



VĚSTNÍK

ÚŘADU PRO OCHRANU OSOBNÍCH ÚDAJŮ

2009

Částka 51

20. března 2009

Cena 120 Kč

OBSAH

Úvod	2982
I. Registrace	
Přehled zrušených registrací za období od 1. 11. 2008 do 20. 2. 2009	2983
II. Stanoviska Úřadu	
Stanovisko č. 1/2009: Zpracování osobních údajů na základě smluv uzavíraných se zpracovateli (tzv. řetězení zpracovatelů osobních údajů)	2984
Stanovisko č. 2/2009: Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště	2985
III. Sdělení Úřadu	
a) Úřad pro ochranu osobních údajů k problémům z praxe – č. 1/2009: K možnosti rozšíření kompetencí Úřadu ve vztahu k zákonu č. 106/1999 Sb., o svobodném přístupu k informacím	2989
b) Komentář ke Stanovisku č. 3/2008 Pracovní skupiny pro ochranu dat podle článku 29 (WP29) k návrhu Mezinárodního standardu pro ochranu soukromí v rámci Světového antidopingového kodexu	2991
c) Stanovisko č. 2/2007 Pracovní skupiny pro ochranu dat podle článku 29 (WP29) k informování cestujících o předávání údajů jmenné evidence cestujících (PNR) orgánům Spojených států přijaté dne 15. února 2007 a revidované a aktualizované dne 24. června 2008 (WP 132, 00345/07/CS; WP 151, 00345-01/07/CS) Překlad pořízený Evropskou komisí, přetisk v původní podobě	2992
d) Stanovisko č. 3/2008 Pracovní skupiny pro ochranu dat podle článku 29 (WP29) k návrhu Mezinárodního standardu pro ochranu soukromí v rámci Světového antidopingového kodexu přijaté dne 1. srpna 2008 (WP 156, 1576-00-00-08/CS) Překlad pořízený Evropskou komisí, přetisk v původní podobě	3005
IV. Materiály z Úředního věstníku Evropské unie	
Rámcové rozhodnutí Rady 2008/977/SVV ze dne 27. listopadu 2008 o ochraně osobních údajů zpracovávaných v rámci policejní a justiční spolupráce v trestních věcech Akty přijaté na základě hlavy VI Smlouvy o EU Přetisk z Úředního věstníku Evropské unie	3015

ÚVOD

Částka 51 Věstníku Úřadu pro ochranu osobních údajů je první částkou roku 2009. Obsahuje přehled zrušených registrací za období od 1. 11. 2008 do 20. 2. 2009.

V rubrice Stanoviska Úřadu jsou publikovány dva materiály. Prvním je Stanovisko č. 1/2009 „Zpracování osobních údajů na základě smluv uzavíraných se zpracovateli (tzv. řetězení zpracovatelů osobních údajů).“ V souvislosti se zpracováním osobních údajů zejména velkými, popřípadě nadnárodními, společnostmi se Úřad setkává s otázkou tzv. řetězení zpracovatelů. Jedná se o situaci, kdy správcem osobních údajů pověřený zpracovatel sám přenáší některé operace s osobními údaji na další subjekty. Stanovisko objasňuje a definuje postavení těchto subjektů z pohledu zákona o ochraně osobních údajů.

Druhým materiálem této rubriky je Stanovisko č. 2/2009 „Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště“. Ochrana soukromí zaměstnanců je zvláště důležitou oblastí zpracování osobních údajů, a proto se jí Úřad opakovaně zabývá. Předmětem tohoto textu je pojednání o ochraně těchto osobních údajů zaměstnanců, které vznikají pomocí technických prostředků, jako jsou například telefonní ústředny či internet.

Rubriku Sdělení Úřadu otevírá materiál oddílu Úřad pro ochranu osobních údajů k problémům z praxe nazvaný „K možnosti rozšíření kompetencí Úřadu ve vztahu k zákonu č. 106/1999 Sb.“. Materiál se zabývá otázkami vztahu mezi zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, a zákona č. 106/1999 Sb., o svobodném přístupu k informacím, a posuzuje možnost bližšího propojení. Na základě předložených právních důvodů Úřad dochází k závěru, že by k takovému propojení nemělo dojít.

Součástí rubriky Sdělení jsou dvě stanoviska Pracovní skupiny pro ochranu dat podle článku 29 (WP29). Prvním je Stanovisko č. 2/2007 k informování cestujících o předávání údajů jmenné evidence cestujících (PNR) orgánům Spojených států.

Druhým publikovaným materiálem výše uvedené pracovní skupiny je Stanovisko č. 3/2008 k návrhu Mezinárodního standardu pro ochranu soukromí v rámci Světového antidopingového kodexu. Toto stanovisko je uvozeno materiálem, který je nazván Komentář ke Stanovisku č. 3/2008 Pracovní skupiny pro ochranu dat podle článku 29 (WP29). Cílem komentáře je upozornit na skutečnost, že výše uvedené stanovisko bylo pracovní skupinou WP29 zpracováno v příliš krátkém termínu a bez znalosti důležitých souvislostí. Předpokládá se, že výše uvedená pracovní skupina se k této záležitosti vrátí a definitivní stanovisko zformuluje v polovině roku 2009. Obě stanoviska pracovní skupiny (WP29) jsou překlady pořízené Evropskou komisí a jsou to přetisky v původní podobě.

Částku uzavírá rubrika Materiály z Úředního věstníku Evropské unie, která obsahuje materiál Rámcové rozhodnutí Rady 2008/977/SVV o ochraně osobních údajů zpracovávaných v rámci policejní a justiční spolupráce v trestních věcech. Jedná se o přetisk z Úředního věstníku Evropské unie.

