních pravidel k ochraně jednotlivců se zřetelem na shromažďování a zpracování dat prostřednictvím kamerového sledování. Tato pravidla by měla dále specifikovat ochranná opatření použitelná pro subjekty údajů, která jsou obsažena v ustanovení příslušných nástrojů Rady Evropy.

c) Listina základních práv Evropské unie
V článku 7 Listiny základních práv Evropské unie je upravena ochrana soukromého a rodinného života, obydlí a korespondence a článek 8 upravuje ochranu osobních údajů.

3. SLEDOVÁNÍ PODLE SMĚRNICE 95/46/ES

Směrnice 95/46/ES výslovně v několika ustanoveních odkazuje na specifické rysy zpracování osobních údajů, které jsou obsaženy ve zvukových a obrazových informacích.

Směrnice zaručuje ochranu soukromí a soukromého života, jakož i širší ochranu osobních údajů s ohledem na základní práva a svobody fyzických osob (čl. 1 odst. 1).

[4)] *Obecnějšími otázkami souvisejícími s aplikací směrnice 95/46/ES na biometrická data se bude Pracovní skupina zabývat ve zvláštním dokumentu.*

Značná část informací, jež jsou shromažďovány prostřednictvím kamerového sledování, se týká identifikovaných a/nebo identifikovatelných osob, které jsou filmovány při svém pohybu na veřejnosti a/nebo na veřejně přístupných místech. Takovéto osoby mohou očekávat menší stupeň soukromí, nejsou však plně zbaveny svých práv a svobod, jež se mj. týkají jejich soukromého života a vzhledu.

V potaz je v této souvislosti bráno také právo na volný pohyb osob, které se zákonně nacházejí na území určitého státu, jež je zaručeno v článku 2 Dodatkového protokolu č. 4 k Evropské úmluvě o ochraně lidských práv a základních svobod.

Tuto svobodu pohybu lze omezit pouze tehdy, je-li to nutné v zájmu demokratické společnosti a v rozsahu nezbytném pro dosažení konkrétního účelu. Subjekty údajů mají právo uplatňovat svou svobodu pohybu, aniž by procházely nadměrnými psychologickými testy s ohledem na svůj pohyb a jednání, a aniž by byly podrobovány detailnímu monitorování, které by umožňovalo sledování jejich pohybu a/nebo spuštění „poplachu“ na základě softwarových prostředků, které automaticky „interpretují“ údajně podezřelé chování osoby bez jakéhokoli lidského zásahu – na základě nepřiměřené aplikace kamerového sledování některými subjekty v řadě veřejných a/nebo veřejně přístupných prostor.

Specifičnost a citlivost zpracování zvukových a obrazových dat týkajících se fyzických osob je zdůrazněna v ustanoveních preambule směrnice. Kromě níže uvedeného rozboru působnosti tohoto předpisu, daná ustanovení preambule a relevantní články směrnice objasňují, že:

a) se směrnice vztahuje v zásadě na předmětnou oblast také s ohledem na význam vývoje technik používaných k získávání, manipulaci a jiné používání konkrétní kategorie takto shromažďovaných osobních údajů (viz bod č. 14 preambule),
b) zásady ochrany stanovené danou směrnicí se vztahují na jakékoli informace, včetně zvukových a obrazových, které se týkají identifikované nebo identifikovatelné osoby, s přihlédnutím ke všem metodám, které mohou být rozumně použity buď správcem nebo jinou osobou k identifikaci dané osoby /viz článek 2 bod a) a bod č. 26 preambule/.

Kromě výše uvedených ustanovení jsou v tomto směru zjevně relevantní ustanovení směrnice, jež se týkají zejména:

1) *Kvality údajů*. Obrazové informace musejí být zpracovávány korektně a zákonným způsobem a ke stanoveným, výslovně vyjádřeným a legitimním účelům. Obrazové informace musejí být používány v souladu se zásadou, že údaje musejí být přiměřené, relevantní a míru nepřesahující, a nesmějí být dále zpracovávány způsobem, který je neslučitelný s těmito účely; musejí být uchovávány pouze po omezenou dobu apod. (viz článek 6),
2) *Kritérií legitimace zpracování dat*. Na základě těchto kritérií je nutné, aby zpracování osobních údajů prostřednictvím kamerového sledování vycházelo alespoň z jednoho z předpokladů uvedených v článku 7 – nezpochybnitelný souhlas, zpracování nezbytné pro splnění smlouvy, splnění právní povinnosti, ochranu důležitých zájmů subjektu údajů, provedení úkolu ve veřejném zájmu nebo výkon úřední moci, vyváženost zájmů,
3) Zpracování *zvláštních kategorií údajů,* které podléhají zárukám, jež se vztahují na používání buď citlivých údajů nebo údajů týkajících se trestné činnosti v rámci kamerového sledování (dle článku 8),
4) *Informací,* které mají být poskytnuty subjektům údajů (viz články 10 a 11),
5) *Práv subjektů údajů,* zejména práva přístupu a práva vznést námitku proti zpracování na základě přesvědčivých legitimních důvodů /viz články 12 a 14 písm. a)/,
6) Záruky, které se uplatňují v souvislosti s *automatizovaně podloženými rozhodnutími* (dle článku 15),
7) *Bezpečnost* zpracování (článek 17),
8) *Oznámení o zpracování* (dle článků 18 a 19),
9) *Předběžné kontroly* zpracování, které by mohlo představovat zvláštní rizika z hlediska práv a svobod subjektu údajů (podle článku 20), a
10) *Předávání osobních údajů do třetích zemí* (dle článku 25 a násl.).

Specifičnost a citlivost zpracování zvukových a obrazových údajů je zmíněna i v posledním článku směrnice, ve kterém se Komise zavazuje přezkoumávat zejména uplatňování směrnice v této oblasti a případně předkládat vhodné návrhy, které se projeví jako nezbytné, s ohledem na vývoj technologií a úroveň pokroku informační společnosti (článek 33).

4. NÁRODNÍ USTANOVENÍ TÝKAJÍCÍ SE KAMEROVÉHO SLEDOVÁNÍ

V některých členských státech již byly provedeny případové studie týkající se kamerového sledování, buď na základě ústavních ustanovení[5)] nebo konkrétních právních předpisů, anebo na základě nařízení a jiných rozhodnutí vydaných příslušnými národními orgány.[6)]

V některých zemích existují také zvláštní ustanovení, jež platí bez ohledu na to, zda kamerové sledování zahrnuje zpracování osobních údajů či nikoli. Podle těchto předpisů se k instalaci a umístění uzavřeného televizního okruhu nebo podobného sledovacího zařízení vyžaduje předchozí souhlas správního orgánu, kterým je zcela nebo zčásti národní úřad pro ochranu osobních údajů. Tyto předpisy se mohou navzájem lišit s ohledem na veřejnou či soukromou povahu subjektu, který odpovídá za provoz daného zařízení.

V jiných zemích není zatím kamerové sledování upraveno zvláštním zákonem; úřady pro ochranu osobních údajů však zajišťují vhodnou aplikaci obecných ustanovení o ochraně dat mimo jiné formou vydávání stanovisek, pravidel a etických kodexů – ta již byla například přijata ve Spojeném království a ve formě návrhu byla předložena v Itálii.

---

5) *Viz rozhodnutí portugalského Ústavního soudu č. 255/2002. Soud rozhodl, že „používání elektronických sledovacích přístrojů a monitorování občanů soukromými bezpečnostními orgány omezuje právo na ochranu soukromého života stanovené v článku 26 Ústavy“.*

6) *Přinejmenším v jedné zemi (Belgie – případ Gaia) vedlo porušení předpisů na ochranu údajů při pořizování obrazových záběrů k odmítnutí přípustných důkazů soudem.*

