VĚSTNÍK
ÚŘADU PRO OCHRANU OSOBNÍCH ÚDAJŮ
2012

Částka 63 | **19. listopadu 2012** | **Cena 79,- Kč**

OBSAH

ÚVOD

V šedesáté třetí částce Věstníku Úřadu pro ochranu osobních údajů je publikován přehled zrušených registrací v období od 16. 6. 2012 do 31. 10. 2012.

Rubrika Stanoviska Úřadu přináší stanovisko č. 14/2012 „Zveřejňování osobních údajů žadatelů o dotaci podle novely rozpočtových pravidel č. 171/2012 Sb.“ Stanovisko se zabývá novelou rozpočtových pravidel č. 171/2012 Sb. (účinná od 1. srpna 2012) z pohledu ochrany osobních údajů.

Rubrika Sdělení Úřadu přináší dokument Pracovní skupiny pro ochranu dat podle článku 29 směrnice 95/46/ES (WP29), kterým je „Stanovisko č. 02/2012 k rozpoznávání tváře u on-line a mobilních služeb“. V posledních letech došlo k rychlému nárůstu dostupnosti a přesnosti technologie rozpoznávání tváře, která navíc začala tvořit součást on-line a mobilních služeb pro účely identifikace, autentizace/verifikace nebo kategorizace jednotlivců. Jako příklady jejího užití v rámci on-line či mobilních služeb lze uvést sociální sítě nebo výrobu chytrých telefonů. Smyslem tohoto stanoviska je posoudit právní rámec ochrany osobních údajů ve vztahu k těmto novým způsobům zpracování osobních dat a a nabídnout vhodná doporučení, která by se mohla uplatnit ve vztahu k užívání této technologie v kontextu on-line a mobilních služeb.

V rubrice Materiály z Úředního věstníku Evropské unie je publikován dokument „Rozhodnutí Komise 2011/61/EU ze dne 31. ledna 2011 o odpovídající ochraně osobních údajů Státem Izrael v souvislosti s automatizovaným zpracováváním osobních údajů“ a dokument „Prováděcí rozhodnutí Komise 2012/484/EU ze dne 21. srpna 2012 o odpovídající ochraně osobních údajů Uruguayskou východní republikou v souvislosti s automatizovaným zpracováváním osobních údajů“. Jedná se o překlady pořízené Evropskou komisí (přetisky v původní podobě).

Přehled zrušených registrací

Číslo registrace	Subjekt	Datum zrušení
00001188/047	UNILEVER ČR, SPOL. S R.O.	13.7.2012
00001601/001	OLOMOUCKÝ KRAJ	31.8.2012
00001726/004	COCA-COLA HBC ČESKÁ REPUBLIKA, S.R.O.	19.10.2012
00001726/005	COCA-COLA HBC ČESKÁ REPUBLIKA, S.R.O.	19.10.2012
00001726/006	COCA-COLA HBC ČESKÁ REPUBLIKA, S.R.O.	19.10.2012
00001726/009	COCA-COLA HBC ČESKÁ REPUBLIKA, S.R.O.	19.10.2012
00003212/001	STUDIJNÍ A VĚDECKÁ KNIHOVNA PLZEŇSKÉHO KRAJE, PŘÍSPĚVKOVÁ ORGANIZACE	29.6.2012
00003212/002	STUDIJNÍ A VĚDECKÁ KNIHOVNA PLZEŇSKÉHO KRAJE, PŘÍSPĚVKOVÁ ORGANIZACE	29.6.2012
00004183/005	SCHLECKER A.S.	7.9.2012
00004715/003	MĚSTO OTROKOVICE	25.7.2012
00004715/004	MĚSTO OTROKOVICE	25.7.2012
00004715/005	MĚSTO OTROKOVICE	25.7.2012
00004715/007	MĚSTO OTROKOVICE	25.7.2012
00012443/001	SIEMENS KOLEJOVÁ VOZIDLA S. R. O.	26.10.2012
00012603/001	NOVÁK ING. ZDENĚK	16.6.2012
00019116/006	SPRÁVA ŽELEZNIČNÍ DOPRAVNÍ CESTY, STÁTNÍ ORGANIZACE	27.7.2012
00019116/014	SPRÁVA ŽELEZNIČNÍ DOPRAVNÍ CESTY, STÁTNÍ ORGANIZACE	27.7.2012
00019116/023	SPRÁVA ŽELEZNIČNÍ DOPRAVNÍ CESTY, STÁTNÍ ORGANIZACE	22.8.2012
00019116/026	SPRÁVA ŽELEZNIČNÍ DOPRAVNÍ CESTY, STÁTNÍ ORGANIZACE	27.7.2012
00019116/028	SPRÁVA ŽELEZNIČNÍ DOPRAVNÍ CESTY, STÁTNÍ ORGANIZACE	27.7.2012
00019116/029	SPRÁVA ŽELEZNIČNÍ DOPRAVNÍ CESTY, STÁTNÍ ORGANIZACE	27.7.2012
00019116/051	SPRÁVA ŽELEZNIČNÍ DOPRAVNÍ CESTY, STÁTNÍ ORGANIZACE	10.8.2012
00019116/070	SPRÁVA ŽELEZNIČNÍ DOPRAVNÍ CESTY, STÁTNÍ ORGANIZACE	27.7.2012
00019116/085	SPRÁVA ŽELEZNIČNÍ DOPRAVNÍ CESTY, STÁTNÍ ORGANIZACE	10.8.2012
00019116/086	SPRÁVA ŽELEZNIČNÍ DOPRAVNÍ CESTY, STÁTNÍ ORGANIZACE	10.8.2012
00019116/087	SPRÁVA ŽELEZNIČNÍ DOPRAVNÍ CESTY, STÁTNÍ ORGANIZACE	10.8.2012
00019116/088	SPRÁVA ŽELEZNIČNÍ DOPRAVNÍ CESTY, STÁTNÍ ORGANIZACE	10.8.2012
00024153/001	KAVKA KAREL	24.7.2012
00033481/006	FAMILY DROGERIE S.R.O.	25.7.2012
00036764/001	TRIGA COLOR, A.S.	31.8.2012
00042053/001	STAVEBNÍ BYTOVÉ DRUŽSTVO POZEMNÍ STAVBY LIBEREC	28.7.2012
00042053/002	STAVEBNÍ BYTOVÉ DRUŽSTVO POZEMNÍ STAVBY LIBEREC	28.7.2012

II. STANOVISKA ÚŘADU

Stanovisko č. 14/2012

listopad 2012

Zveřejňování osobních údajů žadatelů o dotaci podle novely rozpočtových pravidel č. 171/2012 Sb.

Úvod

Dne 1. srpna 2012 nabyla účinnosti novela rozpočtových pravidel č. 171/2012 Sb.,[1] která v čl. I bodu 7 zavádí širokou povinnost Ministerstva financí zveřejnit „veškeré dokumenty a údaje“ v žádosti o dotaci (tj. daru podle § 2055 nového občanského zákoníku s příkazem podle § 2064 nového občanského zákoníku) nebo návratné finanční výpomoci (tj. zápůjčky podle § 2390 nového občanského zákoníku, rovněž s příkazem), které mu poskytovatel dotace nebo návratné finanční výpomoci podle § 18a odst. 1 rozpočtových pravidel předá.

Tato nová byrokratická zátěž byla dále rozpracována ve sdělení Ministerstva financí č. 22/2012, upravujícím elektronickou podobu formátu, ve kterém poskytovatelé předávají podle § 18a odst. 1 zákona č. 218/2000 Sb. v platném znění Ministerstvu financí ke zveřejnění veškeré dokumenty a údaje rozhodné pro poskytování dotací a návratných finančních výpomocí s výjimkami uvedenými v § 18a odst. 2 zákona č. 218/2000 Sb. Toto sdělení bylo zveřejněno ve Finančním zpravodaji 5/2012, pp. 107–118.[2]

Platnou dikci § 18a rozpočtových pravidel považuje Úřad pro ochranu osobních údajů (dále jen „Úřad“) za krajně nevhodnou. Úřad opakovaně upozorňoval na způsob, jak by vládní protikorupční úsilí mělo zohlednit oprávnění týkající se soukromí a nastavit konkrétní pravidla pro zacházení s osobními údaji. V připomínkovém řízení k novele rozpočtových pravidel však nebyly připomínky Úřadu řádně projednány.

Toto stanovisko přitom nijak zásadně neomezuje právo veřejnosti na informace a možnost kontrolovat nakládání s veřejnými prostředky. Vede ke stejnému cíli, který český zákonodárce vytýčil, při plném respektování oprávnění na soukromí, jak je vnímáno v Evropské unii judikaturou Evropského soudního dvora (dále jen „ESD“).

Evropské právo

Úřad upozornil Ministerstvo financí v meziresortním připomínkovém řízení, že připravovaný zákon č. 171/2012 Sb. je v rozporu s evropským právem. Čl. 6 odst. 2 smlouvy o založení Evropské unie stanoví: „Unie ctí základní práva zaručená Evropskou úmluvou o ochraně lidských práv a základních svobod podepsanou v Římě dne 4. listopadu 1950 a ta, jež vyplývají z ústavních tradic společných členským státům, jako obecné zásady práva Společenství.“ V České republice byla tato úmluva (dále jen „EÚLP“) Rady Evropy vyhlášena pod č. 209/1992 Sb. Po Lisabonské smlouvě je základním normativním aktem Evropské unie na ochranu lidských práv Charta základních práv Evropské unie č. 2007/C 303/01 (dále jen „Charta“), která je součástí primárního práva Evropské unie. Vychází z EÚLP a rozšiřuje ji.