Přehled zrušených registrací

Číslo registrace	Subjekt	Datum zrušení
00000473/001	HYPO STAVEBNÍ SPOŘITELNA, A.S.	4.12.2008
00000473/002	HYPO STAVEBNÍ SPOŘITELNA, A.S.	4.12.2008
00000473/003	HYPO STAVEBNÍ SPOŘITELNA, A.S.	4.12.2008
00000492/001	DOMOV PRO OSOBY SE ZDRAVOTNÍM POSTIŽENÍM TRMICE, PŘÍSPĚVKOVÁ ORGANIZACE	1.1.2009
00000492/002	DOMOV PRO OSOBY SE ZDRAVOTNÍM POSTIŽENÍM TRMICE, PŘÍSPĚVKOVÁ ORGANIZACE	1.1.2009
00001188/016	UNILEVER ČR, SPOL. S R.O.	3.1.2009
00001188/046	UNILEVER ČR, SPOL. S R.O.	3.1.2009
00001228/005	VODAFONE CZECH REPUBLIC A.S.	12.12.2008
00001228/007	VODAFONE CZECH REPUBLIC A.S.	12.12.2008
00001228/013	VODAFONE CZECH REPUBLIC A.S.	12.12.2008
00001228/015	VODAFONE CZECH REPUBLIC A.S.	12.12.2008
00001471/012	MĚSTSKÁ ČÁST PRAHA 12	10.2.2009
00002048/001	DELVITA A.S.	1.11.2008
00002048/002	DELVITA A.S.	1.11.2008
00003496/001	BENZINA TRADE A. S.	1.1.2009
00005348/001	ČESKÝ NORMALIZAČNÍ INSTITUT	21.1.2009
00005348/002	ČESKÝ NORMALIZAČNÍ INSTITUT	21.1.2009
00005348/003	ČESKÝ NORMALIZAČNÍ INSTITUT	21.1.2009
00008180/001	EUROPA MÖBEL PRAHA OBCHOD NÁBYTKEM K.S.	20.12.2008
00008181/001	EUROPA MÖBEL OSTRAVA K.S.	20.12.2008
00008226/001	SPRÁVA LETIŠTĚ PRAHA, S.P.	13.1.2009
00008226/002	SPRÁVA LETIŠTĚ PRAHA, S.P.	13.1.2009
00008226/003	SPRÁVA LETIŠTĚ PRAHA, S.P.	13.1.2009
00008226/004	SPRÁVA LETIŠTĚ PRAHA, S.P.	13.1.2009
00008226/005	SPRÁVA LETIŠTĚ PRAHA, S.P.	13.1.2009
00009391/001	EUROPA MÖBEL BRNO K. S.	20.12.2008
00011747/002	HORST, S.R.O.	30.12.2008
00024816/001	KANZELSBERGER A.S.	4.12.2008
00026192/001	SAMSUNG ZRT., ČESKÁ ORGANIZAČNÍ SLOŽKA	4.2.2009
00026192/002	SAMSUNG ZRT., ČESKÁ ORGANIZAČNÍ SLOŽKA	4.2.2009
00026192/003	SAMSUNG ZRT., ČESKÁ ORGANIZAČNÍ SLOŽKA	4.2.2009
00030007/001	TV BARRANDOV S.R.O.	6.11.2008
00032388/001	SLOW GRETY S.R.O.	27.1.2009

II. STANOVISKA ÚŘADU

Stanovisko č. 1/2009

únor 2009

Zpracování osobních údajů na základě smluv uzavíraných se zpracovateli (tzv. řetězení zpracovatelů osobních údajů)

Úvod

V souvislosti se zpracováním osobních údajů zejména velkými popřípadě nadnárodními společnostmi se Úřad setkává s otázkou tzv. řetězení zpracovatelů. Jedná se o situaci, kdy správcem osobních údajů pověřený zpracovatel sám přenáší některé operace s osobními údaji na další subjekty, přičemž otázkou je, zda i tyto subjekty jsou v postavení zpracovatele osobních údajů ve smyslu zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (dále jen „zákon o ochraně osobních údajů“).

Odůvodnění

Východiskem pro posouzení zmíněné otázky jsou především ustanovení definující správce a zpracovatele. Podle § 4 písm. j) a k) zákona o ochraně osobních údajů je správcem každý subjekt, který určuje účel a prostředky zpracování, provádí zpracování a odpovídá za něj, a zpracovatelem každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona. V souladu s § 4 písm. j) zákona o ochraně osobních údajů je oprávněn zpracováním zmocnit nebo pověřit zpracovatele, pokud zvláštní zákon nestanoví jinak, pouze správce.

S ohledem na uvedené je zřejmé, že je to právě správce, který rozhodne, že určitého cíle bude dosahovat pomocí zpracování osobních údajů, a jak konkrétně bude takové zpracování probíhat. Tato pozice (toho, kdo rozhodl o zpracování a jeho veškerých parametrech) se odráží v odpovědnosti správce za celé zpracování, která v sobě zahrnuje i odpovědnost za případné přenechání některých, popř. i všech, fází či kroků zpracování jiným subjektům – zpracovatelům. Je proto nepřipustné, aby zpracovatel, který je pověřen pouze jasně vymezenými úkoly, sám rozhodl o tom, že zpracování bude prováděno jiným způsobem. Takové řetězení zpracovatelů by ve svém důsledku mohlo vést ke vzniku stavu, kdy správce, který o zpracování rozhodl, a jehož jménem se celé zpracování provádí, přestává mít toto zpracování pod kontrolou a nemůže tak dostát svým povinnostem např. podle § 12 a 21 zákona o ochraně osobních údajů.

Zajištění náležité úrovně ochrany osobních údajů, a tedy i ochrany soukromí, které je základním smyslem zákona

o ochraně osobních údajů, je dáno i tím, že v případě, kdy správce ponechává zpracování na zpracovateli, je povinen uzavřít s ním smlouvu o zpracování osobních údajů podle § 6 zákona o ochraně osobních údajů, ve které vymezí úkoly zpracovatele a vyžádá si záruky ohledně zabezpečení dat. Ze znění tohoto ustanovení zcela jednoznačně vyplývá, že tuto smlouvu může uzavřít pouze správce se zpracovatelem, nikoli zpracovatel s dalším subjektem.

Správce i zpracovatel však samozřejmě mohou využívat práce či služeb jiných osob (fyzických i právnických), a to v režimu § 14 zákona o ochraně osobních údajů. Toto ustanovení se vztahuje na zaměstnance správce či zpracovatele a dále na jiné osoby (fyzické i právnické), které zpracovávají údaje na základě smlouvy se správcem nebo zpracovatelem. Smlouvou je v tomto ustanovení myšlena pracovní či jiná obdobná smlouva, nikoli smlouva o zpracování osobních údajů podle § 6 zákona o ochraně osobních údajů.

Zaměstnance nebo např. osoby spolupracující na základě dohody o pracovní činnosti či dohody o provedení práce nelze tedy označit za zpracovatele ve smyslu § 4 písm. k) zákona o ochraně osobních údajů. Na uvedeném nic nemění skutečnost, že osoby spolupracující v režimu podle § 14 zákona o ochraně osobních údajů provádějí, v rámci své pracovní činnosti pro správce nebo zpracovatele, s osobními údaji úkony, které lze označit jako zpracování ve smyslu zákona o ochraně osobních údajů.

Odpovědnost za toto zpracování však nese pouze správce nebo zpracovatel (kromě povinnosti podle § 15 zákona o ochraně osobních údajů). Pro určení odpovědného subjektu v konkrétním případě je rozhodné, zda k zapojení těchto dalších osob na straně zpracovatele došlo v mezích oprávnění vyplývajících mu ze smlouvy uzavřené podle § 6 zákona o ochraně osobních údajů, a to především s ohledem na záruky ohledně zabezpečení ochrany osobních údajů, které zpracovatel v rámci smlouvy o zpracování osobních údajů poskytl, nebo nikoliv. Zapojení třetích osob na straně zpracovatele je tedy nutno posuzovat primárně z hlediska požadavků podle § 13 zákona o ochraně osobních údajů, a to včetně zajištění kontroly dodržování bezpečnostních opatření a plnění pokynů pro zpracování osobních údajů – obdobně, jako by se jednalo o vlastní zaměstnance zpracovatele.