Belgie	Stanoviska úřadu pro ochranu dat (Data Protection Authority, dále jen „DPA“), zejména stanovisko č. 34/99 z 13. prosince 1999, které se týká zpracování obrazových informací zejména pomocí systémů kamerového sledování; stanovisko č. 3/2000 z 10. ledna 2000, které se týká používání systémů kamerového sledování ve vstupních halách obytných budov.
Dánsko	Konsolidovaný zákon č. 76 z 1. února 2000 o zákazu kamerového sledování. Tento zákon obecně zakazuje soukromým subjektům provádět sledování pomocí videokamer na veřejných ulicích, silnicích, náměstích nebo jakýchkoli veřejných podobných místech. Z tohoto zákazu však existují určité výjimky. Rozhodnutí DPA z 3. června 2002 o kamerovém sledování ve velké skupině supermarketů a o živých přenosech z restaurací na Internetu. Rozhodnutí DPA z 1. července 2003, kterým se stanoví, že kamerové sledování ve veřejné dopravě provozované soukromým subjektem musí být přiměřené a musí splňovat pravidla upravená v dánském zákoně o ochraně osobních údajů. Rozhodnutí DPA z 13. listopadu 2003, kterými se stanoví určitá omezení pro kamerové sledování uskutečňované veřejnými orgány.
Finsko	Ve Finsku neexistuje žádný zvláštní právní předpis upravující kamerové sledování, řada různých zákonů však obsahuje ustanovení o kamerovém sledování a jiných metodách technického dozoru, pozorování či monitorování. Otázky ohledně kamerového sledování a uchovávání záznamů jsou relativně časté; několik případů již bylo v tomto směru řešeno. Například ombudsman pro ochranu osobních údajů vydal své stanovisko k pořizování záznamů telefonních hovorů v rámci služeb pro zákazníky a v pracovním poměru (č.j.1061/45/2000 a 525/45/2000). Finsko vydalo brožuru s názvem „Soukromí při kamerovém sledování“ (Asiaa tietosuojasta 4/2001 Yksityisyyden suoja kameravalvonnas sa http://www.tietosuoja.fi/uploads/03wamgvxuybt4ti.rtf).
Francie	Zákon č. 78-17 z 6. ledna 1978, o zpracování, evidenci a svobodách (CNIL). Doporučení DPA č. 94-056 z 21. června 1994. Směrnice DPA týkající se kamerového sledování na pracovišti: http://www.cnil.fr/thematic/index.htm; o jiných otázkách (tzn. webové kamery)[7)] Zvláštní zákon o kamerovém sledování z důvodů veřejné bezpečnosti na veřejných místech: zákon č. 95-73 z 21. ledna 1995, o bezpečnosti (ve znění nařízení 2000-916 z 19. září 2000). Vyhláška č. 96-926 ze 17. října 1996 a oběžník z 22. října 1996 o provedení zákona č. 95-73
Řecko	1) Dopis č. 390 z 28. ledna 2000, o instalaci uzavřeného televizního okruhu v aténském metru 2) Směrnice č. 1122 z 26. září 2000 o uzavřených televizních okruzích 3) Rozhodnutí č. 84/2002, o uzavřených televizních okruzích v hotelech.
Německo	Článek 6 písm. b spolkového zákona z roku 2001. Článek 25 zákona o ochraně hranic. Další ustanovení o kamerovém sledování policií v policejních zákonech spolkových zemí. Návrh zákona, kterým se zakazuje tajné kamerové sledování je projednáván v parlamentu.
Irsko	Zákony o ochraně osobních údajů z let 1998 a 2003. Případová studie č. 14/1996 (používání uzavřených televizních okruhů).
Itálie	Článek 134 Zákoníku o ochraně osobních údajů (legislativní vyhláška č. 196 z 30. června 2003 kterou se přijímají pravidla jednání). Rozhodnutí úřadu pro ochranu dat č. 2 z 10. dubna 2002 (na podporu přijetí pravidel jednání), z 28. září 2001 (biometrické údaje a metody rozpoznávání obličeje používané bankami) a z 29. listopadu 2000 (tzv. „dekalog kamerového sledování“). Výnos prezidenta č. 250 z 22. 6. 1999 (kterým se upravuje příjezd vozidel do centra měst a oblastí s omezeným přístupem) Vyhláška č. 433 z 14.11.1992 a zákon č. 4/1993 (který se vztahuje na muzea, státní knihovny a archivy) Legislativní vyhláška č. 45 z 4. 2. 2000 (osobní lodi na vnitrostátních trasách) Článek 4 zákona č. 300 z 20.5.1970 (tzv. Zákon o pracujících)
Lucembursko	Články 10 a 11 zákona z 2. 8. 2002 o ochraně osob při zpracování osobních údajů.
Nizozemsko	Zpráva úřadu pro ochranu osobních údajů vydaná v roce 1997 obsahuje směrnice pro kamerové sledování, zejména na ochranu osob a majetku na veřejných místech. Směrnice z roku 1997 budou novelizovány v roce 2004. Průzkum kamerového sledování ve všech nizozemských obcích v roce 2003. Dolní sněmovna nedávno schválila změnu trestního zákoníku s účinností od 1. ledna 2004, kterou se rozšiřuje skutková podstata trestného činu pořizování záběrů míst přístupných veřejnosti bez jejího informování. Vláda navrhuje změnu zákona o místní správě, kterou by městské úřady a starostové získali za určitých podmínek (např. povinnost

[7)] *Viz výroční zprávy francouzské Commission Nationale de l'Informatique et des Libertés.*

	pravidelně vyhodnocovat efektivitu kamerového sledování) výslovnou pravomoc používat systémy kamerového sledování na veřejných místech k veřejným účelům.
Portugalsko	Zákonná vyhláška č. 231/98 z 22. července 1998 (soukromé bezpečnostní činnosti a systémy vlastní ochrany). Zákon č. 38/98 z 4. srpna 98 (opatření, jež mají být přijata v případě násilí spojeného se sportovními akcemi) Zákonná vyhláška č. 263/01 z 28. září 2001 (tančírny). Zákonná vyhláška č. 94/2002 z 12. dubna 2002. (sportovní akce)
Španělsko	Zákon č. 4/1997 (kamerové sledování bezpečnostními agenturami na veřejných místech) Královský výnos č. 596/1999, kterým se provádí zákon č. 4/1997
Švédsko	Kamerové sledování je specificky upraveno zákonem (1998:150) o běžném kamerovém sledování a zákonem (1995:1506) o tajném kamerovém sledování (v trestním vyšetřování).[8)] Pro běžné kamerové sledování se obvykle vyžaduje povolení okresního správního výboru. Takové povolení však není nutné např. u pošt, bankovních poboček a obchodů. Tajné kamerové sledování musí povolit soud. Proti rozhodnutí okresního správního výboru se lze odvolat k Soudnímu kancléři. Pořizování videozáznamů s použitím digitální techniky se považuje za zpracování osobních údajů a vztahuje se proto na něj dohled Úřadu pro kontrolu údajů (Data Inspection Board), nepodléhá-li tato činnost zvláštní úpravě v zákoně o běžném kamerovém sledování. Vyšetřovací komise vydala o kamerovém sledování zprávu (SOU 2002:110).
Spojené království	Kodex používání uzavřených televizních okruhů z roku 2000 (Komisař pro informace), v současné době probíhá jeho revize.

Další důležité regulační nástroje byly přijaty na Islandu (článek 4 zákona č. 77/2000), v Norsku (Hlava VII zákona č. 31 z 14. 4. 2000), ve Švýcarsku (doporučení Federálního komisaře) a v Maďarsku (doporučení DPA z 20. 12. 2000).

5. OBLASTI, KDE NELZE SMĚRNICI 95/46/ES ZCELA NEBO ČÁSTEČNĚ POUŽÍT

Směrnice se nevztahuje na zpracování zvukových a obrazových údajů pro účely související s veřejnou bezpečností, obranou, bezpečností státu a jinými činnostmi státu v oblasti trestního práva a/nebo při jiné činnosti, která nespadá do působnosti komunitárního práva.[9)] Řada členských států však při zavádění směrnice 95/46/ES tyto otázky upravuje obecně, i když s některými výjimkami:

A) V některých zemích musí zpracování údajů pro výše uvedené účely v každém případě odpovídat Úmluvě č. 108/1981 a příslušným doporučením Rady Evropy, jakož i některým národním ustanovením (viz článek 3 odst. 2 a bod č. 16 preambule směrnice 95/46/ES). S ohledem na její zvláštní rysy a existenci zvláštních ustanovení, která se také týkají vyšetřovacích aktivit policie a soudních orgánů, a také pro účely bezpečnosti státu[10)] – které mohou zahrnovat kamerové sledování, které je „skryté“, tzn. bez informování na daném místě – nebude tato kategorie zpracování v tomto dokumentu podrobně řešena.

Pracovní skupina však chce zdůraznit, že podobně jako u některých jiných druhů zpracování osobních údajů, které také nespadají do působnosti směrnice, by kamerové sledování prováděné na základě požadavků na veřejnou bezpečnost nebo k odhalování, prevenci a kontrole trestné činnosti mělo odpovídat požadavkům stanoveným v článku 8 Úmluvy o lidských právech a základních svobodách. Mělo by také být upraveno zvláštními předpisy, které jsou veřejně známé, a které souvisejí s prevencí konkrétních rizik a specifických trestných činů a těmto rizikům a činům odpovídat např. v místech, jež jsou vystavena takovýmto rizikům nebo v souvislosti s veřejnými akcemi, které by mohly vést k takové trestné činnosti.[11)] Je třeba také přihlížet k dopadům systémů kamerového sledování např. ke skutečnosti, že protiprávní činnost se může přesunout do jiných oblastí či míst, a že by vždy měl být jasně

---

8) *Ve Švédsku se pro běžné kamerové sledování vyžaduje v zásadě povolení okresního správního výboru; existuje však řada výjimek, např. s ohledem na sledování pošt, bankovních poboček a obchodů. Tajné kamerové sledování musí povolit soud. Proti rozhodnutí okresního správního výboru podle zákona o běžném kamerovém sledování se lze odvolat k Soudnímu kancléři z důvodu ochrany veřejných zájmů. Pořizování videozáznamů s použitím digitálních kamer se považuje za zpracování osobních údajů ve smyslu švédského zákona o ochraně osobních údajů a podléhá proto dohledu ze strany Úřadu pro ochranu osobních údajů. Vyšetřovací komise v současné době analyzuje používání kamerového sledování z hlediska prevence trestné činnosti. Komise mj. hodnotí zákon o běžném kamerovém sledování z hlediska případné potřeby jeho novelizace. Vyšetřovací komise také analyzuje působnost švédského zákona o ochraně osobních údajů s ohledem na kamerové sledování a případnou nutnost přijetí zvláštních předpisů upravujících zpracování osobních údajů v souvislosti s kamerovým sledováním.*

9) *Viz bod č. 16 preambule.*

10) *Na tomto místě lze uvést zásady stanovené Evropským soudem pro lidská práva v případu Rotaru v. Rumunsko, který byl řešen dne 4. května 2000. Viz výše.*

11) *Např. oběžník vydaný ve Francii dne 22. 10. 1996 s ohledem na izolovaná místa a obchody, které jsou otevřeny pozdě večer.*

určen správce údajů tak, aby subjekty údajů mohly uplatnit svá práva.