Ministerstvo financí reagovalo stanoviskem, že evropské právo dopadá pouze na poskytování evropských dotací. Tento právní názor však neobstojí. Česká republika jako člen Evropské unie je povinna transponovat směrnici Evropského parlamentu a Rady 95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Tato povinnost se nevyčerpává přijetím zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů. Ochranu osobních údajů je nutno promítnout rovněž do všech sektorových předpisů, včetně rozpočtových pravidel, jinak Česká republika bude porušovat evropské právo.

Integrální součástí evropského práva jsou nejen směrnice a nařízení, ale rovněž rozsudky ESD. Vzhledem k tomu, že v řízení o předběžné otázce ESD závazným způsobem interpretuje evropské právo, je závazný nejen výrok (vlastní odpověď na otázku), ale rovněž odůvodnění, které je jeho podkladem.

Mezi ochranou soukromí (čl. 7 Charty), konkrétně ochranou osobních údajů (čl. 8 Charty), a oprávněním na informace (čl. 11 a 42 Charty) může přirozeně vzniknout konflikt. Vzhledem k tomu, že oprávnění na informace je politická svoboda, podléhá testu veřejného zájmu. Jak judikoval rozsudek ESD *Rechnungshof v. Österreichischer Rundfunk* z 20. 5. 2003, sp. zn. C-465/00, C-38/01 a C-139/01, § 90,[3] oprávnění na informace je relativní: „Je třeba dospět k závěru, že zásah, který vyplývá z použití vnitrostátní právní úpravy, jež je předmětem věcí v původních řízeních, není odůvodněný s ohledem na čl. 8 odst. 2 EÚLP, jestliže je široké zveřejnění nejen výše ročních příjmů, pokud tyto přesahují určitý strop, osob zaměstnaných subjekty, jež podléhají dohledu *Rechnungshof*, ale i jmen poživatelů těchto příjmů,

[1] http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=24309

[2] http://www.mfcr.cz/cps/rde/xbcr/mfcr/Legislativa_Financni_zpravodaj_-2012-05.pdf

[3] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62000CJ0465:CS:NOT

zároveň nezbytné a vhodné pro cíl udržet platy v rozumných hranicích, což přísluší posoudit předkládajícím soudům," což český zákonodárce v rozpočtových pravidlech ne zcela respektuje. V rozsudku ESD *Schecke a Eifert v. Hessensko* z 9. 11. 2010, sp. zn. C-92/09 a C-93/09, § 85 věta druhá,[4] se konstatuje: „Cíli transparentnosti nelze přitom přiznat automatickou přednost před právem na ochranu osobních údajů […], i když jsou ve hře významné ekonomické zájmy."

U poskytování dotací je významným závěrem, který řeší konflikt ochrany osobních údajů a oprávnění na informace, *Schecke a Eifert v. Hessensko*, § 58: „Není zpochybňováno, že částky, které dotčení příjemci dostávají […] představují část, často značnou, jejich příjmů. Zveřejnění jmenovitých údajů o uvedených příjemcích a přesných částkách, které obdrželi, na internetové stránce tak vzhledem k tomu, že se tyto údaje stávají dostupnými třetím osobám, představuje zásah do jejich soukromého života ve smyslu čl. 7 Charty (vizte v tomto smyslu výše uvedený rozsudek *Österreichischer Rundfunk* a další, §§ 73 a 74)." Důležitý je rovněž § 81: „Nic totiž nenaznačuje, že Rada a Komise při přijímání čl. 44a nařízení č. 1290/2005 a nařízení č. 259/2008 uvažovaly o takových způsobech zveřejňování informací o dotčených příjemcích, které by odpovídaly cíli takového zveřejňování a přitom by představovaly menší zásah do práva těchto příjemců na respektování jejich soukromého života obecně a konkrétně na ochranu jejich osobních údajů, jako je omezení zveřejnění jmenovitých údajů o uvedených příjemcích podle doby, po kterou podpory dostávali, frekvence podpor nebo jejich typu a výše." Promítnutí *Schecke a Eifert v. Hessensko* do evropského práva řeší stanovisko evropského inspektora ochrany údajů z 9. 10. 2012 *Financing, management and monitoring of the common agricultural policy (transparency, post-Schecke)*.[5]

Rechnungshof v. Österreichischer Rundfunk tedy vyložil, jak posuzovat přiměřenost zveřejňování osobních údajů příjemců veřejných prostředků, a ve výroku 2 konstatoval, že čl. 6 odst. 1 písm. c), čl. 7 písm. c) a e) směrnice 95/46/ES mají přímý účinek, tj. že se jich jednotlivec může dovolávat před vnitrostátními soudy. *Schecke a Eifert v. Hessensko* aplikoval tento postup na konkrétní právní předpis. Rozsah zveřejňovaných osobních údajů shledal nepřiměřeným.

Interpretace českých právních norem

Vzhledem k výše uvedené evropské judikatuře je nutno výjimku stanovenou v § 18a odst. 2 písm. b) rozpočtových pravidel (který zní: „dokumenty a údaje, o kterých to stanoví přímo použitelný předpis Evropské unie") vykládat extenzivně, nejen jako konkrétní nařízení EU uvedené v poznámce pod čarou, ale rovněž jako kterýkoliv další právní akt EU, tedy také čl. 6 odst. 1 písm. c), čl. 7 písm. c) a e) směrnice 95/46/ES a rozsudky ESD jako relevantní prameny práva.

Ustanovení § 5 odst. 3 zákona o ochraně osobních údajů zní: „Provádí-li správce zpracování osobních údajů na základě zvláštního zákona, je povinen dbát práva na ochranu soukromého a osobního života subjektu údajů." Na základě principu proporcionality by drobné dotace nebo návratné finanční výpomoci konkrétním lidem neměly být zveřejňovány vůbec, protože ochrana soukromí převáží nad oprávněním na informace.

Z § 8b odst. 3 zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, který upravuje poskytování informací o příjemcích veřejných prostředků, lze dovodit, že u větších dotací nebo návratných finančních výpomocí fyzickým osobám se poskytnou tyto druhy osobních údajů: „jméno, příjmení, rok narození, obec, kde má příjemce trvalý pobyt, výše, účel a podmínky poskytnutých veřejných prostředků", neboť na základě principu proporcionality má tato obecná úprava přednost před zvláštní v § 18a rozpočtových pravidel.

S ohledem na dvě výše uvedená zákonná ustanovení se nezveřejňuje rodné číslo, neboť by to představovalo zbytečný zásah do soukromí příjemce dotace nebo návratné finanční výpomoci.[6] Obdobně by mělo být přistupováno k jiným identifikátorům jako je bydliště nebo místo trvalého pobytu, neboť paušální zveřejnění ani těchto osobních údajů není nezbytné pro dosažení deklarovaného cíle této právní úpravy.

Ze systematického výkladu § 18a odst. 2 rozpočtových pravidel dále vyplývá, že ve zveřejňovaných dokumentech by se neměly objevovat osobní údaje třetích osob. Je tedy nutné postupovat analogicky § 8a zákona o svobodném přístupu k informacím, který zní: „Informace týkající se osobnosti, projevů osobní povahy, soukromí fyzické osoby a osobní údaje povinný subjekt poskytne jen v souladu s právními předpisy, upravujícími jejich ochranu." Tyto údaje je třeba ze zveřejňovaných dokumentů buď zcela odstranit, nebo alespoň jinak znepřístupnit.

Závěr

Úřad je připraven poskytnout ochranu oprávněním jednotlivců, kteří by se proti § 18a odst. 2 rozpočtových pravidel dovolávali aplikace § 5 odst. 3 zákona o ochraně osobních údajů či přímého účinku čl. 6 odst. 1 písm. c), čl. 7 písm. c) a e) směrnice 95/46/ES a považovali rozsah zveřejněných osobních údajů za nepřiměřený pro rozpor s oprávněním na ochranu soukromí.

---

[4] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62009CJ0092:CS:NOT

[5] http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-10-09_CAP_EN.pdf

[6] Z čl. 8 odst. 7 směrnice 95/46/ES vyplývá, že rodné číslo je údaj blízký citlivému.

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

III. SDĚLENÍ ÚŘADU

PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29

00727/12/CS
WP 192

Stanovisko č. 02/2012 k rozpoznávání tváře u on-line a mobilních služeb

Přijaté dne 22. března 2012

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

Sekretariát zajišťuje ředitelství C (Základní práva a občanství Unie) Generálního ředitelství pro spravedlnost Evropské komise, 1049 Brusel, Belgie, kancelář č. MO-59 02/013.

Internetová stránka: http://ec.europa.eu/justice/data-protection/index_cs.htm

1. Úvod

V posledních letech došlo k rychlému nárůstu dostupnosti a přesnosti technologie rozpoznávání tváře. Tato technologie navíc začala tvořit součást on-line a mobilních služeb pro účely identifikace, autentizace/verifikace nebo kategorizace jednotlivců. Tato technologie, která byla kdysi předmětem sci-fi, je nyní dostupná jak pro veřejné, tak soukromé subjekty. Jako příklady jejího užití v rámci on-line či mobilních služeb lze uvést sociální sítě nebo výrobu chytrých telefonů.

Schopnost automaticky zachycovat údaje a rozpoznávat tvář z digitálního obrazu již byla dříve posuzována pracovní skupinou podle článku 29 v pracovním dokumentu o biometrii (WP80) a v nedávno zveřejněném stanovisku č. 03/2012 (WP193) o rozvoji biometrických technologií. Rozpoznávání tváře se posuzuje v rámci biometrie, neboť v mnoha případech tato technologie pracuje s dostatečnými detaily, které umožňují jednoznačnou identifikaci jednotlivce.