K uvedenému výkladu je dále možné doplnit, že v postavení zpracovatele se ocitá pouze ten, kdo se skutečně podílí na zpracování osobních údajů, tj. vykonává pro správce určité operace s těmito daty, nikoli však ten, kdo správci např. pouze poskytuje infrastrukturu (zejména HW či SW) a s osobními údaji jinak

nenakládá. V případě, kdy zpracovatel překročí oprávnění, které mu vyplývá z pověření správce, tj. ze smlouvy podle § 6 zákona o ochraně osobních údajů, fakticky stanoví nový účel zpracování, pro nějž se stává správcem (oprávněným, či neoprávněným) s veškerou z toho vyplývající odpovědností.

Závěr

Řetězení zpracovatelů, tj. situace, kdy by se z rozhodnutí

zpracovatele na zpracování údajů podílel další subjekt v postavení zpracovatele ve smyslu § 4 písm. k) zákona o ochraně osobních údajů, není tímto zákonem umožněno, což nevylučuje, aby se na zpracování osobních údajů ve výše uvedeném smyslu podílely i jiné osoby.

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

Stanovisko č. 2/2009

únor 2009

Ochrana soukromí zaměstnanců se zvláštním zřetelem k monitoringu pracoviště

Úvod

Ochrana soukromí zaměstnanců je zvláště důležitou oblastí zpracování osobních údajů, a proto se jí opakovaně zabýval i Úřad pro ochranu osobních údajů (dále jen „ÚOOÚ“) ve svých vyjádřeních a stanoviscích.

Předmětem tohoto textu není pojednat o ochraně veškerých osobních údajů zaměstnanců, například těch, které jsou součástí osobního spisu, nýbrž pouze těch, které vznikají pomocí technických prostředků, jako jsou telefonní ústředny a internet. Text vychází ze stanoviska Ministerstva práce a sociálních věcí ČR (dále jen „MPSV“) ze dne 14. září 2007, čj. 2007/55722–52.

Biometrické údaje v docházkových systémech, monitorování telefonních rozhovorů a kamerové systémy na pracovišti nejsou předmětem tohoto stanoviska.

Shrnutí právních předpisů, které se problematiky dotýkají

Předpisem, který reguluje osobnostní práva obecně, je zákon č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů. V § 12 odst. 1 stanoví, že písemnosti osobní povahy, podobizny, obrazové snímky a obrazové a zvukové záznamy týkající se člověka nebo jeho projevů osobní povahy, smějí být pořízeny nebo použity jen s jeho svolením. K této právní normě je speciální zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, který je ve vztahu k ochraně soukromí na pracovišti obecným předpisem.¹⁾

Zvláštním předpisem je zákon č. 262/2006 Sb., zákoník

práce, ve znění pozdějších předpisů (dále jen „nový zákoník práce“ nebo „NZZP“), který nabyt účinnosti od 1. 1. 2007. S novým zákoníkem práce se musí vyrovnat při své činnosti i ÚOOÚ. V § 316 odst. 2 a 3 NZP zavádí zcela novou právní úpravu v této oblasti, která je podle stanoviska MPSV čj. 2007/55722–52, p. 2, a rovněž na základě interpretace § 193 sq. nálezu ústavního soudu sp. zn. Pl. ÚS 83/06, který byl vyhlášen pod č. 116/2008 Sb.,²⁾ kogentní. To znamená, že se od nich nelze smluvně ani jinak odchýlit a případný souhlas zaměstnanců je právně bezvýznamný a neúčinný, jelikož by se jednalo o právní jednání *in fraudem legis*, tedy směřující k obcházení zákona:

„(2) Zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci.

(3) Jestliže je u zaměstnavatele dán závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele, který odůvodňuje zavedení kontrolních mechanismů podle odstavce 2, je zaměstnavatel povinen přímo informovat zaměstnance o rozsahu kontroly a o způsobech jejího provádění.“

Druhou linií je regulace elektronických komunikací. Čl. 5 směrnice Evropského parlamentu a Rady 2002/58/ES, o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích), regulující důvěrný charakter sdělení, byl implementován § 89 zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů. Toto ustanovení zakazuje odposlech, ukládání zpráv apod. bez souhlasu dotčených uživatelů. Dále je znovu stanovena informační povinnost.

Obecně k problematice

Rozhodnutí Evropského soudu pro lidská práva ve věci *Niemietz v. Německo* ze dne 16. prosince 1992, stížnost č. 13710/88, se v § 29 vyjádřilo k obsahu pojmu soukromí: „*Respektování soukromého života musí do určité míry zahrnovat právo na vytváření a rozvíjení vztahů s dalšími lidskými bytostmi.*“⁽³⁾ V rámci svých pracovních aktivit má totiž většina lidí největší příležitost navazovat a rozvíjet vztahy s vnějším okolím, a proto právo na respektování soukromého života zahrnuje i právo na respektování soukromí v zaměstnání, neboť z tohoto rozhodnutí vyplývá, že v rámci pracoviště existuje ve vztahu k zaměstnanci značná míra soukromí, se kterou je nutné počítat a kterou je třeba chránit.

Týž soud se v rozsudku ve věci *Coplandová v. Spojené království* ze dne 3. dubna 2007, stížnost č. 62617/00, v §§ 41 a 44 vyslovil k otázce soukromí na pracovišti: „Na telefonní hovory z firemních prostor se podle předchozí judikatury soudu zcela jasně vztahují pojmy „soukromý život“ a „korespondence“ uvedené v čl. 8 odst. 1 [evropské Úmluvy o ochraně lidských práv a základních svobod, CETS 005, vyhlášené pod č. 209/1992 Sb.]... Z toho logicky vyplývá, že obdobně e-maily odesílané z práce by měly spadat pod ochranu podle čl. 8 stejně jako informace pocházející ze sledování osobního užívání internetu... Soud se domnívá, že shromažďování a uchovávání osobních informací bez vědomí stěžovatelky souvisejících s jejím telefonováním a používáním e-mailu a internetu, znamenalo narušení jejího práva na respektování soukromého života a korespondence podle čl. 8.“⁽⁴⁾

Na základě čl. 29 směrnice 95/46/ES Evropského parlamentu a Rady, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, byla zřízena v rámci Evropské komise Pracovní skupina 29 („WP29“). WP29 má poradní a nezávislý status a vydává stanoviska s výkladem směrnice 95/46/ES, aby byla zajištěna jednotná aplikace národních předpisů o ochraně osobních údajů. Takovým stanoviskem k dané věci bylo WP 48 – stanovisko č. 8/2001, o zpracování osobních údajů v kontextu zaměstnání, ze dne 13. září 2001.