Poslední požadavek souvisí také s tím, že kamerové sledování používají stále více společně policejní a jiné veřejné orgány (např. místní úřady) a/nebo soukromé orgány (banky, sportovní asociace, dopravní společnosti), což přináší riziko zamlžení úkolů a odpovědnosti jednotlivých subjektů.[12)]

B) Směrnice se nevztahuje na zpracování, které provádí fyzická osoba výlučně v rámci osobních nebo domácích činností (viz článek 3 odst. 2 a bod 12 preambule).

Zatímco výše uvedené činnosti mohou spočívat např. v kamerovém sledování za účelem vzdálené kontroly domácnosti např. k prevenci krádeží nebo v souvislosti s řízením tzv. e-rodiny. Není tomu tak v případě, kdy jsou kamery instalovány buď mimo soukromé prostory, nebo v jejich blízkosti s cílem zajistit ochranu majetku a/nebo bezpečnost.

V takovém případě se může především stát, že systém neumístí jednotliví vlastníci u dveří do svého obydlí, nýbrž jej použije několik vlastníků společně na základě vzájemné smlouvy či konsorcium nebo vlastníci obytné budovy s cílem monitorovat několik vchodů a prostor v dané budově zároveň. Takové činnosti podléhají ustanovením směrnice.

Je-li takový systém používán ve prospěch jediné rodiny a ke sledování jediných dveří, podesty, parkoviště apod., skutečnost, že se směrnice v takovém případě neuplatní z důvodu výlučně osobního využití systému a nedostupnosti údajů třetím osobám, nezbavuje správce systému povinnosti respektovat legitimní práva a zájmy svých sousedů a ostatních procházejících osob. V členských státech EU jsou tato práva a zájmy chráněny bez ohledu na zásady ochrany údajů obecnými (občanské právo) ustanoveními, jež chrání osobní práva, vzhled, rodinný život a soukromí. Jako příklad lze uvést nastavení zorného pole kamery nainstalované před dveřmi do bytu, které umožňuje systematicky sledovat klienty lékařské kliniky a/nebo advokátní kanceláře, jež se nacházejí na stejném patře, čímž dochází k neoprávněnému zásahu do profesního tajemství.

Zvláštní pozornost bude třeba věnovat orientaci kamerového zařízení, nutnosti vyvěšení oznámení a informací a včasnému mazání nahrávek, a to do několika hodin, – nedojde-li ke vloupání ani jiné trestné činnosti.

C) Článek 9 směrnice předpokládá, že členské státy stanoví výjimky či odchylky od některých ustanovení směrnice v případech, kdy je zpracování prováděno výlučně pro novinářské či literární účely nebo uměleckou činnost, zejména v oblasti audiovizuální tvorby (viz bod č. 17 preambule). Je třeba stanovit pouze výjimky nezbytné k zaručení práva na soukromí v rámci pravidel, jimiž se řídí svoboda projevu.[13)] V této souvislosti bude třeba věnovat zvláštní péči zejména instalaci webových kamer a/nebo on-line kamer, s cílem zamezit chybám a nedostatkům při ochraně osob, které jsou sledovány kamerovými systémy za účelem, kterým může být například reklama a/nebo propagace turistiky.[14)]

6. KAMEROVÉ SLEDOVÁNÍ A ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

S ohledem na různé, výše uvedené situace, chce Pracovní skupina upozornit na skutečnost, že směrnice 95/46/ES se vztahuje na zpracování osobních údajů, včetně obrazových a zvukových dat získaných pomocí uzavřených televizních okruhů a jiných systémů kamerového sledování, zcela nebo zčásti automatickými prostředky, a na jiné zpracování osobních údajů než automatickými prostředky, které tvoří součást evidenčního systému nebo které má tvořit součást takového systému.

Obrazové a zvukové údaje, které se týkají identifikovaných nebo identifikovatelných fyzických osob, jsou osobními údaji:

a) i pokud jsou záběry používány v rámci uzavřeného televizního okruhu, a to i pokud nejsou spojeny s údaji o dané osobě,
b) i pokud se netýkají osob, jejichž obličeje byly nafilmovány, avšak obsahují jiné informace jako např. státní poznávací značky vozidel nebo čísla PIN získaná v souvislosti se sledováním bankomatů,
c) bez ohledu na média používaná ke zpracování (např. pevné a/nebo mobilní obrazové systémy, jako jsou přenosné videopřijímače, systémy barevných a/nebo černobílých obrazů – používané techniky – kabelová zařízení nebo systémy s optickými vlákny – druh zařízení – stacionární, rotující, mobilní – aspekty záznamu obrazových informací – např. nepřetržité či naopak přerušované pořizování záznamů, jako např. v případě pořízení záznamu jen při překročení povolené rychlosti, což nemá nic společného s náhodným, dílčím pořizováním záběrů – a používané komunikační nástroje, např. spojení s „centrem“ a/nebo“ zasílání obrazových záznamů na vzdálené terminály apod.).

Možnost identifikace ve smyslu směrnice může také vycházet ze spojení údajů s informacemi, které jsou v držení třetích osob, nebo v jednotlivých případech z použití zvláštních technik a/nebo přístrojů.

[12)] *Významné riziko s sebou přinášejí například činnosti některých obcí v Itálii, které monitorují kamerovými systémy veřejná místa, kde se v noci vyskytují prostitutky. Řada obcí v minulosti uvedla, že mají - což je sporné - pravomoc v oblasti prevence tohoto jevu, zatímco jiné obce vydaly nařízení, jimiž pouze zakázaly klientům prostitutek parkovat a/nebo projíždět svými vozidly danými oblastmi a hrozily v případě neuposlechnutí zasláním fotografií na jejich domácí adresu. Italský úřad vydal v tomto směru rozhodnutí, jež mělo za cíl vyjasnit možnost stíhání pro porušení příslušných ustanovení.*

[13)] *Viz doporučení 1/97 Pracovní skupiny pro legislativu pro ochranu dat a média.*

[14)] *Webová kamera, která byla tajně nainstalována poblíž schodiště vedoucího ze stanice metra v Milánu zaznamenávala intimní partie procházejících žen za účelem, který jen zdánlivě souvisel s novinářskou činností, a tyto obrázky byly přímo vysílány na internetu. Skutečnost, že dané osoby nebylo možno identifikovat, neumožnila národnímu úřadu pro ochranu údajů v této souvislosti zasáhnout.*

Jedním z prvních opatření, které musí správce dat přijmout, je kontrola, zda kamerové sledování zahrnuje zpracování osobních údajů z toho důvodu, v daném případě použijí bez ohledu na národní ustanovení, která navíc vyžadují povolení z důvodů veřejné bezpečnosti.

Tak tomu může být např. v případě zařízení, které je umístěno u vchodu nebo uvnitř banky, umožňuje-li toto zařízení identifikaci zákazníků; naopak, za určitých okolností může být aplikace směrnice vyloučena v případě leteckých snímků, které nelze dostatečně zvětšit nebo které nezahrnují informace týkající se fyzických osob, např. snímky pořizované k identifikaci vodních zdrojů nebo skládek, a v případě otočných zařízení, která pořizují snímky různých situací v silniční dopravě.

7. POVINNOSTI A ODPOVÍDAJÍCÍ OPATŘENÍ ZE STRANY SPRÁVCE ÚDAJŮ

A) Zákonnost zpracování

Také s ohledem na požadavek zákonnosti zpracování údajů /dle článku 6 písm. a) směrnice/ musí správce údajů předem ověřit, zda sledování odpovídá obecným a zvláštním ustanovením platným pro daný sektor – jako jsou zákony, nařízení, etické kodexy s právní relevancí. Tato ustanovení mohou být upravena v souvislosti s veřejnou bezpečností a také k jiným účelům, které nesouvisejí s ochranou osobních údajů – např. nutnost získání zvláštních povolení od konkrétních správních orgánů a splnění jejich pokynů.