Stanovisko č. 03/2012 připomíná:

> *„[biometrie] umožňuje automatizované stopování, sledování nebo profilování osob, a proto má velký potenciální dopad na soukromí jednotlivců a jejich práva na ochranu údajů.“*

Tento výrok je obzvláště pravdivý v případě rozpoznávání tváře u on-line a mobilních služeb, kde může být zachycen obraz jednotlivce (s jeho vědomím nebo bez něj) a následně může dojít k jeho předání na vzdálený server pro další zpracování. Služby on-line, jež jsou často vlastněné a provozované soukromými subjekty, si již vytvořily rozsáhlou sbírku obrazů, které jim poskytli jejich subjekty sami (formou uploadu). V některých případech může dojít k pořízení takových obrazů nelegálním způsobem z jiných veřejných stránek. Takovým zdrojem může být například *caches* u internetových vyhledávačů (*search engine caches*). Malé mobilní přístroje s kamerami s vysokým rozlišením svým uživatelům umožňují zachycovat obrazy a díky neustálému připojení je v reálném čase umísťovat na on-line službu. V důsledku toho jsou uživatelé schopni sdílet tyto obrazy s jinými uživateli nebo provést identifikaci, autentizaci/verifikaci nebo kategorizaci za účelem získání přístupu k dodatečným informacím o známé či neznámé osobě, se kterou přijdou do styku.

Rozpoznávání tváře u on-line a mobilních služeb tedy vyžaduje zvláštní pozornost pracovní skupiny podle článku 29, neboť s použitím této technologie je spojeno mnoho obav, pokud jde o ochranu údajů.

Smyslem tohoto stanoviska je posoudit právní rámec a nabídnout vhodná doporučení, která by se mohla uplatnit ve vztahu k užívání technologie rozpoznávání tváře v kontextu on-line a mobilních služeb. Toto stanovisko je určeno evropským a vnitrostátním zákonodárným orgánům, správcům údajů a uživatelům uvedených technologií. Není záměrem tohoto stanoviska opakovat zásady, na něž se odkazuje ve stanovisku č. 03/2012. Spíše z nich vychází a aplikuje je pro situaci on-line a mobilních služeb.

2. Definice

Technologie rozpoznávání tváře není nová. Zároveň existuje mnoho jejích definicí a interpretací. Je tudíž užitečné jasně definovat technologii, kterou se toto stanovisko zabývá.

Digitální obraz: digitální obraz je dvourozměrné zobrazení v digitální podobě. Nedávné pokroky v technologii rozpoznávání tváře ovšem vyžadují, aby byly k statickým i pohyblivým obrazům (tj. fotografie a nahrané či live video) ještě přidány obrazy trojrozměrné.

Rozpoznávání tváře: rozpoznávání tváře je automatické zpracování digitálních obrazů, která zahrnují tváře jednotlivců, za účelem identifikace, autentizace/verifikace nebo kategorizace[1] těchto jednotlivců. Proces samotného rozpoznávání tváře sestává z několika vzájemně oddělených dílčích procesů:

a) pořízení obrazu: proces zachycení tváře jednotlivce a převedení do digitální podoby (digitální obraz). V rámci on-line a mobilních služeb může být obraz pořízen i pomocí jiného systému, např. pořízení fotografie digitálním fotoaparátem a její převedení do on-line služby;

b) detekce tváře: proces detekce přítomnosti tváře v rámci digitálního obrazu a označení dané oblasti;

c) normalizace: proces, jehož cílem je zahladit variace v oblastech, v nichž byly detekovány tváře, např. převedení na standardní velikost, rotace nebo vyrovnání rozmístění barev;

d) extrakce rysů: proces izolování a zobrazení opakovatelných a charakteristických rysů z digitálního obrazu jednotlivce. Extrakce rysů může být holistická[2], zaměřená na určité rysy[3] nebo kombinace obou metod[4]. Soubor klíčových rysů může být uchován pro pozdější srovnávání v rámci referenční šablony[5];

e) registrace: jestliže je to poprvé, co se jednotlivec setkal se systémem rozpoznávání tváře, obraz a/nebo referenční šablona mohou být uchovány jako záznam pro pozdější srovnávání;

f) srovnávání: proces měření podobností mezi souborem rysů (vzorkem) a souborem již registrovaným v systému. Hlavním smyslem srovnávání je identifikace a autentizace/verifikace. Třetím účelem srovnávání je kategorizace, která spočívá v procesu extrakce rysů z obrazu jednotlivce s cílem klasifikovat jej v rámci několika širších kategorií (např. věk, pohlaví, barva oblečení atd.). Není nutné, aby systém kategorizace zahrnoval i proces registrace.

3. Příklady rozpoznávání tváře u on-line a mobilních služeb

Rozpoznávání tváře může být do on-line a mobilních služeb zahrnuto různými způsoby a za různými účely. V souvislosti s tímto stanoviskem se pracovní skupina podle článku 29 soustředí na několik různých příkladů, jejichž smyslem je poskytnout doplňující kontext pro právní analýzu. Tyto příklady se týkají užití rozpoznávání tváře za účelem identifikace, autentizace/verifikace a kategorizace.

---

1 Identifikace, autentizace/verifikace nebo kategorizace jsou definovány ve stanovisku č. 03/2012.

2 Holistická extrakce rysů: matematická prezentace celého obrazu, jako například ta, jež vychází z analýzy hlavních komponent.

3 Extrakce zaměřující se na určité rysy: určení umístění zvláštních rysů tváře, jako jsou oči, nos a ústa.

4 Taktéž známá jako metoda hybridní extrakce rysů.

5 Šablona je ve stanovisku č. 03/2012 definována jako *„(h)lavní rysy extrahované z hrubé formy biometrických údajů (např. rozměry tváře v zobrazení), jež jsou uchované pro pozdější zpracování namísto uchování samotných hrubých dat.*“

3.1. Rozpoznávání tváře jako prostředek identifikace

Příklad 1: Služba sociální sítě (dále jen „SSS“)[6] umožňuje uživatelům přidat ke svému profilu digitální obraz. Uživatelé navíc mohou nahrávat obrazy, které tak mohou sdílet s jinými registrovanými nebo neregistrovanými uživateli. Registrovaní uživatelé mohou v jimi nahraných obrazech manuálně identifikovat jiné jednotlivce (kteří mohou nebo nemusí být registrovanými uživateli) a přiřadit jim jmenovku (*tag*). Tyto jmenovky je možné zobrazit prostřednictvím tvůrce jmenovek (*tag creator*) a sdílet je v širší skupině přátel nebo všech registrovaných či neregistrovaných uživatelů. SSS dokáže použít obrazy opatřené jmenovkou pro vytvoření referenční šablony u každého registrovaného uživatele a díky technologii rozpoznávání tváře pak automaticky navrhuje jmenovky u nově nahraných obrazů.

Takové obrazy jednotlivců, jež jsou veřejně dostupné pro uživatele, by mohly posléze být zpřístupněny a uloženy do vyrovnávací paměti internetového vyhledavače. Vyhledávač může chtít zvýšit efektivitu svého vyhledávání tím, že umožní uživatelům poskytnout obraz jednotlivce, na jehož základě poskytne podobné obrazy a také odkaz na stránku profilu daného jednotlivce v rámci SSS. Obraz použitý pro hledání přitom může být zachycen přímo kamerou chytrého telefonu.

3.2. Rozpoznávání tváře jako prostředek autentizace/verifikace

Příklad 2: Systém rozpoznávání tváře se používá k nahrazení uživatelského jména/hesla pro kontrolu přístupu k on-line nebo mobilním službám nebo přístrojům. Pro registraci se využívá kamera přístroje k pořízení obrazu schváleného uživatele přístroje a dále vytvořená referenční šablona, která může být uchována přímo v přístroji, nebo poskytována vzdálenou on-line službou. Pro získání přístupu ke službě nebo k přístroji se pořizuje nový obraz jednotlivce, který se pokouší vstoupit, a ten je porovnán s referenčním obrazem. Přístup je poskytnut, jestliže systém vyhodnotí schodu.

3.3. Rozpoznávání tváře jako prostředek kategorizace

Příklad 3: SSS popsaná v příkladu 1 může dát třetí straně, která provozuje on-line službu rozpoznávání tváře, koncesi k přístupu do knihovny obrazů. Služba umožňuje zákazníkům třetí strany zahrnout technologii rozpoznávání tváře do dalších produktů. Tato další produkty mají funkce, které umožňují předkládat obrazy jednotlivců za účelem detekce a kategorizace tváří podle stanovených nebo předem definovaných kritérií, např. pravděpodobný věk, pohlaví a momentální nálada.

Příklad 4: Herní konzole užívá pohybového ovladače (*gesture control system*), v rámci kterého se detekují pohyby uživatele za účelem ovládání hry. Kamera nebo kamery užívané u pohybových ovladačů sdílejí obrazy jednotlivců se systémem rozpoznávání tváře, který předvídá pravděpodobný věk, pohlaví a náladu hráčů hry. Údaje, včetně těch, co pochází z jiných multimodálních činitelů, poté mohou vést ke změně průběhu hry tak, že herní zkušenost uživatele je zintenzívněna, nebo mohou vést ke změně prostředí, které by odráželo předvídaný profil uživatele. Podobným způsobem by systém mohl uživatele třídit, aby jim mohl povolit/odmítnout přístup k obsahu závislému na věku nebo aby jim mohl uvnitř hry zobrazit cílenou reklamu.

---

[6] Služba sociální sítě je široce definována ve stanovisku č. 05/2009 o on-line sociálních sítích jako „*komunikační platforma v on-line prostředí, která jednotlivcům umožňuje připojit se k sítím podobně smýšlejících uživatelů nebo takové sítě vytvářet*“.