Pracovní poměr má vyživovací (alimentační) charakter, zaměstnanec je na něj zpravidla odkázán svým živobytím, a proto ho právo zvýšenou měrou reguluje, zhusta ve prospěch zaměstnance. Pravidlem je úzký osobní vztah mezi zaměstnancem a jeho nadřízeným, byť ten může být v některých specifických případech oslaben, např. u zaměstnanců pracujících doma nebo podomních prodejců. I ti sice vykonávají pro zaměstnavatele nesamostatnou práci, avšak nemusejí a nebývají se zaměstnavatelem v bližším kontaktu, vyjma e-mailu nebo telefonu, a vzájemně se s ním téměř neznají. Je-li důvěra mimoprávně poškozena, právo obvykle není schopno tento nežádoucí stav zhojit. Snaha míru nedů-

věry zaměstnavatele k zaměstnanci objektivizovat prostřednictvím monitoringu nemůže vést k úspěchu.

První vůdčí zásadou proto je **zásada proporcionality**, tedy, že na základě principu poměrnosti/úměrnosti (proportionality) musejí být oprávnění zaměstnance v rovnováze s legitimními oprávněními a zájmy zaměstnavatele, což vychází z rozložení oprávnění a povinností zaměstnance a zaměstnavatele v rámci pracovněprávního vztahu. Zaměstnanec očekává, že také v pracovním právu bude přiměřeně zachováno jeho právo na soukromí, jehož součástí je i právo na ochranu jeho osobních údajů, a že tato práva bude zaměstnavatel respektovat. Oprávněním zaměstnavatele je vyžadovat efektivní práci zaměstnance a chránit své aktivity před nebezpečími jako je trestná činnost či škoda způsobená zaměstnancem. Zaměstnavatel je oprávněn požadovat, aby zaměstnanec své soukromé záležitosti v pracovní době a na pracovišti vyřizoval pouze v přiměřené a nezbytné míře.

Při zkoumání oprávnění zaměstnavatele je třeba vycházet z § 316 odst. 1 NZP, který zaměstnancům zakazuje používat výrobní a pracovní prostředky zaměstnavatele pro svou osobní potřebu bez jeho souhlasu, včetně implicitního. Dodržování tohoto zákazu je zaměstnavatel oprávněn přiměřeným způsobem dozorovat. Dozorem se však nerozumí monitoring, zejména obsahu zasílaných zpráv či hovorů, který je přípustný pouze výjimečně, za níže stanovených podmínek.

Druhou vůdčí zásadou při hledání souladu práv a povinností zaměstnanců a zaměstnavatelů je **zásada přiměřenosti** (adekvátnosti), již je třeba aplikovat jako co nejmenší počet shromažďovaných osobních údajů výlučně kategorií odpovídajících účelu, ke kterému zaměstnavatel osobní údaje zpracovává.

Třetím principem je **zásada analogie**. Nové informační technologie je vhodné připodobnit starým technologiím (např. poště) a právní normy je regulující používat obdobně. Zaměstnavatelé jsou povinni respektovat lidská práva zaměstnanců, včetně ochrany jejich listovního tajemství a důvěrnosti nebo tajemství dopravovaných zpráv.

Čtvrtým principem je **informační povinnost** zaměstnavatele podle § 11 zákona o ochraně osobních údajů a §§ 30 a 31 NZP. Informační povinnost správce v rámci pracoviště má dvě roviny. První představují zaměstnanci a ty subjekty, které jsou správci předem známy, že budou pravidelně do monitorovaných prostor docházet. Vůči těmto je třeba splnit informační povinnost v plném rozsahu a předem.

Podle § 31 vůči zaměstnancům je třeba informační povinnost splnit ještě před vznikem pracovněprávního poměru. Vhodným prostředkem pro informaci o všech opatřeních, která zasahují do soukromí zaměstnance, je pracovní řád. Podle § 37 odst. 5 NZP ve spojení s § 11 zákona o ochraně osobních údajů vyplývá, že zaměstnavatel má povinnost seznámit zaměstnance s tímto vnitřním předpisem a splnit

tak svou informační povinnost, jestliže ji hodlá plnit jeho prostřednictvím, opět nejpozději při nástupu do práce, jestliže nebylo ze strany zaměstnavatele spojeno informování podle § 31 NZP a § 37 odst. 5 NZP v jedno.

Pro vymezení působnosti stanoviska je klíčový institut **pracoviště**. Pojem „pracoviště“ není v právním řádu definován. Je používán v různých významech – v širokém a úzkém. V širokém pojetí, které vychází z § 2 odst. 3 zákona 119/1992 Sb., o cestovních náhradách, ve znění pozdějších předpisů, který byl převzat do § 34 odst. 2 nového zákoníku práce, je pracovištěm místo výkonu práce, případně celá obec.⁵⁾ Přitom je však zřejmé, že zaměstnavatel může mít více pracovišť. V úzkém pojetí, které vychází z § 134 zákoníku práce z roku 1965 ve znění I. euronovely č. 155/2000 Sb. a které bylo převzato do § 103 nového zákoníku práce, je pracovištěm pracovní místo. Nejedná se však o funkční zařízení, nýbrž např. o židli a pracovní stůl s bezprostředním pracovním okolím.

a) Listovní tajemství

Listovní tajemství platí pro soukromé zásilky bezvýjimečně i na pracovišti. V prvotním třídění se soukromá zásilka od úřední rozezná podle obálky. Soukromá je primárně adresována zaměstnanci jako soukromé osobě (jméno a příjmení je uvedeno na prvním místě) a název zaměstnavatele slouží toliko jako adresní údaj (je uveden až na dalších místech). Naproti tomu úřední zásilka je primárně adresována instituci (její název je uveden na prvním místě) a na dalších místech je případně uvedeno k urychlení poštovního styku jméno zaměstnance jako úřední osoby.⁶⁾

Je-li uvedena doložka „do rukou X. Y.“ nebo „k rukám X. Y.“, je sporné, jak s takovou zásilkou zacházet. Podle převažujícího názoru se jedná o úřední zásilku, podle menšinového o soukromou. S ohledem na přílohu č. 2 poštovních podmínek základní poštovní služby⁷⁾ se má postupovat podle prvního názoru s tím, že pokud adresát nebo podatelna zjistí, že se ve skutečnosti jedná o soukromou poštu, nechá dokument ze spisové služby vyřadit, resp. ho do ní vůbec nezařazuje.

b) Elektronická pošta

Elektronické dokumenty (např. soubory typu docx, xlsx, pdf či jpeg) jsou podle § 40 občanského zákoníku písemnostmi, byť nejsou listinami. Proto pro ně platí stejná pravidla jako pro ostatní písemnosti.