Je třeba přijmout všechna vhodná opatření k tomu, aby kamerové sledování odpovídalo zásadám ochrany údajů a je třeba zamezit nevhodným zásahům do soukromí.[15)]

V této souvislosti je třeba také přihlížet k nejlepším postupům, jež jsou případně upraveny v doporučeních vydaných orgány dozoru, a k jiným seberegulačním nástrojům.

Je také třeba ověřit jiná ustanovení vnitrostátního práva, včetně ústavních zásad, občanskoprávních a trestněprávních ustanovení, s ohledem zejména na ustanovení upravující „droit à l'image“[16)] (doslova „právo na obrázek“, pozn. překladatele) nebo na ochranu obydlí; je třeba přihlédnout k relevantní judikatuře, jež může obsahovat rozhodnutí, podle nichž se prostory mimo obydlí, např. hotelové pokoje, kanceláře, toalety, šatny, telefonní budky uvnitř budovy apod., považují za soukromé prostory.

V případech, kdy bylo zařízení nainstalováno soukromými subjekty nebo veřejnými orgány, zejména místními úřady, údajně z důvodů zabezpečení nebo případně odhalování, prevence a kontroly trestné činnosti, je třeba při stanovení daného účelu a poskytování informací o tomto účelu věnovat zvláštní pozornost stanovení činností, jež mohou být zákonným způsobem prováděny správcem údajů – vzhledem k tomu, že některé veřejné funkce lze vykonávat pouze na základě zákona konkrétními neadministrativními orgány, jako jsou např. policejní orgány.

Tato otázka byla vznesena zejména s ohledem na činnost některých místních orgánů, které nemají přímou pravomoc ve vztahu k veřejnému pořádku a k otázkám veřejné bezpečnosti a které přesto provádějí některé dílčí činnosti za účelem veřejného dohledu. Podobně, kamerové sledování, které je odůvodňováno kontrolou trestné činnosti, je často ve skutečnosti zaměřeno na získávání důkazů o spáchaných trestných činech.

B) Specifičnost, specifikace a zákonnost účelů

Správce údajů by měl zajistit, aby sledovaný účel nebyl nejasný ani nejednoznačný, a to i proto, aby měl k dispozici jasné kritérium pro hodnocení slučitelnosti účelů sledovaných zpracováním údajů /viz článek 6 písm. b) směrnice/.

Tato analýza je nezbytná také s ohledem na uvedení účelu jak v rámci informování subjektů údajů a v rámci příslušného oznámení, tak v souvislosti s předběžnou kontrolou, která může být provedena s ohledem na zpracování v souladu s ustanoveními článku 20 směrnice.

Je třeba jasně vyloučit použití shromážděných obrazových údajů k jiným účelům, zejména s ohledem na možnosti technické reprodukce např. formou výslovného zákazu kopírování.

Příslušné účely by měly být uvedeny v dokumentu, v jehož rámci by měly být shrnuty také ostatní důležité aspekty politiky ochrany soukromí s ohledem na důležité otázky, jako je zaznamenání času, kdy byly záběry smazány, možné žádosti o přístup ze strany subjektů údajů a/nebo zákonné sdělení údajů.

C) Kritéria zajišťující legitimitu zpracování

Správce údajů by měl ověřit, zda kamerové sledování splňuje nejen konkrétní ustanovení uvedená v bodu A), ale také přinejmenším jedno z kritérií zajišťujících legitimitu zpracování podle článku 7 směrnice, konkrétně s ohledem na ochranu osobních údajů.

Kromě méně častých případů, kdy má být splněna právní povinnost – např. s ohledem na aktivity v kasinu, nebo kdy je zpracování nezbytné k ochraně důležitých zájmů např. u dálkového monitorování pacientů na resuscitačních jednotkách, je správce údajů často povinen provést určitý úkol ve veřejném zájmu nebo při výkonu úřední moci, případně na základě konkrétních předpisů, např. odhalovat dopravní přestupky nebo násilné jednání v hromadných dopravních prostředcích v oblastech s vysokou mírou zločinnosti – např. dle článku 7 písm. e) směrnice; správce údajů může také sledovat legitimní zájem, před kterým nejsou upřednostněny zájmy subjektů údajů nebo základní práva a svobody /viz článek 7 písm. f)/.

V obou případech, zejména ve druhém uvedeném případě, vyžaduje citlivost zpracování pečlivé posouzení rozsahu úkolů, pravomocí a legitimních zájmů s ohledem na správce údajů. V rámci této analýzy je nutno zcela

---

15) *Banka a místní policejní stanice nedávno odmítly žádost zákazníka na vynětí ze záznamu pořízeného kamerou, jež sledovala bankomat; tento záznam se týkal zloděje, který po krádeži bankovní karty zákazníka tuto kartu neoprávněně použil k výběru peněz z bankomatu, a to z důvodů souvisejících údajně s ochranou „soukromí“.*

16) *Na základě tohoto práva se ve Francii a Belgii vyžaduje „předchozí souhlas“.*

vyloučit povrchnost a bezdůvodné rozšiřování těchto úkolů.

Zejména pokud jde o vyvažování rozdílných zájmů, bude nutno věnovat zvláštní pozornost, a to i formou předběžného jednání s dotčenými stranami, možnosti, kdy nějaký zájem zasluhující ochranu bude v konfliktu buď s instalací systému nebo s určitými opatřeními k uchovávání údajů či s jinými zpracovatelskými operacemi.[17)]

Konečně, pokud jde o získání souhlasu subjektu údajů, tento souhlas musí být jednoznačný a musí se opírat o jasné informace. Souhlas musí být poskytnut zvlášť a konkrétně ve vztahu ke sledování prostor, ve kterých probíhá soukromý život dané osoby.[18)]

Zákonnost zpracování je třeba posuzovat také s přihlédnutím k ustanovením směrnice, která stanoví zvláštní ochranná opatření s ohledem na údaje, které se týkají protiprávních činů (viz článek 8 odst. 5 směrnice).[19)]

Další opatření mohou vycházet z předběžného posouzení zpracování údajů na základě mechanizmu předběžné kontroly, pokud s sebou kamerové sledování nese zvláštní rizika pro práva a svobody jednotlivců (viz článek 20 směrnice 95/46/ES).

Zpracování údajů prostřednictvím kamerového sledování by vždy mělo mít oporu ve výslovných právních ustanoveních, je-li prováděno veřejnými orgány.

D) Přiměřenost využití kamerového sledování

Zásada, že údaje musejí být odpovídající a přiměřené sledovaným účelům, znamená především, že uzavřené televizní okruhy a podobná zařízení pro kamerové sledování mohou být použity pouze podpůrně, tzn.:

pro účely, které skutečně odůvodňují použití těchto systémů.

Ze zásady přiměřenosti vyplývá, že tyto systémy lze použít v případě, že se jiná opatření směřující k prevenci, ochraně a/nebo zabezpečení fyzické a/nebo logické povahy, která nevyžadují pořizování obrazových záznamů, např. použití pancéřových dveří proti vandalismu, instalace automatických bran a kontrolních zařízení, společné poplachové systémy, lepší a silnější osvětlení ulic během noci a podobně, ukáží být nedostatečnými a/nebo nepoužitelnými s ohledem na výše uvedené legitimní účely.

Stejná zásada platí také pro výběr vhodné technologie, kritéria pro konkrétní využití daného zařízení a specifikaci opatření ke zpracování údajů, mj. i s ohledem na zásady přístupu k údajům a dobu jejich uchování.

Je třeba zamezit např. tomu, aby správní orgán nainstaloval kamerové zařízení v souvislosti s menšími přestupky, např. k vynucování zákazu kouření ve školách a na jiných veřejných místech nebo zákazu vyhazování nedopalků cigaret a odpadků na veřejných místech.

Jinými slovy, je třeba v jednotlivých případech uplatňovat *zásadu přiměřenosti* s ohledem na sledované účely, která zahrnuje určitou *povinnost minimalizace údajů* na straně správce údajů.

Přiměřené kamerové sledování a poplašné systémy lze sice považovat za zákonné v případě, že dojde k několika násilným aktům v blízkosti stadionu nebo pokud dojde opakovaně k napadení osob v autobusech v příměstských oblastech nebo v blízkosti autobusových zastávek. Není tomu již tak v případě systému zaměřeného na prevenci inzultace řidičů autobusů a znečišťování vozidel, jak bylo uvedeno úřadem pro ochranu osobních údajů, a v případě identifikace občanů, kteří se dopustí menších přestupků, jako je vyhazování pytlů s odpadky mimo kontejnery a/nebo na místech, kde je vyhazování odpadků zakázáno, či u odhalování osob odpovědných za příležitostné krádeže v prostorách bazénů.

Přiměřenost je třeba posuzovat na základě ještě přísnějších kritérií, pokud jde o veřejně nepřístupné prostory.