4. Právní rámec

Příslušným právním rámcem pro rozpoznávání tváře je směrnice o ochraně údajů (95/46/ES), o které se v této souvislosti diskutovalo ve stanovisku č. 03/2012. Tento oddíl má za cíl pouze shrnout právní rámec související s rozpoznáváním tváře u on-line a mobilních služeb, a to na základě příkladů uvedených v oddíle 3. Ve stanovisku č. 03/2012 se posuzují i další příklady rozpoznávání tváře.

4.1. Digitální obrazy coby osobní údaje

V momentě, kdy digitální obraz zahrnuje tvář jednotlivce, která je zřetelná a umožňuje jeho identifikaci, považuje se za osobní údaj. To bude záležet na několika parametrech, jako například kvalita obrazu nebo zvláštní úhel pohledu. Obrazy situací, na kterých jsou jednotlivci v dálce nebo tváře jsou rozmazané, vesměs pravděpodobně nebudou považovány za osobní údaje. Je ovšem nutné dodat, že digitální obrazy mohou obsahovat osobní údaje více než jednoho jednotlivce (např. pokud jde o příklad 4, v herním rámci může být vícero hráčů) a přítomnost jiných jednotlivců na fotografii může naznačovat existující vztah.

Stanovisko č. 04/2007 k pojmu osobní údaje znovu zdůrazňuje fakt, že v případě, že údaje odkazují na „*charakteristické znaky nebo chování jednotlivce nebo pokud použití těchto informací určuje nebo ovlivňuje způsob zacházení s touto osobou nebo způsob jejího hodnocení*“, pak se taktéž jedná o osobní údaje.

Referenční šablona vytvořená z obrazu jednotlivce je z definice taktéž osobním údajem, neboť obsahuje soubor charakteristických rysů tváře jednotlivce, který je poté vztažen ke konkrétnímu jednotlivci a uchován jako reference pro pozdější srovnávání v rámci identifikace a autentizace/verifikace.

Šablony nebo soubory charakteristických rysů využívané pouze pro systém kategorizace obecně neobsahují dostatečně informací k identifikaci jednotlivce. Měly by obsahovat pouze tolik informací, jež jsou nutné k provedení kategorizace (např. muž, nebo žena). V tomto případě by se nejednalo o osobní údaje za předpokladu, že šablona (nebo výsledek) nebude vztažena k záznamu, profilu nebo originálnímu obrazu jednotlivce (které stále budou považovány za osobní údaje).

Digitální obrazy jednotlivců a šablony, které souvisí s „*biologickými vlastnostmi, prvky chování, fyziologickými rysy, znaky živého organismu nebo opakovatelnými úkony, které jsou jedinečné pro daného jednotlivce a současně měřitelné*“[7], by navíc měly být považovány za biometrické údaje.

4.2. Digitální obrazy coby zvláštní kategorie osobních údajů

Digitální obrazy osob mohou být v některých specifických případech považovány za zvláštní kategorii osobních údajů[8]. Konkrétně v případech, kdy jsou digitální obrazy jednotlivců nebo šablony dále zpracovávány pro odvození zvláštních kategorií údajů, se takové digitální obrazy jednotlivců nebo šablony budou považovat za zvláštní kategorii osobních údajů. Pokud budou například použity za účelem zjištění etnického původu, náboženství nebo informací o zdravotním stavu.

---

[7] Definice biometrických údajů ze stanoviska č. 03/2012.

[8] Judikatura v některých zemích označuje digitální obrazy tváří za zvláštní kategorie údajů – LJN BK6331 nizozemský vrchní soud, 23. března 2010.

4.3. Zpracovávání osobních údajů v souvislosti se systémem rozpoznávání tváře

Jak již bylo popsáno, rozpoznávání tváře závisí na několika automatizovaných fázích zpracování. Rozpoznávání tváře tudíž představuje automatizovanou formu zpracovávání osobních údajů, včetně biometrických údajů.

Systémy rozpoznávání tváře mohou být v důsledku využívání biometrických údajů předmětem dodatečných kontrol (např. schvalování *ex ante*) nebo jiných právních předpisů (např. pracovněprávní předpisy) v jednotlivých členských státech. Užitím biometrie v souvislosti se zaměstnáním se podrobněji zabývá stanovisko č. 03/2012.

4.4. Správce údajů

Na základě zmíněných příkladů budou správci údajů většinou vlastníci internetových stránek a/nebo poskytovatelé on-line služeb či provozovatelé mobilních aplikací, kteří se zabývají rozpoznáváním tváře a určují účely a/nebo prostředky zpracování[9]. Toto konstatování odpovídá závěrům stanoviska č. 05/2009 o internetových sociálních sítích, podle kterého „poskytovatelé SSS jsou správci údajů podle směrnice o ochraně údajů“.

4.5. Oprávněný důvod

Směrnice 95/46/ES stanoví podmínky, které musejí být při zpracovávání osobních údajů splněny. To znamená, že zpracovávání musí být v prvé řadě v souladu se zásadami pro kvalitu údajů (článek 6). Pro účely zpracovávání rozpoznávání tváře musí být digitální obrazy jednotlivců a příslušné šablony v tomto případě „podstatné“ a „nepřesahující míru“. Zpracování se může kromě toho uskutečnit pouze v případě, kdy je splněno jedno z kritérií specifikovaných v článku 7.

Vzhledem k zvláštnímu riziku souvisejícímu s biometrickými údaji je v souladu se směrnicí nutný vědomý souhlas jednotlivce, který musí být získán ještě před začátkem zpracovávání digitálních obrazů pro účely rozpoznávání tváře. Může se však stát, že správce údajů bude muset dočasně provést určité kroky v procesu rozpoznávání tváře přesně za tím účelem, aby posoudil, zda uživatel dal souhlas, který je právním základem pro zpracování údajů, či jej nedal. Toto počáteční zpracování (tj. pořízení obrazu, detekce tváře, srovnání atd.) se může v takovém případě opírat o odlišný právní základ, který zejména souvisí s legitimním zájmem správce údajů na plnění pravidel pro ochranu údajů. Údaje zpracované během těchto fází by měly být použity pouze pro přísně omezený účel ověření souhlasu uživatele a měly by být tudíž poté ihned smazány.

V příkladu 1 správce údajů rozhodl, že všechny nové obrazy nahrané registrovanými uživateli SSS by měly projít detekcí tváře, procesem extrakce rysů a srovnáním. Shoda s těmito novými obrazy bude nalezena pouze u registrovaných uživatelů, jejichž referenční šablona je zaregistrována v identifikační databázi. Jmenovka u nich bude tudíž navrhována automaticky. Jestliže by měl být souhlas jednotlivce považován za jediný možný právní základ pro každé zpracování, celá služba by byla zablokována, neboť zde například neexistuje možnost získat souhlas od neregistrovaných uživatelů, jejichž osobní údaje byly zpracovány během fáze detekce tváře a extrakce rysů. Bez toho, aby bylo nejprve provedeno rozpoznání tváře, by nebylo navíc možné rozlišit mezi tvářemi registrovaných uživatelů, kteří dali svůj souhlas, a těmi, kteří jej nedali. Teprve až po úspěšné (nebo neúspěšné) identifikaci by správce údajů mohl určit, zda pro to či ono zpracování údajů má k dispozici řádný souhlas, či nikoli.

---

[9] Viz stanovisko č. 01/2010 k pojmům „správce“ a „zpracovatel“.

Ještě před nahráním obrazů do SSS musí být registrovaní uživatelé jasně uvědomeni o tom, že tyto obrazy budou předmětem systému rozpoznávání tváře. Je ještě důležitější, aby registrovaným uživatelům byla také povinně dána možnost vyjádřit (ne)souhlas s tím, že jejich referenční šablona bude zaregistrována do identifikační databáze. U neregistrovaných a registrovaných uživatelů, kteří nedali souhlas se zpracováním, by tedy nemělo docházet k automatickému navrhování jmenovky, protože obrazy, na kterých se objeví, nebudou vykazovat shodu.

Souhlas poskytnutý osobou nahrávající obraz by se neměl zaměňovat s potřebou legitimního základu pro zpracování osobních údajů jiných jednotlivců, kteří se mohou na obrazu objevit. Za tímto účelem může správce údajů použít jiné legitimní odůvodnění pro zpracování v rámci mezistupňových fází (detekce tváře, normalizace a srovnání), například svůj legitimní zájem, pokud jsou ovšem zavedeny dostatečné omezení a kontroly k ochraně základních práv a svobod subjektů údajů, kteří nejsou těmi, kdo obraz nahrává. Takové kontroly by zajistily, že žádné údaje pocházející ze zpracování nebudou po té, co nebyla zjištěna shoda, nijak uchovány (tj. všechny šablony a přidružené údaje budou bezpečně vymazány). Správce údajů taktéž může chtít zvážit možnost poskytnout svým uživatelům nástroje, které osobě nahrávající obraz umožní rozmazat tváře těch jednotlivců, u kterých nebude nalezena shoda s šablonou v referenční databázi. Registrace šablony jednotlivce v identifikační databázi, což by ve svém důsledku umožnilo nalézt shodu a následně navrhnout jmenovku, by byla možná pouze s vědomým souhlasem subjektu údajů.