Ačkoliv e-mailová adresa patří zaměstnavateli, je-li složená z jména a příjmení zaměstnance např. Jan.Svoboda@doména.cz, je e-mail na ni doručený soukromou elektronickou poštou a taková e-mailová adresa je sama o sobě vždy osobním údajem, avšak takovým osobním údajem, k jehož zpracování je zaměstnavatel oprávněn; včetně jeho zveřejnění, komunikuje-li takový zaměstnanec se třetími osobami. Naproti tomu věcně konstruovaná e-mailová adresa, např.

info@doména.cz, je úřední elektronickou adresou, a to i v případě, že ji spravuje pouze jeden zaměstnanec.

Zaměstnavatel **není oprávněn** sledovat, monitorovat a zpracovávat **obsah** korespondence svých zaměstnanců. Zaměstnavatel případně smí u svých zaměstnanců pouze sledovat počet došlých a odeslaných e-mailů, případně (tj. zejména vznikne-li podezření ze zneužití pracovních prostředků, resp. využití k jiným než pracovním účelům) včetně hlavičky, tj. komu píše a od koho je dostávají. Tato činnost je zpracováním osobních údajů zaměstnance, byť za uvedených podmínek oprávněným zpracováním, a je tedy nezbytné dodržovat všechny zákonem o ochraně osobních údajů stanovené povinnosti.

Soukromý e-mail zaměstnance smí zaměstnavatel na základě oprávnění daných mu novým zákoníkem práce otevřít a přečíst pouze výjimečně, v zájmu ochrany svých práv, především jestliže je zřejmé, že se jedná o pracovní e-mail, tj. lze-li tento závěr učinit na základě údajů uvedených v hlavičce, a jestliže je pravděpodobné, že z objektivních důvodů, jako je dlouhodobá nemoc zaměstnance, by k jejímu vyřízení zaměstnancem mohlo dojít natolik pozdě, že by zaměstnavatel mohl utrpět újmu na svých právech. Zaměstnavatel tak fakticky využívá svého práva chránit majetek podle nového zákoníku práce. Při nařizování dovolené by měl zaměstnavatel předem přijmout taková opatření k zastupování, aby k poškození soukromí zaměstnance nedošlo.

c) Webové stránky

Při ochraně soukromí zaměstnance při pohybu na webových stránkách je nutno analogicky vycházet z odstavce 26 preambule směrnice o soukromí a elektronických komunikacích: „údaje o účastnících, které jsou zpracovávány v rámci sítí elektronických komunikací pro navázání spojení a přenos informací, obsahují informace o soukromém životě fyzických osob a dotýkají se práva na ochranu jejich korespondence nebo se dotýkají oprávněných zájmů právnických osob. Takové údaje je možno uchovávat pouze v rozsahu, který je nezbytný pro poskytování služby pro účely účtování a platby za propojení, a to po omezenou dobu. Poskytovatelé služeb by měli účastníky vždy informovat o druhu zpracovávaných údajů, účelech a délce trvání takového zpracování“. Jak již bylo řečeno, v zásadě by měl být uživatel o všech monitorovacích nástrojích předem informován.

Sledovat používání webových stránek zaměstnanci pro účely zaměstnavatele tedy možné není, pokud nejsou splněny zákonem stanovené podmínky, tj. závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele. Pod tím si lze představit například mezinárodní bankovní převody nebo dozor nad prací vězňů.

Ani statistické sledování využívání přístupu k internetu, například doby strávené „surfováním“ po internetu, není v souladu s novým zákoníkem práce, nejsou-li splněny

podmínky stanovené výše. Avšak ničím zde uvedeným nejsou dotčena práva zaměstnavatele postihnout zaměstnance v souladu s pracovněprávními předpisy, jestliže nevyužívá řádně pracovní doby a prostředků, které mu byly zaměstnavatelem svěřeny.

Procesní ustanovení

Ustanovení § 316 odst. 2 a 3 nového zákoníku práce stanoví povinnosti zaměstnavatele, tedy komplementárně též oprávnění zaměstnance. Na základě § 3 odst. 1 písm. a) zákona o inspekci práce jsou ke správnímu dozoru nad ním kompetentní Státní úřad inspekce práce a oblastní inspektoráty práce, přičemž ale není stanoven správní delikt za porušení těchto ustanovení.

Porušením § 316 odst. 2 a 3 nového zákoníku práce může kromě porušení soukromí zaměstnanců dojít též k porušení ochrany osobních údajů zaměstnanců nebo i třetích osob, např. klientů. V tomto případě je kompetentním ke správnímu dozoru též ÚOOÚ.⁸⁾

Závěr

V zásadě platí, že monitorování zaměstnanců je zakázáno, pokud nejsou splněny zvláštní, zákonem stanovené, podmínky. Pokud se zaměstnavatel rozhodne monitorovat zaměstnance, pak musí:

- a) informovat zaměstnance podle § 11 zákona o ochraně osobních údajů a §§ 30 a 31 nového zákoníku práce. V případě monitorování zaměstnanců při používání internetu, je součástí informace vysvětlení principů monitorování jako je například soubor logů apod.;
- b) se všemi zaměstnanci zacházet rovně a
- c) vycházet ze skutečného stavu. Byť zákon umožňuje, aby zaměstnancům byly některé činnosti zaměstnavatelem zakázány, zaměstnavatelem stanovená pravidla by měla odrážet realitu, tj. nezakazovat něco, co je u zaměstnavatele běžnou tolerovanou praxí.

Zároveň by bylo vhodné, aby zaměstnavatelé vydali vnitřní předpis, kde by stanovili jasná pravidla, přičemž platí, že čím má zaměstnavatel více zaměstnanců, tím by pravidla měla být detailnější, protože vztahy na pracovišti jsou

pak anonymnější. Nejlepším řešením je, aby tato pravidla byla součástí pracovního řádu.

Při tom by zaměstnavatelé měli zvážit, zda povolí svým zaměstnancům používání internetu pro soukromé účely, např. během přestávek na jídlo a oddech. Lze doporučit zákaz pouze vytípaných služeb, např. download souborů s mediálním obsahem, chatu a přeposílání řetězových e-mailů.