V tomto směru by mohla napomoci výměna informací a zkušeností mezi příslušnými orgány jednotlivých členských států.[20)]

Výše uvedené úvahy souvisejí zejména s čím dál běžnějším používáním kamerových systémů k sebeobraně a ochraně majetku – takřka u všech veřejných budov a kanceláří včetně jejich okolí. Tento druh sledování vyžaduje mnohem obecnější hodnocení nepřímých důsledků masivního využívání kamerových systémů – např. zda je instalace několika zařízení skutečně účinným odrazujícím prostředkem nebo zda se pachatelé trestných činů a/nebo vandalové jen přesunou do jiných oblastí a uchýlí k jiným aktivitám.

E) Přiměřenost při provádění kamerového sledování

Zásada, podle níž musejí být údaje přiměřené, relevantní a míru nepřesahující vyžaduje pečlivé posouzení přiměřenosti systému zpracování údajů poté, co je ověřena zákonnost tohoto zpracování.

V první řadě je třeba vzít úvahu systém filmování, s ohledem především na tyto aspekty:

a) úhel záběru ve vztahu ke sledovaným účelům[21)] – např. pokud je sledování prováděno na veřejném

---

[17)] *Podle článku 6b nového německého spolkového zákona o ochraně osobních údajů, který nabyl účinnosti dne 23. května 2001, je sledování veřejně přístupných míst pomocí optických a elektronických zařízení povoleno, pokud mj. neexistují žádné důvody se domnívat, že je třeba dát přednost zájmům subjektu údajů, které zasluhují ochranu.*

[18)] *Zvláštní pozornost je třeba věnovat reálné možnosti vyjádřit platný souhlas ve smyslu článku 2 písm. h) směrnice 95/46/ES („jakýkoli svobodný, zřejmý a vědomý projev vůle, kterým subjekt údajů dává najevo své svolení se zpracováním osobních údajů, které se ho týkají“) v případě instalace kamerového systému ve společných prostorách (bytové domy apod.).*

[19)] *Zde je možno zmínit ustanovení článku 8 portugalského zákona č. 67/98 s ohledem na údaje, které se týkají osob podezřelých z účasti na protiprávní a/nebo trestné činnosti.*

[20)] *Tím by se umožnila lepší harmonizace regulačních koncepcí a správních rozhodnutí, které se v některých případech liší např. u heren Bingo.*

[21)] *Příkladem konkrétních opatření, která je třeba přijmout s ohledem na úhel záběru, mohou být dvě ustanovení vydaná italským úřadem pro ochranu osobních údajů. Zdravotnické zařízení, které plánovalo zavedení služby, jež by umožňovala příbuzným nepřetržitě sledovat ze vzdáleného místa pacienty v komatu, v karanténě a/nebo s vážnou nemocí na jednotce intenzivní péče, bylo upozorněno na nutnost přijetí vhodných opatření, která by zabránila současnému sledování jiných pacientů. V jiném případě úřad upozornil policejní orgány, že v rámci systému odhalování případů překročení nejvyšší povolené rychlosti lze pořizovat závěry pouze státních poznávacích značek a nikoli vnitřních prostor vozidla.*

místě, neměl by tento úhel umožňovat pozorování detailů a/nebo tělesných rysů, které nejsou relevantní z hlediska daného účelu, ani nedaleké soukromé prostory, zejména v případě využití funkcí přiblížení,

b) druh zařízení používaného k pořizování záběrů, tzn. pevné nebo mobilní systémy,
c) vlastní instalace systému, tzn. umístění kamer, používání pevných a/nebo pohyblivých kamer apod.,
d) možnost zvětšení a/nebo přiblížení obrazů buď v okamžiku jejich pořízení nebo později, tzn. u uchovaných záznamů, a možnost rozmazání a vymazání jednotlivých obrazů,
e) funkce zmrazení záběru,
f) spojení s „centrem" využívané k zasílání zvukových a/nebo obrazových poplašných signálů,
g) kroky učiněné v důsledku kamerového sledování, tzn. uzavření vchodů, přivolání dozorčí služby apod.

Za druhé, je třeba zvážit rozhodnutí, která mají být přijata v souvislosti s uchováváním obrazových informací a stanovením doby jejich uchování – tato lhůta musí být poměrně krátká v souladu s konkrétními aspekty dotyčného případu.

Zatímco v některých případech může postačovat systém, který umožňuje pouze vizualizaci záběrů na uzavřeném okruhu, které nejsou zaznamenávány např. u pultů v supermarketech, v jiných případech, např. k ochraně soukromých prostor, lze odůvodnit pořizování záznamů a jejich uchování po dobu několika hodin, s následným vymazáním, a to nejpozději na konci dne a případně na konci týdne. Výjimkou z tohoto pravidla je zjevně případ, kdy došlo ke spuštění poplachu nebo kdy byla podána žádost, která vyžaduje zvláštní pozornost; v takových případech existuje rozumný důvod vyčkat krátkou dobu na případné rozhodnutí policejních nebo soudních orgánů.

Jiným příkladem může být systém zaměřený na odhalování neoprávněného vjezdu vozidel do center měst a oblastí s omezenou dopravou, který by měl pořizovat záznam pouze v případě přestupku.

Otázku přiměřenosti je třeba řádně posoudit, kdykoli se považuje za nezbytné uchovat záznam po delší dobu, jež by však neměla přesahovat jeden týden[22], např. s ohledem na záběry pocházející z kamerového sledování, které lze použít k identifikaci osob, které se pohybovaly v prostorách banky před provedením loupeže.

Za třetí, pozornost bude třeba věnovat také případům, *kdy je identifikace osob usnadněna* spojením záběru obličeje osoby s jinými informacemi, které se týkají zobrazeného jednání a/nebo činností např. v případě spojení záběrů a činností prováděných klienty v bance ve snadno zjistitelnou dobu.

V této souvislosti bude třeba přihlížet k jasnému rozdílu mezi dočasným uchováním záběrů z kamerového sledování pořízených pomocí zařízení umístěného u vchodu do banky a zjevně mnohem invazivnějším zřizováním databank včetně fotografií a otisků prstů poskytnutých klienty banky s jejich souhlasem.

Konečně bude třeba vzít v úvahu rozhodnutí, jež mají být přijata s ohledem na *případné sdělení údajů třetím osobám,* jimiž by v zásadě neměly být osoby, které nemají vztah ke kamerovému sledování, a jejich úplné nebo částečné zpřístupnění do zahraničí či dokonce on-line, také s ohledem na ustanovení týkající se odpovídající ochraně; viz článek 25 a následující články směrnice.

Požadavek, aby záběry byly relevantní a míru nepřesahující také zjevně platí pro kombinaci informací, které jsou v držení různých správců kamerových systémů.

Výše uvedené záruky mají i v praxi zajistit dodržování zásady označované ve vnitrostátním právu některých zemí jako zásada *zmírňování použití osobních údajů,* jejímž účelem je zamezit, nebo co možná nejvíce omezit, zpracování osobních údajů.

Tuto zásadu je třeba uplatňovat ve všech oblastech také s ohledem na skutečnost, že řady účelů lze ve skutečnosti dosáhnout bez použití osobních údajů nebo použitím skutečně anonymních údajů, i když se zpočátku zdá, že použití osobních informací bude nevyhnutelné.

Výše uvedené úvahy platí také v případě oprávněné potřeby zlepšit používání obchodních zdrojů[23] nebo zkvalitnění služeb poskytovaných uživatelům.[24]

F) Informování subjektů údajů

Otevřenost a přiměřenost použití zařízení pro kamerové sledování zahrnuje poskytování odpovídajících informací subjektům údajů podle ustanovení článků 10 a 11 směrnice.

Subjekty údajů by měly být informovány v souladu s ustanoveními článků 10 a 11 směrnice. Měly by si být vědomy skutečnosti, že je kamerový systém v provozu, i pokud jde o veřejné akce a pořady či o reklamní činnosti (webové kamery); měly by být také podrobně informovány o sledovaných místech.

Není nezbytné určit přesné umístění sledovacího zařízení, je však třeba jednoznačně vysvětlit podmínky sledování.

Informace je třeba umístit v rozumné vzdálenosti od sledovaných míst – nikoli jako v některých případech, kdy bylo umístění informačních desek ve vzdálenosti 500m od sledovaných prostor shledáno přijatelným – a také s ohledem na systém sledování.