Pokud jde o příklad 2, je zcela jistě možné získat souhlas jednotlivce, který je schválen pro přístup k přístroji, již během procesu registrace. Aby byl souhlas platný, musí být k dispozici alternativní a stejně bezpečný systém kontroly přístupu (například silné heslo). Taková alternativní možnost, jež zesiluje aspekt soukromí, by měla být nastavena jako výchozí funkce. Jakmile se jednotlivec sám uvede před kameru propojenou s přístrojem s jasným cílem k němu získat přístup, můžeme se domnívat, že tento jednotlivec tím poskytuje souhlas pro následné zpracování údajů o tváři nutné pro autentizaci, a to i za předpokladu, že tento jednotlivec není schváleným uživatelem přístroje. Úroveň poskytnutých informací však stále musí být dostatečná pro zajištění platnosti souhlasu.

Další využití knihovny obrazů SSS popsané v příkladu 3 by bylo jasným případem porušením zásady účelového omezení, a tudíž nabídnutí takové služby musí být podmíněno apriorním platným souhlasem jednotlivce, ze kterého bude jasně zřejmé, že dojde k uvedenému zpracování obrazů. Týká se to také případu vyhledávače popsaného v příkladu 1. Obrazy, které vyhledávač získal, byly zobrazeny s úmyslem zhlédnutí a nikoli pro účely systému rozpoznávání tváře. Po provozovateli vyhledávače by se požadovalo, aby od subjektů dat získal souhlas k tomu, že budou registrováni v druhém systému rozpoznávání tváře.

Týkalo by se to také případu uvedeného v příkladu 4, neboť uživatel nemůže předpokládat, že obrazy pořízené pro účely ovládání pohybu budou dále zpracovávány. Jestliže správce údajů požaduje souhlas pro zpracovávání z dlouhodobého hlediska (tj. po dlouhou dobu nebo v rámci různých her), musí tento správce uživatelům pravidelně připomínat, je-li tento systém v provozu, a zároveň musí dbát o to, aby byl systém ve výchozím nastavení vypnut.

Stanovisko č. 15/2011 k definici souhlasu se zabývá kvalitou, přístupností a viditelností informací, jež souvisí se zpracováním osobním údajů. Stanovisko říká:

> *„informace musí být poskytovány přímo fyzickým osobám. Nestačí, aby byly informace někde „k dispozici“.*

Informace týkající se funkce rozpoznávání tváře u on-line nebo mobilní služby by tudíž neměly být skryty, ale naopak by měly být jednoduše přístupné a srozumitelné. To zahrnuje i záruku, že samotné kamery nejsou nijak skryté. Správci údajů by měly při uplatňování technologie rozpoznávání tváře zohlednit odůvodněná očekávání veřejnosti ohledně soukromí a měly by se těmito otázkami řádně zabývat.

V této souvislosti není možné souhlas s registrací vyvodit na základě toho, že uživatel přijal obecné podmínky dotyčné služby, kromě případů, kdy hlavním smyslem služby má být rozpoznávání tváře. Je tomu tak proto, že ve většině případů je registrace dodatečnou funkcí a není přímo spojená s používáním on-line nebo mobilní služby. Uživatelé nemusí nutně předpokládat, že tato funkce bude použitím služby aktivována. Za tímto účelem by měla být uživatelům jasně dána možnost vyjádřit s touto funkcí souhlas, a to buď během registrace, nebo později v závislosti na tom, kdy je funkce spuštěna.

Aby mohl být souhlas považován za platný, musí být poskytnuty adekvátní informace o zpracování údajů. Uživatelé by vždy měli mít k dispozici možnost svůj souhlas jednoduše stáhnout. Jakmile by byl souhlas stažen, zpracování pro účely rozpoznávání tváře by mělo okamžitě přestat.

5. Konkrétní rizika a doporučení

Rizika pro soukromí plynoucí ze systému rozpoznávání tváře budou zcela odvislá od druhu uplatněného zpracování a jeho účelu/účelů. V konkrétních fázích procesu rozpoznávání tváře jsou však některá rizika více relevantní. Následující oddíl staví do popředí hlavní rizika a nabízí příslušná doporučení pro osvědčené způsoby.

5.1. Nezákonné zpracování za účelem rozpoznávání tváře

V rámci nastavení on-line může správce údajů obrazy získávat mnoha způsoby. Mohou je poskytnout uživatelé on-line nebo mobilních služeb, jejich přátelé a kolegové nebo třetí strana. Obrazy mohou obsahovat tváře samotných uživatelů a/nebo jiných registrovaných či neregistrovaných uživatelů nebo mohou být získány, aniž by o tom subjekt údajů věděl. Bez ohledu na možné způsoby získání těchto obrazů je nutný právní základ pro jejich zpracování.

Doporučení 1: Jestliže správce údajů obraz získá přímo od subjektu údajů (např. tak, jak je uvedeno v příkladech 2 a 4), musí disponovat jejich platným souhlasem ještě před získáním obrazu a poskytnout dostatečné informace o tom, kdy je spuštěna kamera za účelem rozpoznávání tváře.

Doporučení 2: Jestliže jsou to jednotlivci, kdo pořizuje digitální obrazy a nahrává je do on-line nebo mobilních služeb za účelem rozpoznávání tváře, správci údajů musí zajistit, aby osoby nahrávající obrazy vyjádřily souhlas se zpracováním obrazů, které se může uskutečnit za účelem rozpoznávání tváře.

Doporučení 3: Jestliže správci údajů digitální obrazy jednotlivců získají od třetí strany (např. zkopírováním z internetové stránky, zakoupením od jiného správce údajů), musí pečlivě zhodnotit zdroj a kontext, v němž byly originální obrazy pořízeny, a ujistit se, že obrazy byly zpracovány se souhlasem subjektu údajů.

Doporučení 4: Správci údajů musí zaručit, že digitální obrazy a šablony budou použity pouze pro onen specifický účel, pro který byly poskytnuty. Správci údajů by měly zavést technické kontroly, aby se snížilo riziko, že digitální obrazy budou dále zpracovávány třetí stranou pro účely, k nimž uživatelé nedali souhlas. Správci údajů by měli dát uživatelům k dispozici nástroje pro kontrolu viditelnosti obrazů, které nahráli, a zároveň upravit výchozí nastavení tak, že tyto obrazy nebudou přístupné třetím stranám.

Doporučení 5: Správci údajů musí zaručit, že digitální obrazy jednotlivců, kteří nejsou registrovanými uživateli služby nebo nijak neposkytli souhlas se zpracováním obrazů, budou ze strany správce údajů zpracovávány jenom, pokud bude mít správce legitimní zájem tak činit. V příkladu 1 za situace, kdy není nalezena shoda, by tedy bylo například nutné zpracovávání zastavit a všechny údaje vymazat.

Narušení bezpečnosti během transferu údajů

U on-line a mobilních služeb je pravděpodobné, že bude mezi fází získání obrazu a dalšími fázemi jeho zpracování (např. nahrání obrazu z kamery na internetovou stránku pro extrakci rysů a srovnání) docházet k transferu údajů.

Doporučení 6: Správci údajů musí učinit vhodná opatření k zajištění bezpečnosti transferu údajů. Vhodnými opatřeními mohou být zakódování komunikačních kanálů nebo zakódování obrazu samotného. Měla by být, pokud možno (a zejména v případě autentizace/verifikace), dána přednost lokálnímu zpracování.

5.2. Detekce tváře, normalizace, extrakce rysů

Minimalizace údajů

Šablony, které vytvoří systém rozpoznávání tváře, mohou obsahovat více údajů, než je nezbytně nutné pro provedení specifického účelu nebo účelů.

Doporučení 7: Správci údajů musí zajistit, že údaje extrahované z digitálního obrazu pro vytvoření šablony nebudou nadměrné a budou obsahovat pouze ty informace, jež jsou nezbytné pro specifický účel, přičemž by se tak mělo zabránit dalšímu možnému zpracovávání. Šablony by neměly být mezi systémy rozpoznávání tváře převoditelné.

Narušení bezpečnosti během uchovávání údajů

Pokud jde o identifikaci a autentizaci/verifikaci, je pravděpodobné, že bude nutné šablony uchovávat pro pozdější srovnávání.

Doporučení 8: Správce údajů musí zvážit nejvhodnější umístění pro uchované údaje. Vhodným místem může být přístroj uživatele nebo systémy správy údajů. Správce údajů musí učinit vhodná opatření k zajištění bezpečnosti uchovaných údajů. Vhodným opatřením může být zakódování šablony. Nemělo by být možné získat k šabloně nebo uchovaným údajům neschválený přístup. Zejména co se týče rozpoznávání tváře za účelem verifikace, je možné použít metody biometrického kódování; u těchto metod je kryptografický klíč přímo svázán s biometrickými údaji a vytvoří se znovu pouze tehdy, když je verifikován správný živý biometrický vzorek, zatímco se neuchovává žádný obraz nebo šablona (tím se tvoří druh „nevystopovatelné biometrie“).

Přístup subjektu

Doporučení 9: Správce údajů by měl subjektům údajů poskytnout vhodné mechanismy pro zajištění práva na případný přístup jak k originálním obrazům, tak k šablonám vytvořeným v souvislosti s rozpoznáváním tváře.

V Bruselu dne 22. března 2012

Za pracovní skupinu
předseda
Jakob KOHNSTAMM

IV. MATERIÁLY Z ÚŘEDNÍHO VĚSTNÍKU EVROPSKÉ UNIE

Příloha Věstníku Úřadu pro ochranu osobních údajů (s. 3489 – 3496)

ROZHODNUTÍ KOMISE

ze dne 31. ledna 2011

podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně osobních údajů Státem Izrael v souvislosti s automatizovaným zpracováváním osobních údajů

(oznámeno pod číslem K(2011) 332)

(Text s významem pro EHP)

(2011/61/EU)

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na směrnici Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů [1], a zejména na čl. 25 odst. 6 uvedené směrnice,

po konzultaci s evropským inspektorem ochrany údajů,

vzhledem k těmto důvodům:

(1) V souladu se směrnicí 95/46/ES jsou členské státy povinny zajistit, aby k předávání osobních údajů do třetí země docházelo, pouze pokud dotyčná třetí země zajišťuje odpovídající úroveň ochrany a pokud jsou před předáním údajů dodržovány právní předpisy členských států provádějící ostatní ustanovení směrnice.