Poznámka:

- ¹⁾ Cf. rozhodnutí ÚOOÚ ze dne 9. února 2007, zn. SPR-0225/07-9.
- ²⁾ <http://nalus.usoud.cz/Search/ResultDetail.aspx?id=58004>
- ³⁾ <http://cmiskp.echr.coe.int//tkp197/viewhbk.asp?action=open&table=F69A27FD8FB86142BF01C1166DE-A398649&key=468&sessionId=13929620&skin=hudoc-en&attachment=true> (DOC), český překlad: <http://sccp.prf.cuni.cz/judikat/es27-96.htm>
- ⁴⁾ <http://cmiskp.echr.coe.int//tkp197/viewhbk.asp?action=open&table=F69A27FD8FB86142BF01C1166DE-A398649&key=61533&sessionId=17144564&skin=hudoc-en&attachment=true> (DOC)
- ⁵⁾ Eva Dandová: Výklad ustanovení § 134 zák. č. 65/1965 Sb. (zákoníku práce). ASPI: 18818.
- ⁶⁾ Podle čl. 4 odst. 7 rozhodnutí Českého telekomunikačního úřadu čj. 40106/05-608, ve znění rozhodnutí čj. 43575/05-608, čj. 10 610/2006-608, čj. 26 701/2006-608, čj. 31 482/2006-608, čj. 32 763/2006-608, čj. 42 856/2006-608, čj. 56 854/2006-608, čj. 56 855/2006-608, čj. 61 853/2006-608, čj. 2 923/2007-608, čj. 17 088/2007-608, čj. 19 617/2007-608, čj. 33 117/2007-608, čj. 40 328/2007-608, čj. 57 147/2007-608, čj. 63 088/2007-608, čj. 75 263/2007-608 a čj. 82 545/2007-608: „Je-li v poštovní adrese uvedena na prvním místě právnická osoba a na druhém místě fyzická osoba, za adresáta se považuje právnická osoba. Je-li v poštovní adrese uvedeno na prvním místě jméno a příjmení fyzické osoby a na druhém místě označení právnické osoby, za adresáta se považuje fyzická osoba s tím, že poštovní zásilka má být dodána prostřednictvím této právnické osoby. Je-li v poštovní adrese namísto jména a příjmení určité fyzické osoby uvedena pouze její funkce v právnické osobě, za adresáta se považuje právnická osoba.“
- ⁷⁾ <http://www.cpost.cz/data/psc/zps.zip>
- ⁸⁾ Rozhodnutí ÚOOÚ zn. REG-3554/07-8.
- ⁹⁾ Publikované stanovisko je také k dispozici na internetové adrese Úřadu <http://www.uoou.cz> v sekci Názory Úřadu/Stánoviska.

III. SDĚLENÍ ÚŘADU

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ K PROBLÉMŮM Z PRAXE

č. 1/2009

březen 2009

K možnosti rozšíření kompetencí Úřadu ve vztahu k zákonu č. 106/1999 Sb., o svobodném přístupu k informacím

Aplikace principů ochrany soukromí podle zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů měla vždy zásadní význam i pro aplikaci principů práva na přístup k informacím podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, proto se nelze divit minulým ani současným snahám o bližší propojení těchto agend. V následujícím vyjádření je obsaženo několik právních důvodů, proč by k tomu dojít nemělo.

I.

Při posuzování vztahu zákona č. 101/2000 Sb. a zákona č. 106/1999 Sb. byl prosazován vztah jistého přednostního uplatnění i zákona č. 101/2000 Sb., který se odvíjí od ústavního rámce právní úpravy práva na ochranu soukromí, jako základního lidského práva (východiskem je článek 8 Úmluvy o ochraně lidských práv a svobod) byl vyjádřen jak v původním § 2 odst. 3 tak, že **zákon č. 106/1999 Sb. se nevztahoval na poskytování osobních údajů** a informací podle zvláštního právního předpisu, který byl platný až do roku 2007; tak **podle současně platné právní úpravy** § 8a tohoto zákona, podle které „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** (v odkazu k tomuto ustanovení na poznámku pod čarou jsou uvedeny občanský zákoník a §§ 5 a 10 zákona č. 101/2000 Sb.).

Slovní spojení „přednostní uplatnění“ ochrany osobnosti a s tím souvisejících podmínek pro zpracování osobních údajů eventuálně podmínek pro zpřístupňování informací nelze však chápat nějakým dehonestujícím způsobem. V tomto směru oba zákony mají ještě další ustanovení, která tento vztah doplňují a prohlubují.

V zákoně č. 101/2000 Sb. je to například ustanovení § 4 písm. l) definující pojem „**zveřejněný osobní údaj**“ jako osobní údaj zpřístupněný zejména hromadnými sdělovacími prostředky, jiným veřejným sdělením nebo jako součást veřejného seznamu, nebo dále § 5 odst. 3 tohoto zákona, podle něhož: Provádí-li správce zpracování osobních údajů na základě zvláštního zákona, je povinen dbát

práva na ochranu soukromého a osobního života subjektu údajů.

V zákoně č. 106/1999 Sb. lze pak najít ustanovení § 8b, které upravuje podmínky pro povinný subjekt při **poskytování základních osobních údajů** o osobě, které poskytl veřejné prostředky.

II.

Zatímco právo na ochranu soukromí má ryze hmotně právní podstatu v ochraně osobnosti a všech osobnostních práv ve vztahu ke skupině základních lidských práv, právo na přístup k informacím, které je tradičně spíše spojováno s právem na svobodu projevu a informací (východiskem je článek 10 citované Evropské úmluvy), je svou podstatou spíše právem procesním, v některých státech vnímáno dokonce jako právo povahy administrativní neboli právo zajišťující přístup k informacím, které ve své podstatě nejsou osobnostní povahy.

Tím máme na mysli zejména skupinu informací, které jsou vymezeny v § 2 zákona č. 106/1999 Sb. jako:

- informace vztahující se k působnosti povinných osob, kterými jsou státní orgány, územní samosprávné celky a jejich orgány a veřejné instituce;
- informace týkající se rozhodování o právech, právům chráněných zájmech nebo povinnostech fyzických nebo právnických osob v oblasti veřejné správy, a to pouze v rozsahu této jejich rozhodovací činnosti;
- informace, které nejsou předmětem průmyslového vlastnictví;
- informace, pokud zvláštní zákon neupravuje jejich poskytování, zejména vyřízení žádosti včetně náležitostí a způsobu podání žádosti, lhůt, opravných prostředků a způsobu poskytnutí informací;
- informace, které nejsou dotazem na názory, budoucí rozhodnutí a nejde o vytváření nových informací;
- informace vztahující se výlučně k vnitřním pokynům a personálním předpisům povinného subjektu;
- informace, které nejsou předmětem utajení;
- informace, které nejsou předmětem ochrany obchodního tajemství;

Jak je z kontextu základní hmotné právní úpravy obou předpisů patrné, zatímco v případě zpracování osobních údajů a jejich ochrany lze dospět k poznání, zda jde, či nejde o zákonem regulované zpracování poměrně jednoznačně, v případě pestrosti druhů informací, na které lze zákon č. 106/1999 Sb. aplikovat a to jak pozitivně, tak negativně, je sjednocení výkladových a rozhodovacích kompetencí do jediného správního úřadu velmi obtížné, protože se tato oblast dotýká velmi širokého spektra právních předpisů, které jsou hmotně právně v gesci mnoha subjektů.