Informace by měly být viditelné a měly by být poskytnuty souhrnným způsobem, bude-li takový systém efektivní; lze použít i symboly, které již prokázaly svou užitečnost ve spojení s kamerovým dohledem a informa-

---

[22] *Dánský a švédský DPA vyjádřily stanovisko, že videozáznam lze uchovávat pouze po krátkou dobu nepřesahující 30 dnů.*

[23] *Tak tomu může být například v případě nutnosti stanovení počtu pultů, které je třeba současně obsluhovat v supermarketu v závislosti na počtu přicházejících zákazníků, nebo v případě požadavku na vybudování optimálních nákupních tras pro zákazníky supermarketů.*

[24] *K usnadnění přístupu na pracoviště a/nebo u konkrétních dopravních prostředků, kde se vyžaduje kontrola totožnosti, mohou postačovat průkazy s fotografií, případně i na počítačovém médiu, bez použití systému rozpoznávání obličeje.*

cemi o zákazu kouření. Tyto symboly se mohou lišit v závislosti na tom, zda jsou záběry nahrávány či nikoli. Ve všech případech je třeba uvést účely sledování a označit příslušného správce systému. Velikost informačního sdělení je třeba přizpůsobit podmínkám jeho umístění. [25)]

Konkrétní, dobře odůvodněná omezení požadavků na informování lze připustit pouze v případech uvedených v článcích 10, 11 a 13 směrnice (např. dočasné omezení lze použít s ohledem na údaje shromážděné v průběhu vyšetřování, které zákonně provádí obhájce, nebo s ohledem na uplatnění práva na obhajobu, pokud by poskytnutí informací mohlo ohrozit splnění sledovaného účelu).

Zvláštní pozornost je třeba věnovat také vhodnému způsobu poskytování informací nevidomým osobám.

G) Další požadavky

V souvislosti s těmito dalšími požadavky, preventivními a ochrannými opatřeními uvedenými v legislativě na ochranu osobních údajů a shrnutými v bodu 3), i s ohledem na nutnost oznámení zpracování osobních údajů nezávislému orgánu a nutnost dozoru tohoto orgánu nad daným zpracováním v souladu s články 18, 19 a 28 směrnice, by Pracovní skupina chtěla upozornit zejména na následující aspekty:

a) Možnost shlédnout případný záznam záběrů a přístup k tomuto záznamu by měl získat jen omezený počet fyzických osob, které musejí být navíc konkrétně určeny, a to výhradně za účelem, který prostředky kamerového sledování mají, nebo z důvodu údržby daného zařízení k ověření jeho správné funkce; alternativně se tak může stát na základě žádosti subjektu údajů o přístup k těmto údajům či na základě platného příkazu vydaného policejním či soudním orgánem za účelem odhalování trestné činnosti.

   Pokud je kamerové sledování zaměřeno pouze na prevenci, odhalování a kontrolu trestné činnosti může být v řadě případů vhodným řešením použití dvou přístupových klíčů, z nichž jeden má k dispozici správce a druhý policie; tento systém zajistí, aby možnost shlédnout pořízené záběry měli jen policisté a nikoli neoprávněné osoby, aniž by tím byla dotčena možnost legitimního uplatnění práva subjektu údajů na přístup k údajům na základě žádosti učiněné v průběhu krátkého období uchovávání záznamu.

b) K prevenci událostí uvedených v článku 17 směrnice je třeba přijmout vhodná bezpečnostní opatření, včetně zveřejnění informací, jež mohou napomoci ochraně práv subjektu údajů, třetích osob nebo samotného správce údajů a také s ohledem na prevenci manipulace, změny či zničení údajů a souvisejících důkazů.

c) Zásadní význam má také kvalita pořízených záběrů, zejména pokud je opakovaně používáno totéž záznamové médium, což s sebou nese riziko neúplného smazání dřívějšího záznamu.

d) Konečně, je nezbytně nutné, aby provozovatelé, kteří se přímo podílejí na kamerovém sledování, prošli odpovídajícím školením a byli poučeni o opatřeních, jež je třeba přijmout k úplnému splnění relevantní požadavků. Za vhodné opatření lze také považovat školení správců a provozovatelů v souvislosti s relevantními riziky a mechanizmy správného určení zobrazovaných osob.

H) Práva subjektů údajů

Zvláštní rysy shromážděných osobních údajů nevylučují uplatnění práv subjektů údajů uvedených v článcích 13 a 14 směrnice, zejména s ohledem na právo podat námitku proti zpracování. Směrnice 95/46/ES totiž umožňuje subjektu údajů kdykoli vznést námitku proti zpracování údajů, které se jej týkají,[26)] na základě přesvědčivých legitimních důvodů souvisejících s jeho situací.

Právo subjektu údajů na opominutí, a obvykle krátká doba uchovávání záznamů, omezují rozsah aplikace práva subjektu údajů na přístup k osobním údajům, které umožňují jeho identifikaci; toto právo musí být zaručeno zejména v případě podání podrobné žádosti, aby bylo možno příslušné záběry snadno nalézt. Přihlédnout je třeba také k nutnosti dočasného zaručení práv třetích osob.

Jakákoli omezení vyplývající z nesnadnosti získání příslušných záběrů, pokud námaha s tím spojená zjevně neodpovídá danému účelu s ohledem na vynaložené prostředky a zdroje z důvodu krátké doby uchovávání záběrů, je třeba výslovně stanovit v primární legislativě (viz článek 13 odst. 1 směrnice) s náležitým ohledem na právo subjektu údajů bránit se v případě některých událostí, jež nastanou v průběhu dotyčného období.

I) Další záruky související s konkrétními zpracovatelskými operacemi

Je třeba zakázat provádění kamerového dohledu výlučně z důvodu rasového původu zobrazovaných osob, jejich náboženského nebo politického přesvědčení, jejich členství v odborech či sexuálního života (článek 8 směrnice).

Aniž by uvedla vyčerpávající výčet všech rozmanitých aplikací kamerového sledování, chce Pracovní skupina zdůraznit nutnost větší pozornosti, zásadně v rámci případné předchozí kontroly zpracovatelských operací uvedených v článku 20 směrnice, některým případům pořizování záběrů identifikovaných nebo identifikovatelných osob, neboť takové případy je třeba posuzovat samostatně.

Jde o následující případy vycházející ze zkušeností a/nebo již probíhajících testů:

a) trvalé propojení kamerových systémů provozovaných různými správci údajů,

b) možné spojení záběrů a biometrických údajů, jako např. otisků prstů (např. při vstupu do bank),

---

[25)] *Tuto koncepci lze označit jako „vícevrstevný“ systém.*

[26)] *Nestanoví-li vnitrostátní právní předpisy jinak.*

c) používání hlasových identifikačních systémů,
d) provozování systémů indexace pořízených záběrů a/nebo systémů jejich simultánního automatického vyhledávání, zejména pomocí identifikačních údajů, v souladu se zásadou přiměřenosti a na základě konkrétních ustanovení,
e) používání systémů rozpoznávání obličeje, které se neomezují na identifikaci maskování procházejících osob, jako např. falešné vousy a kníry, avšak vycházejí z vyhledávání podezřelých osob, např. na základě schopnosti systému automaticky identifikovat určité osoby na základě vzorů a/nebo standardních identifikačních souborů, které vyplývají z některých vnějších rysů (např. barva kůže, očí, vystouplé lícní kosti apod.) nebo na základě předem definovaného abnormálního chování (náhlé pohyby, opakované přecházení i v určitých intervalech, způsob parkování vozidla apod.). V této souvislosti je vhodný lidský zásah, ostatně i s ohledem na možnost omylu v těchto případech, jak je uvedeno v bodu f),
f) možnost automatického sledování tras a stop a/nebo rekonstrukce či předpovědi chování určité osoby,
g) přijímání automatických rozhodnutí na základě profilu určité osoby nebo na základě inteligentní analýzy a intervenčních systémů, které nesouvisejí s běžnými poplašnými signály jako je vstup do určitého místa bez požadované identifikace nebo požární poplach.

8. KAMEROVÉ SLEDOVÁNÍ V RÁMCI PRACOVNÍHO POMĚRU

Ve svém Stanovisku č. 8/2001 ke zpracování osobních údajů v rámci pracovního poměru, které bylo přijato dne 13. září 2001, a ve svém *Pracovním dokumentu o sledování elektronické komunikace na pracovišti,* který byl přijat dne 29. května 2002[27)], tato Pracovní skupina již upozornila z obecnějšího hlediska na několik zásad zaměřených na ochranu práv, svobod a důstojnosti subjektů údajů v rámci pracovního poměru.

Kromě úvah popsaných ve výše uvedených dokumentech, pokud se skutečně týkají kamerového sledování, je na místě upozornit, že kamerové systémy zaměřené přímo na kontrolu kvality a objemu pracovní činnosti ze vzdáleného místa, jež tedy zahrnují i zpracování osobních údajů v tomto rámci, nejsou zpravidla přípustné.

Jinak je tomu v případě kamerových systémů, které slouží, na základě odpovídajících bezpečnostních opatření, ke splnění požadavků na výrobu a/nebo bezpečnost při práci a zahrnují mj., i když nepřímo, také vzdálené monitorování[28)].

Zkušenosti z praxe navíc ukazují, že sledovány by neměly být prostory, které jsou buď vyhrazeny pro soukromé účely zaměstnanců nebo nejsou určeny k plnění pracovních povinností jako např. toalety, sprchy, šatny a oblasti určené k odpočinku; že záběry pořízené výlučně na ochranu majetku a/nebo k odhalení, prevenci a kontrole závažné trestné činnosti by neměly být používány ke stíhání zaměstnanců pro méně významné disciplinární prohřešky; a že by zaměstnanci měli mít vždy možnost uplatňovat své argumenty na základě obsahu pořízených záběrů.