(2) Komise může dospět k závěru, že třetí země zajišťuje odpovídající úroveň ochrany. Takové zemi mohou členské státy předávat osobní údaje, aniž by byly nutné dodatečné záruky.

(3) V souladu se směrnicí 95/46/ES má být úroveň ochrany údajů hodnocena s ohledem na všechny okolnosti související s předáním nebo předáváním údajů, a to se zvláštním zřetelem na celou řadu podmínek týkajících se předávání a uvedených v článku 25 této směrnice.

(4) S ohledem na rozdíly v přístupu třetích zemí k ochraně údajů by mělo být dbáno na to, aby hodnocení odpovídající úrovně této ochrany a uplatňování všech rozhodnutí na základě čl. 25 odst. 6 směrnice 95/46/ES nebyla svévolně nebo neodůvodněně diskriminační vůči třetím zemím, kde jsou obdobné podmínky, nebo mezi nimi, a aby nevytvářela skrytou překážku obchodu s ohledem na stávající mezinárodní závazky Evropské unie.

(5) Právní řád Státu Izrael nemá psanou ústavu, avšak ústavní sílu dovodil Nejvyšší soud Státu Izrael u některých „základních zákonů“. Tyto „základní zákony“ doplňuje objemný soubor judikatury, jelikož se právní řád Izraele ve značném rozsahu řídí zásadami obyčejového práva. Právo na soukromí je zahrnuto v „základním zákonu o právu na lidskou důstojnost a svobodu“ v oddíle 7.

(6) Právní normy upravující ochranu osobních údajů ve Státě Izrael vycházejí ve velké míře z norem stanovených směrnicí 95/46/ES a jsou stanoveny v zákoně o ochraně soukromí 5741-1981, naposledy pozměněném v roce 2007 za účelem zavedení nových požadavků na zpracování osobních údajů a podrobné organizace orgánu dozoru.

(7) Tyto právní předpisy v oblasti ochrany údajů dále doplňují vládní rozhodnutí provádějící zákon o ochraně soukromí 5741-1981 a o organizaci a fungování orgánu dozoru, která povětšinou vycházejí z doporučení formulovaných ve zprávě Komise pro přezkum právních předpisů týkajících se databází (Schoffmanova zpráva) pro ministerstvo spravedlnosti.

(8) Ustanovení ohledně ochrany údajů jsou rovněž obsažena v celé řadě právních nástrojů upravujících různá odvětví, jako jsou předpisy ve finančním sektoru, ve zdravotnictví a předpisy týkající se veřejných rejstříků.

(9) Právní normy v oblasti ochrany údajů platné ve Státě Izrael pokrývají všechny základní zásady nutné pro odpovídající úroveň ochrany pro fyzické osoby ve vztahu k zpracování osobních údajů automatizovanými databázemi. Kapitola 2 zákona o ochraně soukromí 5741-1981, která stanoví zásady zpracování osobních údajů, se nevztahuje na zpracování osobních údajů v databázích, které nejsou automatizované (manuální databáze).

(10) Uplatňování právních norem ochrany osobních údajů zaručují správní a soudní prostředky nápravy a nezávislý dozor prováděný dozorčím orgánem, jímž je Izraelský úřad pro právo, informace a technologie (ILITA), který je nadán pravomocemi k provádění šetření a zásahů a je zcela nezávislý.

[1] Úř. věst. L 281, 23.11.1995, s. 31.

(11) Izraelské orgány pro ochranu osobních údajů poskytly vysvětlení a záruky ohledně způsobu výkladu izraelského práva a poskytly záruky ohledně provádění izraelských předpisů na ochranu údajů v souladu s takovým výkladem. Toto rozhodnutí přihlíží k uvedeným vysvětlením a zárukám, a je jimi proto podmíněno.

(12) Stát Izrael je proto třeba považovat za zemi zajišťující odpovídající úroveň ochrany osobních údajů podle směrnice 95/46/ES, pokud jde o automatizované mezinárodní předávání osobních údajů z Evropské unie do Státu Izrael nebo o případy, kdy toto předávání není automatizováno, avšak tyto údaje jsou předmětem dalšího automatizovaného zpracování ve Státě Izrael. Opačně, na mezinárodní předávání osobních údajů z EU do Státu Izrael, u kterého samo předávání a následné zpracování je prováděno výlučně neautomatizovanými prostředky, by se toto rozhodnutí nemělo vztahovat.

(13) V zájmu průhlednosti a aby příslušné orgány v členských státech zajistily ochranu fyzických osob v souvislosti se zpracováním jejich osobních údajů, je nezbytné uvést výjimečné okolnosti, za nichž může být odůvodněno pozastavení určitých toků údajů, bez ohledu na zjištění odpovídající úrovně ochrany.

(14) Závěry týkající se úrovně ochrany osobních údajů v tomto rozhodnutí odkazují na Stát Izrael vymezený podle mezinárodní práva. Další následné předávání příjemci mimo Stát Izrael vymezený podle mezinárodního práva by mělo být považováno za předávání osobních údajů do třetí země.

(15) Pracovní skupina pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů, zřízená podle článku 29 směrnice 95/46/ES, předložila kladné stanovisko k úrovni ochrany osobních údajů, pokud jde o automatizované mezinárodní předávání osobních údajů z Evropské unie, nebo o případy, kdy předávání není automatizované, avšak tyto údaje jsou předmětem dalšího automatizovaného zpracování ve Státě Izrael. Ve svém kladném stanovisku pracovní skupina vyzvala izraelské úřady, aby přijaly další ustanovení, která rozšíří uplatňování izraelských právních předpisů na manuální databáze, výslovně uznají, že bude uplatňování zásada proporcionality na zpracování osobních údajů v soukromé sféře, a která budou vykládat výjimky při mezinárodním předávání tak, aby byl jejich výklad v souladu s požadavky stanovenými v jejím „pracovním dokumentu o jednotném výkladu čl. 26 odst. 1 směrnice 95/46/ES“ ([1]). Toto stanovisko bylo zohledněno při přípravě toho rozhodnutí ([2]).

([1]) Dokument WP114 ze dne 25. listopadu 2005. K dispozici na internetové stránce: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_en.pdf

([2]) Stanovisko 6/2009 k úrovni ochrany osobních údajů v Izraeli. K dispozici na internetové stránce http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp165_en.pdf

(16) Výbor zřízený podle čl. 31 odst. 1 směrnice 95/46/ES nepředložil stanovisko ve lhůtě stanovené jeho předsedou,

PŘIJALA TOTO ROZHODNUTÍ:

Článek 1

1. Pro účely čl. 25 odst. 2 směrnice 95/46/ES se Izrael považuje za zemi poskytující odpovídající úroveň ochrany osobních údajů předávaných z Evropské unie, pokud jde o automatizované předávání osobních údajů z Evropské unie do Izraele nebo o případy, kdy toto předávání není automatizováno, avšak tyto údaje jsou předmětem dalšího automatizovaného zpracování ve Státě Izrael.

2. Orgánem dozoru Státu Izrael, který má pravomoc uplatňovat normy ochrany osobních údajů ve Státě Izrael, je Izraelský úřad pro právo, informace a technologie (ILITA) uvedený v příloze tohoto rozhodnutí.

Článek 2

1. Toto rozhodnutí se zabývá pouze úrovní ochrany zajišťované ve Státě Izrael vymezeném podle mezinárodního práva s cílem naplnit požadavky čl. 25 odst. 1 směrnice 95/46/ES a nedotýká se ostatních podmínek nebo omezení provádějících ostatní ustanovení zmíněné směrnice, které se vztahují na zpracování osobních údajů v členských státech.

2. Toto rozhodnutí se použije v souladu s mezinárodním právem. Rozhodnutím není dotčen status Golanských výšin, pásma Gazy a Západního břehu Jordánu, včetně východního Jeruzaléma podle mezinárodního práva.

Článek 3

1. Aniž jsou dotčeny pravomoci příslušných orgánů členských států přijímat opatření, která zajišťují, aby byly dodržovány vnitrostátní předpisy přijaté na základě jiných ustanovení než článku 25 směrnice 95/46/ES, mohou tyto orgány vykonávat své stávající pravomoci, aby pozastavily předávání údajů příjemci ve Státě Izrael s cílem chránit fyzické osoby v souvislosti se zpracováním jejich osobních údajů v těchto případech:

a) pokud příslušný izraelský orgán zjistí, že příjemce nedodržuje standardy uplatňované v oblasti ochrany, nebo

b) pokud je velmi pravděpodobné, že nebyly dodržovány normy týkající se ochrany, pokud se lze důvodně domnívat, že příslušný orgán Státu Izrael včas nepřijal nebo nepřijme odpovídající opatření nezbytná pro vyřešení dané věci; pokud by pokračování v předávání údajů vyvolalo bezprostřední riziko vzniku vážné újmy subjektům údajů a pokud příslušné orgány členského státu za daných okolností přiměřeně usilují o informování strany odpovědné za zpracování údajů usazené ve Státě Izrael a poskytly jí příležitost zaujmout stanovisko.

2. Pozastavení předávání údajů skončí, jakmile je zajištěno dodržování norem ochrany a jakmile je o této skutečnosti informován příslušný orgán členského stát.