V případě zpracování osobních údajů se jedná o určitý soubor operací s osobními údaji, který je prováděn po určité době, za konkrétním účelem a stanoveným způsobem, přičemž se dotýká předem neurčitého počtu občanů. Zejména soustavnost neboli nepřetržitost této činnosti představuje zásadní rozdíl oproti poskytnutí informace na základě zákona č. 106/1999 Sb. Ve vztahu k zpracování osobních údajů je konstituování Úřadu pro ochranu osobních údajů (dále jen „ÚOOÚ“), jakožto dozorového orgánu a pravomoci jeho inspektorů způsobem, jakým stát občanům (a to ne jednomu, ale všem, kterých se zpracování týká) zajišťuje a garantuje ochranu základního práva na ochranu soukromí a osobních údajů. Naproti tomu je poskytování informací činností jednorázovou, vyvolanou zájmem konkrétní osoby k naplnění jejího politického práva. Je proto rozhodováno o této konkrétní žádosti, přičemž současná právní úprava poskytuje dostatečné prostředky pro ochranu a domožení se svého práva.

Zákon č. 106/1999 Sb. je *a priori* nastaven na potřebu široké dostupnosti informací, ale dalším nakládáním s informacemi se věnuje jako pouze jednomu dílčímu postupu, a to zpřístupnění. Oproti tomu zákon o ochraně osobních údajů reguluje celý proces zpracování osobních údajů (od shromažďování do likvidace), a přitom s přihlédnutím k zásadám účelného zpracování údajů stanoví zvláštní podmínky, kdy lze vybrané osobní údaje zveřejnit.

III.

V očekávání možného vývoje je třeba si tedy ujasnit a vyjádřit základní přístupy:

1. V případě srovnání obou právních předpisů z hlediska hmotného i procesního zde hovoříme o nakládání se dvěma často značně nesourodými skupinami údajů (informace a osobní údaje). Na rozdíl od přístupu k informacím je přístup k osobním údajům často podrobován nesrovnatelně přísnějším kritériím, např. již před zpřístupněním či zveřejněním údajů je třeba zohlednit, jak budou osobní údaje po zpřístupnění uchovávány a využívány a komu budou dále předávány. (Zde ochrana osobních údajů vychází z premisy, že i další nakládání se zveřejněnými údaji musí být účelné a nemůže nepřiměřeně zasáhnout do soukromí dotčených osob.)
2. Jaká by tedy měla být role správního úřadu ve vztahu k zákonu č. 106/1999 Sb.? Pokud by se v této oblasti jednalo o orgán dozorový se všemi pravomocemi, které má ÚOOÚ v oblasti ochrany osobních údajů, k čemu by jejich uplatnění směřovalo? Pokud by mělo být rozhodováno nezávisle o plnění povinnosti dle zákona č. 106/1999 Sb., tedy o ne/poskytnutí vyžádaných informací, byla by tímto dublována činnost odvolacího orgánu dle současných právních předpisů, resp. činnost nezávislých soudů a hrozilo by rozdvojení výkladu zákona jednak soudem a jednak správním úřadem a tedy ještě větší vznik nejistoty. Pokud by byl správní orgán mezistupněm mezi povinným subjektem a soudem, vedlo by to pouze k prodloužení celého procesu, tedy doby, než by se žadatel domohl informace, neboť nelze očekávat, že by povinné subjekty ve větší míře respektovaly a dodržovaly závěry správního úřadu (pokud mnohdy nerespektují ani závěry soudů). V daném případě by nepochybně využívaly možnosti soudního přezkumu závěrů správního úřadu. Za neakceptovatelné lze přitom považovat, aby byl správní úřad poslední instancí v oblasti poskytování informací a jeho rozhodnutí a závěry nebyly dále soudně přezkoumatelné, a to především z níže uvedeného konfliktu ochrany osobních údajů a poskytování informací (nebylo by to akceptováno ani ostatními státními orgány a organizací české veřejné správy je toto naprosto cizí).
3. Spojení obou kompetencí by ve svém důsledku znamenalo, že Úřad a předseda budou rozhodovat jak ve věcech týkajících se ochrany osobních údajů, tak ve věcech týkajících se jejich zpřístupňování podle přísných a konkrétních podmínek zákona č. 101/2000 Sb., ale v kontextu širšího množství informací dle obecných, výkladově často nejasných a až judikaturou sjednocovaných pravidel dle zákona č. 106/1999 Sb. V praxi správních úřadů však působnost vrcholového dozorového orgánu vybaveného procesně náležitými kompetencemi, ale s dopadem pro dvě tak odlišné oblasti, rozhodně není standardem. Podíváme-li se na ty evropské úřady pro ochranu osobních údajů, které současně vykonávají působnost i pro oblast práva na informace, pak jde buď o úřady federální, kdy výkon dozorových kompetencí je vykonáván na úrovni územní (Německo), nebo jde o orgány, které nemají srovnatelné správní kompetence jako je tomu v případě České republiky (Slovinsko, Velká Británie). Přijetím tohoto záměru by tak mohlo vést k paradoxu, kdy by byl vyvíjen tlak na změnu dosavadních postupů a přístupů Úřadu pro ochranu osobních údajů a snahy omezit dosavadní působnost tohoto úřadu, což je nepřijatelný kompromis.
4. Jak rozhodovat spravedlivě? Domníváme se, že právě zásada spravedlivého procesu by byla jednou z těch, které by v tomto ohledu nebylo možné zcela dodržet, a Úřad, respektive jeho předseda, by byl terčem kritiky,

že straní jednomu právu na úkor práva druhého. Prakticky by ve stejné kauze současně rozhodoval jak o podnětu dotčených osob (subjektů údajů) podle § 21 zákona č. 101/2000 Sb., tak o nárocích neuspokojených žadatelů o informace podle zákona č. 106/1999 Sb. V důsledku střetu těchto dvou kompetencí by tak mohlo dojít i k rozdílnému přístupu inspektora pro ochranu dat při posuzování podnětu subjektu údajů, který se bude cítit poškozen zpřístupněním informací o své osobě, které bylo povinným subjektem realizováno na základě doporučení informačního inspektora téhož úřadu.

5. V dnešním technickém světě informační společnosti je trend informace sdílet či předávat. Jak tento trend sílí, ochrana soukromí nabývá na významu a je vždy chápána jako omezující pravidlo zpřístupňování informací, jako zásadní výjimka z obecně požadované dostupnosti informací. Regulace takto nově nahlížené ochrany soukromí je dána jasně vymezenými pravidly. Není zřejmé, proč za přesně odlišené hmotněprávní úpravy je třeba uvažovat o spojení na úrovni procesní, resp. institucionální (ÚOOÚ jako informační úřad).

Silné dozorové kompetence ÚOOÚ, odpovídající mj. požadavkům evropského práva, vyplývají z jasně deklarovaného zájmu chránit a vynucovat zákonné zpracování osobních údajů. Je otázkou, zda i široká oblast zpřístupňování informací má být obdobně přísně regulována a zda by ve spojení se soudním přezkumem nebyly pro tuto agendu dostačující např. kompetence odpovídající postupům Veřejnému ochránci práv.