Informace musí být poskytovány zaměstnancům a všem osobám, které působí na pracovišti. Tyto informace by měly zahrnovat určení totožnosti správce a účel dohledu a jiné údaje nezbytné k zaručení spravedlivého zpracování s ohledem na subjekt údajů, například informace o tom, v jakých případech bude záběry zkoumat management společnosti, o době uchovávání záznamu a o případech, kdy budou záběry poskytnuty orgánům činným v trestním řízení. Poskytnutí informací s pomocí symbolů nelze v rámci pracovního poměru považovat za postačující.

9. ZÁVĚR

Pracovní skupina vypracovala tento pracovní dokument za účelem jednotné aplikace národních opatření přijímaných podle směrnice 95/46/ES v oblasti kamerového sledování.

V tomto rámci je také nezbytně nutné, aby členské státy vydaly pravidla zaměřená na činnosti výrobců, poskytovatelů služeb a distributorů, a také výzkumných pracovníků, s ohledem na rozvoj technologií, softwaru a technických přístrojů tak, aby odpovídaly zásadám uvedeným v tomto dokumentu.

V Bruselu, dne 11. února 2004

Za Pracovní skupinu
předseda
Stefano RODOTÀ

---

27) *Oba dokumenty jsou k dispozici na následující internetové adrese: www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index/htm.*

28) *V těchto případech je třeba kromě aspektů popsaných v tomto dokumentu přihlédnout také k nutnosti respektovat práva uvedená v kolektivních smlouvách, která někdy vycházejí z kolektivního informování zaměstnanců a/nebo jejich odborových organizací tzn. kromě informací, které mají být poskytnuty jednotlivě na základě zákonů na ochranu osobních údajů; v jiných případech je třeba získat předběžný souhlas buď zástupců zaměstnanců nebo odborových organizací s instalací dotyčných systémů, i s ohledem na dobu trvání sledování a na jiné požadavky na pořizování záběrů. V některých zemích může být nutný zásah státu v případech, kdy příslušné strany nedosáhnou dohody.*

---

*) Poznámka: V češtině je text Stanoviska č. 8/2001 zpracován v Doporučení Rady Evropy č. R (89)2, které je k dispozici ve Věstníku Úřadu v částce 26 z roku 2003, nebo na internetové adrese Úřadu www.uoou.cz/zahr_RE_dok.php3 .

Překlad pořízený Evropskou komisí

Článek 29 Pracovní skupina pro ochranu údajů

11733/04/CS
WP 97

Stanovisko č. 8/2004 o informovanosti cestujících o přenosu údajů obsažených v záznamech o knihování cestujících na letech mezi Evropskou unií a Spojenými státy

Přijato dne 30. září 2004

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

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

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

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

přijala toto stanovisko

Komise rozhodla ve svém rozhodnutí ze dne 14. května 2004[2)], že Úřad pro cla a ochranu hranic (CPB) Spojených států zajišťuje odpovídající úroveň ochrany údajů obsažených v záznamech o knihování cestujících v souvislosti s lety do nebo z USA předávaných ze Společenství.

Toto rozhodnutí se týká přiměřenosti ochrany poskytované úřadem CBP vzhledem ke splnění požadavků čl. 25 odst. 1 směrnice 95/46/ES. Nemá vliv na další podmínky a omezení provádějící ostatní ustanovení uvedené směrnice, které se vztahují na zpracování osobních údajů v členských státech. Jednou z těchto podmínek je povinnost správců údajů informovat subjekty údajů o hlavních prvcích zpracování údajů. Proto jsou správci údajů, kteří provádějí zpracování údajů obsažených v záznamech o knihování cestujících a podléhají vnitrostátním právním předpisům členských států EU přijatým podle směrnice 95/46/ES, povinni poskytnout cestujícím úplné a přesné informace o předání údajů PNR (Passenger Name Record) úřadu CBP, v souladu s jejich vnitrostátními právními předpisy přijatými podle článků 10 a 11 směrnice.

Pracovní skupina přijala připomínky přiložené jako přílohy 1 a 2 tohoto stanoviska. Tyto připomínky by měly sloužit jako návod, pokud jde o informace, které by měly být poskytovány cestujícím zaoceánských letů a měly by být v co nejširší míře použity leteckými přepravci, cestovními kancelářemi a počítačovými rezervačními systémy účastnícími se při registračním procesu.

V Bruselu dne 30. září 2004

Za pracovní skupinu
Předseda
Peter Schaar

---

1) *Úř. věst. L 281, 23.11.1995, s. 31, dostupný na: http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm.*

2) *Rozhodnutí Komise ze dne 14. května 2004 o odpovídající úrovni ochrany osobních údajů obsažených v záznamech o knihování cestujících v letecké dopravě, které se předávají Úřadu USA pro cla a ochranu hranic (K(2004) 1914) Úř. věst. L 235, 6.7.2004, s. 11.*

PŘÍLOHA I

Stručné oznámení týkající se cest mezi Evropskou unii a Spojenými státy

Podle zákonů Spojených států obdrží Úřad pro cla a ochranu hranic (CPB) Spojených států některé informace o cestě a rezervaci, které jsou známy jako záznamy o knihování cestujících (PNR Passenger Name Record) a které se týkají cestujících létajících mezi Evropskou unií a Spojenými státy.

Úřad CBP se zavázal, že použije údaje PNR pro účely prevence a boje proti terorismu a dalším závažným nadnárodním trestným činům. PNR mohou obsahovat informace poskytnuté během knihování či držené leteckými společnostmi nebo cestovními kancelářemi.

Informace budou uchovány nejméně tři roky a šest měsíců a mohou být poskytovány ostatním orgánům.

Další informace týkající se těchto opatření, včetně opatření na ochranu osobních údajů lze získat od letecké společnosti nebo cestovní kanceláře. *[letecká společnost nebo cestovní kancelář může tedy poskytnout informace obsažené v úplném znění nebo Vás přímo odkáže na internetovou stránku úřadu CBP]*

PŘÍLOHA 2

Často kladené otázky související s přijímáním záznamů o knihování cestujících na letech mezi Evropskou unií a Spojenými státy Úřadem pro cla a ochranu hranic

Zákony Spojených států vyžadují od leteckých společností provozujících lety z nebo do Spojených států, aby poskytovaly Úřadu pro cla a ochranu hranic (CBP), který je součástí Ministerstva pro vnitřní bezpečnost USA, určité údaje o cestujících pro usnadnění bezpečného cestování a pro zajištění bezpečnosti USA.

Letecká společnost XXX se musí těmito požadavky řídit.

Evropská komise rozhodla, že úřad CBP poskytuje odpovídající úroveň ochrany, což umožňuje předávání údajů PNR do USA. Více informací naleznete na internetové stránce http://www.europa.eu.int/comm/internal_market/privacy/adequacy_en.htm.

Obsáhlé vysvětlení způsobu, jakým úřad nakládá s údaji PNR shromážděnými při letech mezi Evropskou unií (EU) a USA, naleznete v Závazném prohlášení Úřadu pro cla a ochranu hranic Ministerstva pro vnitřní bezpečnost („Závazné prohlášení PNR“) http://www.dhs.gov/interweb/assetlibrary/CBP-DHS_PNRUndertakings5-25-04.pdf.

1. Proč je můj PNR záznam předáván úřadu CBP před cestou do Spojených států, z nich, či přes ně?

Hlavním důvodem pro shromažďování údajů PNR před uskutečněním letů je umožnit bezpečné cestování mezi Evropskou unií a Spojenými státy a zajistit bezpečnost USA. Úřad CBP používá údaje PNR z letů mezi Evropskou unií a Spojenými státy pro účely prevence a boje proti:

a. terorismu a s ním související trestnou činností,
b. ostatní závažnou trestnou činností mající nadnárodní povahu zahrnující organizovanou trestnou činnost a
c. únikem před zatčením nebo vzetím do vazby na základě výše uvedených trestných činů.

Většina informací obsažených v údajích PNR může být získána úřadem CBP na vstupním letišti při kontrole letenky a dalších cestovních dokladů v rámci běžných hraničních kontrol. Možnost získat tyto údaje v elektronické formě před příletem či odletem cestujícího z/do USA výrazně zvyšuje schopnost úřadu CBP provádět předem účinné a efektivní vyhodnocení rizik cestujících.

2. Jaký je právní rámec pro předávání údajů PNR?

Podle zákona (title 49, United States Code, section 44909(c)(3)) a jeho (prozatímních) prováděcích předpisů (title 19, Code of Federal Regulations, section 122.49b) musí každý letecký dopravce, který provozuje mezinárodní leteckou přepravu cestujících do Spojených států nebo ze Spojených států, umožnit CBP elektronický přístup k údajům PNR v rozsahu, v němž jsou shromažďovány a obsaženy v rezervačních či odbavovacích kontrolních systémech leteckých dopravců.