Článek 4

1. Členské státy neprodleně uvědomí Komisi o přijetí opatření podle článku 3.

2. Členské státy a Komise se rovněž vzájemně informují o případech, kdy opatření přijatá subjekty pověřenými zajištěním dodržování norem ochrany ve Státě Izrael nejsou dostatečná.

3. Pokud informace shromážděné podle článku 3 a podle odstavců 1 a 2 tohoto článku prokážou, že kterýkoli subjekt pověřený zajištěním dodržování norem ochrany ve Státě Izrael neplní účinně svou úlohu, uvědomí o tom Komise příslušný orgán Státu Izrael a, bude-li třeba, předloží návrh opatření postupem podle čl. 31 odst. 2 směrnice 95/46/ES s cílem zrušit toto rozhodnutí, pozastavit je nebo omezit jeho oblast působnosti.

Článek 5

Komise sleduje provádění tohoto rozhodnutí a jakékoli předmětné poznatky sdělí výboru zřízenému podle článku 31 směrnice 95/46/ES, včetně jakýchkoliv důkazů, které by mohly mít vliv na hodnocení prováděné podle článku 1 tohoto rozhodnutí, zda je úroveň ochrany ve Státě Izrael odpovídající ve smyslu článku 25 směrnice 95/46/ES, a jakýchkoliv důkazů, že se toto rozhodnutí provádí diskriminačním způsobem. Komise zejména sleduje zpracovávání osobních údajů v manuálních databázích.

Článek 6

Členské státy přijmou veškerá opatření, která jsou nezbytná pro dosažení souladu s tímto rozhodnutím, do tří měsíců od data jeho oznámení.

Článek 7

Toto rozhodnutí je určeno členským státům.

V Bruselu dne 31. ledna 2011.

Za Komisi

Viviane REDING

místopředsedkyně

PŘÍLOHA

Příslušný orgán dozoru uvedený v čl. 1 odst. 2 tohoto rozhodnutí:

The Israeli Law, Information and Technology Authority (Izraelský úřad pro právo, informace a technologie)
The Government Campus
9th floor
125 Begin Rd.
Tel Aviv
Izrael
Poštovní adresa:
P.O. Box 7360
Tel Aviv, 61072
Tel.: + 972 3 7634050
Fax: + 972 2 6467064
E-mail: ILITA@justice.gov.il
Internetová stránka: http://www.justice.gov.il/MOJEng/RashutTech/default.htm

ROZHODNUTÍ

PROVÁDĚCÍ ROZHODNUTÍ KOMISE

ze dne 21. srpna 2012

podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně osobních údajů Uruguayskou východní republikou v souvislosti s automatizovaným zpracováváním osobních údajů

(oznámeno pod číslem C(2012) 5704)

(Text s významem pro EHP)

(2012/484/EU)

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na směrnici Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů [1], a zejména na čl. 25 odst. 6 uvedené směrnice,

po konzultaci s evropským inspektorem ochrany údajů [2],

vzhledem k těmto důvodům:

(1) V souladu se směrnicí 95/46/ES jsou členské státy povinny zajistit, aby k předávání osobních údajů do třetí země docházelo, pouze pokud dotyčná třetí země zajišťuje odpovídající úroveň ochrany a pokud budou před předáním údajů dodržovány právní předpisy členských států provádějící ostatní ustanovení směrnice.

(2) Komise může dospět k závěru, že třetí země zajišťuje odpovídající úroveň ochrany. Takové zemi mohou členské státy předávat osobní údaje, aniž by byly nutné dodatečné záruky.

(3) V souladu se směrnicí 95/46/ES má být úroveň ochrany údajů hodnocena s ohledem na všechny okolnosti související s předáním nebo předáváním údajů, a to se zvláštním zřetelem na celou řadu podmínek týkajících se předávání a uvedených v článku 25 této směrnice.

(4) S ohledem na rozdíly v přístupu třetích zemí k ochraně údajů by mělo být dbáno na to, aby hodnocení odpovídající úrovně této ochrany a uplatňování všech rozhodnutí na základě čl. 25 odst. 6 směrnice 95/46/ES nebyla svévolně nebo neodůvodněně diskriminační vůči třetím zemím, kde jsou obdobné podmínky, nebo mezi nimi, a aby nevytvářela skrytou překážku obchodu s ohledem na stávající mezinárodní závazky Evropské unie.

(5) Ústava Uruguayské východní republiky přijatá v roce 1967 výslovně neuznává právo na soukromí ani právo na ochranu osobních údajů. Seznam základních práv však není konečný, jelikož v článku 72 ústavy je stanoveno, že „uvedení práv, povinností a záruk v ústavě nevylučuje ostatní práva, povinnosti a záruky, jež jsou neodmyslitelně spjaty s osobností člověka nebo které vyplývají z republikánské formy vlády“. Paragraf 1 zákona č. 18.331 o ochraně osobních údajů a opravném prostředku „Habeas Data“ ze dne 11. srpna 2008 (Ley Nº 18.331 de Protección de Datos Personales y Acción de „Habeas Data“) jednoznačně uvádí, že „člověku je vlastní právo na ochranu osobních údajů, a je proto obsaženo v článku 72 ústavy republiky“. V článku 332 ústavy je uvedeno, že uplatňování pravidel obsažených v této ústavě, která uznávají práva jednotlivců, jakož i pravidel přiznávajících práva a ukládajících povinnosti orgánům veřejné správy, by nemělo být znemožněno neexistencí příslušných předpisů, nýbrž tyto budou nahrazeny použitím základů podobných zákonů, právních zásad a obecně uznávaných doktrín.

(6) Právní normy ochrany osobních údajů v Uruguayské východní republice vycházejí především ze standardu stanoveného směrnicí 95/46/ES a jsou uvedeny v zákoně č. 18.331 o ochraně osobních údajů a opravném prostředku „Habeas Data“ (Ley Nº 18.331 de Protección de Datos Personales y Acción de „Habeas Data“) ze dne 11. srpna 2008. Tento zákon se vztahuje jak na fyzické, tak na právnické osoby.

(7) Tento zákon je dále doplněn vyhláškou č. 414/009 ze dne 31. srpna 2009, která byla přijata za účelem vyjasnění některých aspektů zákona a stanovení podrobné

[1] Úř. věst. L 281, 23.11.1995, s. 31.
[2] Dopis ze dne 31. srpna 2011.

úpravy organizace, pravomocí a fungování orgánu dohlížejícího na ochranu údajů. V preambuli vyhlášky se uvádí, že v této věci je vhodné přizpůsobit vnitrostátní právní systém nejuznávanějšímu srovnatelnému právnímu režimu, a to v zásadě režimu stanovenému evropskými zeměmi prostřednictvím směrnice 95/46/ES.

(8) Ustanovení o ochraně údajů jsou obsažena rovněž v řadě zvláštních právních předpisů, kterými je upraveno vytváření a správa databází, zejména v právních předpisech, které upravují určité veřejné rejstříky (veřejných listin, průmyslového vlastnictví a obchodních značek, osobních úkonů, nemovitostí, těžebních práv, nebo úvěrové solventnosti). Ve smyslu článku 332 ústavy se zákon č. 18.331 dodatečně k těmto předpisům používá ve vztahu k těm otázkám, jež nejsou upraveny zvláštními právními předpisy.

(9) Právní normy o ochraně údajů uplatňované v Uruguayské východní republice obsahují všechny základní zásady nezbytné pro zajištění odpovídající úrovně ochrany fyzických osob a současně stanoví výjimky a omezení pro ochranu důležitých veřejných zájmů. Do těchto právních norem o ochraně údajů a výjimek se promítají zásady stanovené ve směrnici 95/46/ES.

(10) Uplatňování právních norem o ochraně údajů je zaručeno správními a soudními opravnými prostředky, zejména žalobou „habeas data“, která subjektu údajů umožňuje pohnat správce údajů před soud za účelem vymožení svého práva na přístup k údajům, jejich opravu a výmaz, a dále nezávislým dohledem prováděným orgánem dozoru (Útvar pro regulaci a kontrolu osobních údajů, Unidad Reguladora y de Control de Datos Personales (URCDP)), který je vybaven pravomocí vyšetřovat, zasahovat a sankcionovat v souladu s článkem 28 směrnice 95/46/ES, a který koná zcela nezávisle. Kterákoli zainteresovaná strana má navíc právo vymáhat soudní cestou náhradu škody, kterou utrpěla v důsledku protiprávního zpracování jejích osobních údajů.

(11) Uruguayské orgány na ochranu osobních údajů poskytly vysvětlení a záruky ohledně způsobu výkladu uruguayského práva a poskytly záruky ohledně provádění uruguayských předpisů na ochranu údajů v souladu s takovým výkladem. Uruguayské orgány na ochranu údajů vysvětlily, že podle článku 332 ústavy se zákon č. 18.331 používá dodatečně ke zvláštním právním předpisům, které upravují vytváření a správu specifických databází, ve vztahu k těm otázkám, které tyto zvláštní právní nástroje neupravují. Stejně tak vysvětlily, že pokud jde o seznamy uvedené v paragrafu 9 C) zákona č. 18.331, a které nevyžadují souhlas subjektu údajů se zpracováním, ze zákona se uplatňují také práva subjektů údajů, zejména zásady omezení účelu a přiměřenosti údajů, a že tato práva jsou pod dohledem orgánů pro ochranu údajů. Co se týče zásady transparentnosti, uruguayské orgány pro ochranu údajů informovaly, že ve všech případech se uplatňuje povinnost poskytnout subjektu údajů nezbytné informace. Pokud jde o právo na přístup k údajům, orgán na ochranu údajů vysvětlil, že při podání žádosti stačí, když subjekt údajů prokáže svou totožnost. Uruguayské orgány pro ochranu údajů objasnily, že výjimky týkající se zásady předávání údajů do jiných zemí, které jsou uvedeny v paragrafu 23 odst. 1 zákona č. 18.331, nelze chápat v tom smyslu, že mají širší uplatnění, než jaké je uvedeno v čl. 26 odst. 1 směrnice 95/46/ES.

(12) Toto rozhodnutí přihlíží k uvedeným vysvětlením a zárukám a vychází z nich.

(13) Uruguayská východní republika je také smluvní stranou Americké úmluvy o lidských právech (Pakt ze San José, Costa Rica) ze dne 22. listopadu 1969, která vstoupila v platnost dne 18. července 1978 ([1]). Článek 11 této úmluvy stanoví právo na soukromí a v článku 30 je uvedeno, že omezení uplatnění nebo využití práv či svobod, které úmluva uznává, lze použít podle této úmluvy pouze v souladu s právními předpisy přijatými v obecném zájmu a v souladu s účelem, pro který bylo takové omezení přijato (článek 30). Uruguayská východní republika se navíc podřizuje jurisdikci Meziamerického soudu pro lidská práva. Poté co příslušný poradní výbor vydal kladné stanovisko, vyzvali zástupci ministrů Rady Evropy na svém 1118. zasedání dne 6. července 2011 Uruguayskou východní republiku, aby přistoupila k Úmluvě o ochraně osob s ohledem na automatizované zpracování osobních údajů (ETS č. 108) a k jejímu dodatkovému protokolu (ETS č. 118) ([2]).

(14) Uruguayskou východní republiku je proto třeba považovat za zemi zajišťující odpovídající úroveň ochrany osobních údajů podle směrnice 95/46/ES.

(15) Toto rozhodnutí by se mělo týkat přiměřenosti ochrany zajištěné v Uruguayské východní republice s cílem splnit požadavky čl. 25 odst. 1 směrnice 95/46/ES. Nemělo by

([1]) Organizace amerických států; OAS, Sbírka smluv, č. 36, 1144 U.N.T.S. 123. http://www.oas.org/juridico/english/treaties/b-32html

([2]) Rada Evropy: https://wcd.coe.int/wcd/ViewDoc.jsp?Ref=CM/Del/Dec(2011)1118/10.3&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864

se týkat jiných podmínek či omezení, které provádějí jiná ustanovení zmíněné směrnice, a které se týkají zpracování osobních údajů v členských státech.

(16) V zájmu transparentnosti, a aby příslušné orgány v členských státech zajistily ochranu fyzických osob v souvislosti se zpracováním jejich osobních údajů, je nezbytné uvést výjimečné okolnosti, za nichž může být odůvodněno pozastavení určitých toků údajů, bez ohledu na zjištění odpovídající úrovně ochrany.

(17) Komise by měla sledovat, jak toto rozhodnutí funguje, a veškeré relevantní poznatky sdělovat výboru zřízenému podle článku 31 směrnice 95/46/ES. Sledování by se mělo zaměřit mimo jiné na režim předávání údajů, který Uruguayská východní republika používá v rámci mezinárodních smluv.

(18) Pracovní skupina pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů, zřízená podle článku 29 směrnice 95/46/ES, předložila kladné stanovisko k úrovni ochrany osobních údajů, k němuž bylo přihlédnuto při přípravě tohoto rozhodnutí ([1]).

(19) Opatření tohoto rozhodnutí jsou v souladu se stanoviskem výboru zřízeného podle čl. 31 odst. 1 směrnice 95/46/ES,

PŘIJALA TOTO ROZHODNUTÍ:

Článek 1

1. Pro účely čl. 25 odst. 2 směrnice 95/46/ES se Uruguayská východní republika považuje za zemi zajišťující odpovídající úroveň ochrany osobních údajů předávaných z Evropské unie.

2. V příloze tohoto rozhodnutí je uveden příslušný orgán dozoru Uruguayské východní republiky pro uplatňování právních norem ochrany údajů v Uruguayské východní republice.

Článek 2

1. Aniž jsou dotčeny pravomoci příslušných orgánů členských států přijímat opatření, která zajišťují, aby byly dodržovány vnitrostátní předpisy přijaté na základě jiných ustanovení než článku 25 směrnice 95/46/ES, mohou tyto orgány vykonávat své stávající pravomoci, aby pozastavily předávání údajů příjemci v Uruguayské východní republice s cílem chránit fyzické osoby v souvislosti se zpracováním jejich osobních údajů v těchto případech:

a) pokud příslušný uruguayský orgán zjistí, že příjemce nedodržuje standardy uplatňované v oblasti ochrany, nebo

b) pokud existuje důvodná pravděpodobnost, že normy ochrany jsou porušovány, a pokud se lze důvodně domnívat, že příslušný uruguayský orgán včas nepřijal nebo nepřijme odpovídající opatření nezbytná pro vyřešení dané věci; pokud by pokračování v předávání údajů vyvolalo bezprostřední riziko vzniku vážné újmy subjektům údajů a pokud příslušné orgány členského státu za daných okolností vyvinuly přiměřené úsilí o informování strany odpovědné za zpracování údajů usazené v Uruguayské východní republice a poskytly jí příležitost zaujmout stanovisko.

2. Pozastavení předávání údajů skončí, jakmile je zajištěno dodržování norem ochrany a jakmile je o této skutečnosti informován příslušný orgán členského státu.

Článek 3

1. Členské státy neprodleně uvědomí Komisi o přijetí opatření podle článku 2.

2. Členské státy a Komise se rovněž vzájemně informují o případech, kdy opatření přijatá subjekty pověřenými zajištěním dodržování norem ochrany v Uruguayské východní republice nejsou dostatečná.

3. Pokud informace shromážděné podle článku 2 a podle odstavců 1 a 2 tohoto článku prokážou, že kterýkoli subjekt pověřený zajištěním dodržování norem ochrany v Uruguayské východní republice neplní účinně svou úlohu, uvědomí o tom Komise příslušný uruguayský orgán a v případě potřeby předloží návrh opatření postupem podle čl. 31 odst. 2 směrnice 95/46/ES s cílem zrušit toto rozhodnutí, pozastavit je nebo omezit jeho oblast působnosti.

Článek 4

Komise sleduje provádění tohoto rozhodnutí a jakékoli předmětné poznatky sdělí výboru zřízenému podle článku 31 směrnice 95/46/ES, včetně jakýchkoliv důkazů, které by mohly mít vliv na hodnocení prováděné podle článku 1 tohoto rozhodnutí, zda je úroveň ochrany v Uruguayské východní republice odpovídající ve smyslu článku 25 směrnice 95/46/ES, a jakýchkoliv důkazů, že se toto rozhodnutí provádí diskriminačním způsobem.

Článek 5

Členské státy přijmou veškerá opatření, která jsou nezbytná pro dosažení souladu s tímto rozhodnutím, do tří měsíců od data jeho zveřejnění.

([1]) Stanovisko č. 6/2010 o úrovni ochrany osobních údajů v Uruguayské východní republice. Dostupné na http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp177_en.pdf

Článek 6

Toto rozhodnutí je určeno členským státům.

V Bruselu dne 21. srpna 2012.

Za Komisi
Viviane REDING
místopředsedkyně

PŘÍLOHA

Příslušný orgán dozoru uvedený v čl. 1 odst. 2 tohoto rozhodnutí:

Unidad Reguladora y de Control de Datos Personales (URCDP),
Andes 1365, Piso 8
Tel. +598 2901 2929 linka: 1352
11.100 Montevideo
URUGUAY

Kontaktní e-mailová adresa: http://www.datospersonales.gub.uy/sitio/contactenos.aspx

Elektronické stížnosti: http://www.datospersonales.gub.uy/sitio/contactenos.aspx

Internetová stránka: http://www.datospersonales.gub.uy/sitio/contactenos.aspx

Vyberte si z nabídky věstníků a zpravodajů

Předpokládaná výše předplatného pro rok 2013 a periodicita distribuovaných věstníků a zpravodajů:		
Název věstníku, zpravodaje	**Předpokládaná periodicita**	**Záloha na předplatné**
Věstník Úřadu pro ochranu osobních údajů	4krát ročně	300 Kč
Ústřední věstník ČR	6krát ročně	400 Kč
Věstník Ministerstva zemědělství	3krát ročně	200 Kč
Věstník Ministerstva zdravotnictví	10krát ročně	1500 Kč
Cenový věstník Ministerstva financí	16krát ročně	1800 Kč
Finanční zpravodaj	6krát ročně	600 Kč
Věstník Ministerstva školství, mládeže a tělovýchovy ČR	12krát ročně	500 Kč

SEVT®

Objednávky přijímá a vyřizuje: SEVT, a. s., oddělení předplatného, Pekařova 4, 181 06 Praha 8 – Bohnice
Tel.: 283 090 354 • Fax: 233 553 422
e-mail: predplatne@sevt.cz
Obsahy věstníků a zpravodajů na www.sevt.cz

Oficiální distributor Úředního věstníku EU

www.sevt.cz

Věstník Úřadu pro ochranu osobních údajů

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

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

Distribuce: Předplatné, jednotlivé částky na objednávku i za hotové – SEVT, a. s., Pekařova 4, 181 06 Praha 8-Bohnice, telefon: 283 090 352, 283 090 354, fax: 233 553 422; drobný prodej v prodejnách SEVT, a. s. – Praha 4, Jihlavská 405, tel.: 261 260 414 – Brno, Česká 14, tel.: 542 213 962– 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

62012003