Evropská komise rozhodla, že úřad CBP poskytuje odpovídající úroveň ochrany předávaných údajů. Předávání údajů je zahrnuto v mezinárodní dohodě mezi Evropským společenstvím a Spojenými státy.

Rozhodnutí Komise bylo založeno na Závazných prohlášení úřadu CBP a jeho souhlasu se jimi řídit. Proti neplnění těchto závazků by bylo možné zasáhnout vhodnými prostředky a v případě přetrvávajícího neplnění dojde k pozastavení účinků uvedeného rozhodnutí.

Příslušné orgány členských států mohou využít svou stávající pravomoc pozastavit toky údajů do CBP s cílem ochránit fyzické osoby v souvislosti se zpracováním jejich osobních údajů v případech, kdy CBP porušuje platné normy ochrany, které jsou předepsány rozhodnutím Komise.

3. Jaké druhy informací o mně získá úřad CBP prostřednictvím PNR?

Úřad CBP obdrží některé údaje PNR související s cestujícími na letech do, z, nebo přes USA. Letecké společnosti vytvářejí údaje PNR v rezervačních systémech pro každou zarezervovanou cestovní trasu. Tyto údaje PNR mohou být také obsaženy v odbavovacích systémech leteckých dopravců.

Údaje PNR obsahují různé informace poskytnuté během rezervace či držené leteckými společnostmi nebo cestovními kancelářemi, jako je jméno cestujícího, kontaktní údaje, podrobnosti o trase cesty (datum cesty, místo nástupu a místo určení, číslo sedadla a počet zavazadel) a podrobnosti o rezervaci (cestovní kancelář a informace o platbě) či jiné informace (např. účast v programu častých letů).

4. Jsou citlivé údaje zahrnuty do předávaných údajů PNR ?

Jisté údaje PNR označené jako „citlivé" mohou být obsaženy v PNR během jejich předávání z rezervačních systémů nebo odbavovacích systémů leteckých dopravců v EU do úřadu CBP. Tyto „citlivé" údaje PNR by zahrnovaly některé informace prozrazující rasový či etnický původ cestujícího, jeho politické názory, náboženské vyznání, zdravotní stav či sexuální orientaci. Úřad CBP se zaručil, že nebude používat žádné „citlivé" informace PNR, které obdrží z rezervačních či odbavovacích kontrolních systémů leteckých dopravců v EU. Úřad CBP nainstaluje automatický filtrační program pro mazání „citlivých" údajů PNR.

5. Budou údaje PNR o mé osobě předávány dalším orgánům?

Údaje PNR získaná v souvislosti s lety mezi EU a USA mohou být případ od případu a při dodržování zvláštních záruk ochrany údajů sdíleny s dalšími domácími či zahraničními vládními orgány, jež jsou odpovědné za boj proti terorismu nebo za výkon veřejné moci, za účelem prevence a boje proti terorismu a ostatním závažným trestným činům včetně organizované trestné činnosti, jež mají nadnárodní povahu, a prevence a boje proti úniku před zatčením nebo vzetím do vazby na základě výše uvedených trestných činů.

Údaje PNR mohou být také předány ostatním příslušným vládním subjektům z důvodů ochrany životně důležitých zájmů cestujícího nebo jiných osob, zejména pokud jde o závažná zdravotní rizika nebo pokud to jinak vyžaduje zákon.

6. Jak dlouho budou mé údaje PNR úřad CBP uchovávat?

Údaje PNR z letů mezi EU a USA bude úřad CBP uchovávat po dobu tří let a šesti měsíců, pokud není nutno ručně do těchto údajů nahlédnout. V těchto případech bude úřad CBP uchovávat údaje po dobu dalších 8 let. Kromě toho budou informace související s konkrétním trestním záznamem uchovávána úřadem CBP, po dobu archivace tohoto záznamu.

7. Jak budou mé údaje PNR zabezpečeny?

Úřad CBP bude zacházet s údaji PNR z letů mezi EU a USA bezpečně a důvěrně. Pečlivá úschova, včetně vhodného zabezpečení údajů a kontroly přístupu, zaručí, že údaje PNR nebudou využity nepatřičně.

8. Kdo vykonává dohled nad dodržováním Závazných prohlášení ohledně údajů PNR?

Vedoucí Úřadu na ochranu soukromí Ministerstva pro vnitřní bezpečnost USA je ze zákona povinen zajistit, aby všechny složky ministerstva nakládaly s osobními informacemi způsobem, který je v souladu s příslušným právem. Je nezávislý na jakémkoli řídícím orgánu v rámci tohoto ministerstva a jeho zjištění jsou pro ministerstvo závazná. Bude vykonávat dohled nad programem tak, aby zajistil přísné dodržování ze strany CBP a ověřil, že jsou uplatňována náležitá bezpečnostní opatření.

9. Mohu požádat o kopii údajů PNR, které o mně shromáždil úřad pro clo a ochranu hranic (CBP) ?

Každý cestující může požádat o podrobnější informace o druhu údajů PNR sdílených úřadům CBP a může požádat o kopii údajů PNR o své osobě, které má úřad CBP v databázi.

Jak je povoleno v zákoně o svobodě informací (Freedom of Information Act) a v ostatních zákonech, nařízeních a politikách USA, úřad CBP přezkoumá žádosti o dokumenty zahrnující dokumenty PNR, jež má k dispozici bez ohledu na státní příslušnost či zemi pobytu žadatele. Úřad CBP může za určitých podmínek zamítnout či odložit zveřejnění všech či některých záznamů PNR (např. pokud by zveřejnění na základě všeobecného úsudku mohlo narušit případné trestní řízení nebo by mělo za následek prozrazení metod a postupů používaných při trestním stíhání)

V případech, kdy úřad CBP zamítne přístup k údajům PNR na základě výjimky podle zákona o svobodě informací, (Freedom of Information Act) lze proti tomuto rozhodnutí podat odvolání k vedoucímu Úřadu na ochranu soukromí Ministerstva pro vnitřní bezpečnost, který je odpovědný jak za ochranu soukromí, tak za postup politiky odhalování Ministerstva pro vnitřní bezpečnost. Konečné rozhodnutí může být napadeno v rámci soudního řízení podle právních předpisů Spojených států amerických.

10. Mohu požádat o to, aby byly v mých údajích PNR provedeny opravy?

Ano. Cestující mohou požádat o opravu údajů PNR obsažených v databázi úřadu CBP tak, že se obrátí na úřady uvedených níže v otázce č. 12. Úřad CBP provede změny, o kterých rozhodne, že jsou odůvodněné a řádně doložené.

11. Na koho se mám v USA obrátit ohledně tohoto programu?

Obecné dotazy související s údaji PNR a dotazy související s údaji PNR o mé osobě

Chcete-li učinit dotaz ohledně údajů PNR, ke kterým má přístup úřad CBP, nebo chcete-li získat přístup k Vašim údajům PNR uloženým v úřadu CBP, zašlete žádost poštou na adresu: Freedom of Information Act (FOIA) Request, U.S. Customs and Border Protection, 1300 Pennsylvania Avenue, N.W., Washington, D.C. 20229. Další informace o postupech pro podávání žádostí je možné nalézt v oddíle 19 Code of Federal Regulations, oddíl 103.5 (www.dhs.gov/foia).

Obavy, stížnosti a žádosti o opravy

Přejete-li si podat stížnost či žádost o opravu údajů PNR, zašlete žádost na adresu: Assistant Commissioner, CBP Office of Field Operations, U.S. Customs and Border Protection, 1300 Pennsylvania Avenue, N.W., Washington, D.C. 20229.

Rozhodnutí úřadu CBP může být přezkoumáno vedoucím Úřadu na ochranu soukromí Ministerstva pro vnitřní bezpečnost, Washington, DC 20528. Cestující mohou svůj dotaz, stížnost či žádost o opravu údajů PNR popřípadě jejich další přezkoumání doručit rovněž orgánů pro ochranu údajů v příslušném členském státě.

12. Na koho se mám obrátit, nejsou-li mé stížnosti vyřešeny?

V případě, že úřad CBP nemůže stížnost vyřešit, může být předána písemně vedoucímu Úřadu na ochranu soukromí Ministerstva pro vnitřní bezpečnost, Washington, DC 20528. Vedoucí Úřadu na ochranu soukromí přezkoumá situaci a pokusí se stížnost vyřešit.

Vedoucí Úřadu na ochranu soukromí se zavázal, že bude neprodleně vyřizovat stížnosti obdržené od orgánů na ochranu údajů členských států Evropské unie jménem občana EU v takovém rozsahu, v jakém občan pověřil orgán na ochranu osobních údajů jednat jeho jménem.

13. Kde získám další informace?

Další informace o předávání údajů PNR do USA získáte, obrátíte-li se na orgán pro dohled nad ochranou údajů ve Vaší zemi.

V [název členského státu EU] jsou kontaktní údaje tyto:

[Kontaktní údaje orgánu na ochranu osobních údajů v každém členském státě EU]

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, Bohumír Lukaj, 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 700 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, Nádražní 29, 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