Závěr

Z hlediska hmotně právního je problematika zákona č. 106/1999 Sb. podstatně širší, vyžaduje posuzování velmi širokého spektra problematiky, jako jsou záležitosti obchodního tajemství, utajovaných informací apod. Jediným styčným bodem je problematika ochrany osobních údajů resp. soukromí, nicméně i zde je třeba poukázat na jeden základní rozdíl: Zatímco úkolem zákona č. 101/2000 Sb. je primárně data chránit, primárním úkolem zákona č. 106/1999 Sb. je umožnit zpřístupnění dat.

Z hlediska procesního je možno poukázat na fakt, že zatímco zákon č. 101/2000 Sb. je založen na výkonu dozoru, zákon č. 106/1999 Sb. by evidentně vyžadoval individuální řešení případů, tj. řešení na základě sporu.

Je tak možno shrnout, že **obě problematiky vykazují podstatně více diferencí, a to dosti zásadních**, než styčných bodů. S ohledem na stávající zkušenosti s aplikací zákona č. 106/1999 Sb. a bohatou judikaturu by podle názoru ÚOOÚ bylo zcela nevhodné měnit současný proces pro podávání žádostí o informace a jejich navazující soudní přezkum.

Úřad se domnívá, že právě z výše uvedených důvodů byla tato problematika až dosud oddělena, a podle našeho uvážení by tak mělo být i nadále.

Poznámka: Materiál je také k dispozici na internetové adrese Úřadu <http://www.uoou.cz> v sekci Názory Úřadu/K problémům z praxe.

Komentář ke Stanovisku č. 3/2008 Pracovní skupiny pro ochranu dat podle článku 29 (WP29) k návrhu Mezinárodního standardu pro ochranu soukromí v rámci Světového antidopingového kodexu

Viz text na str. 3005

Jak je patrné z textu stanoviska, na řadu podstatných problémů se pouze poukazuje, aniž by pracovní skupina došla k jednoznačnému závěru. Důvodem je skutečnost, že stanovisko je zpracované v příliš krátkém termínu „na zakázku“ Evropské komise, která chtěla být informována před přijetím Standardu agenturou WADA.

Pracovní skupina postrádala celou řadu informací o po-

stupech a mechanismech spojených se shromažďováním, následným zpracováním a využíváním údajů sportovců antidopingovými organizacemi a následně centrální databází ADAMS nezbytných k řádnému posouzení adekvátnosti a legitimitě při nakládání s osobními údaji.

Předpokládá se proto, že pracovní skupina se k záležitosti ještě vrátí, a definitivní stanovisko zformuluje zhruba v květnu 2009.

ČLÁNEK 29 Pracovní skupina pro ochranu osobních údajů



00345/07/CS
WP 132
00345-01/07/CS
WP 151

**Stanovisko č. 2/2007 k informování cestujících
o předávání údajů jmenné evidence cestujících (PNR) orgánům Spojených států**

**přijaté dne 15. února 2007
a
revidované a aktualizované dne 24. června 2008**

Tato pracovní skupina byla zřízena na základě ustanovení článku 29 směrnice 95/46/ES. Skupina představuje nezávislý evropský poradní orgán pro ochranu osobních údajů a soukromí. Její úkoly jsou popsány v článku 30 směrnice 95/46/ES a v článku 15 směrnice 2002/58/ES.

Sekretariát zajišťuje ředitelství C (Občanskoprávní soudnictví, práva a občanství) Evropské komise, Generální ředitelství pro spravedlnost, svobodu a bezpečnost, B-1049 Brusel, Belgie, kancelář LX-46 06/80.

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

Shrnutí

Toto stanovisko a jeho přílohy (často kladené otázky a vzorová sdělení) jsou určeny cestovním kancelářím, leteckým společnostem a dalším organizacím poskytujícím přepravní služby cestujícím leteckých spojů do USA a z USA. Toto stanovisko a jeho přílohy aktualizují a nahrazují předchozí stanovisko ze dne 30. září 2004 (WP97).

Současný právní rámec pro předávání informací PNR orgánům USA vychází z dohody z července 2007.

Cestovní kanceláře, letecké společnosti a další organizace mají i nadále povinnost informovat cestující o zpracovávání jejich osobních údajů a toto stanovisko má za cíl vyjasnit, kdo, kdy a jakým způsobem je povinen jim tyto informace podávat.

Informace mají být podány cestujícím v okamžiku souhlasu s koupí letenky a jejího potvrzení.

V tomto stanovisku pracovní skupina radí, jakým způsobem mají být tyto informace sdělovány telefonicky, osobně a prostřednictvím internetu.

Pracovní skupina zřízená podle článku 29 vytvořila vzorová informační sdělení (přílohy k tomuto stanovisku), aby organizacím sdělování těchto informací usnadnila a aby zajistila, že budou dané informace podávány jednotným způsobem v celé Evropské unii.

Stručné a velmi stručné informační sdělení podávají cestujícím souhrnnou informaci o předávání jejich údajů orgánům USA a poučí je, jak a kde naleznou další informace.

Delší verze sdělení má podobu často kladených otázek a nabízí více podrobností o postupu předávání a zpracování informací. Podrobněji osvětluje pojem „osobní údaje cestujících“ a poté se zaměřuje na údaje PNR. Kromě toho obsahuje hypertextové odkazy na stávající dohodu a další relevantní dokumenty.

Stanovisko č. 2/2007 k informování cestujících o předávání údajů jmenné evidence cestujících (PNR) orgánům Spojených států

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

zřízená směrnicí Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995¹,

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

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

přijala toto stanovisko:

Úvod

Po útocích ze dne 11. září 2001 přijaly Spojené státy řadu zákonů a nařízení, které požadují, aby letecké společnosti nabízející lety na jejich území předávaly orgánům veřejné správy USA osobní údaje o cestujících a členech posádek letadel směřujících do Spojených států, vypravených ze Spojených států nebo přelétávajících území USA. Orgány USA uložily leteckým společnostem zejména povinnost poskytovat Ministerstvu vnitřní bezpečnosti Spojených států (Department of Homeland Security – DHS) elektronický přístup k osobním údajům cestujících obsaženým ve jmenné evidenci cestujících (PNR) ohledně letů do USA a z USA, jakož i přeletů území Spojených států. Leteckým společnostem, které těmto žádostem nevyhoví, hrozí vysoké pokuty a mohou dokonce ztratit práva k přistávání na území USA, případně může docházet ke zdržením při odbavování jejich cestujících po příletu do Spojených států.

Evropský právní rámec umožňující leteckým společnostem předávat PNR cestujících byl vytvořen rozhodnutím Evropské komise ze dne 14. května 2004 a byl doplněn mezinárodní dohodou uzavřenou dne 28. května 2004 mezi Evropskou unií a Spojenými státy americkými. Po zrušení těchto dvou nástrojů Evropským soudním dvorem v roce 2006 byl uvedený rámec nahrazen nejprve prozatímní dohodou mezi Evropskou unií a Spojenými státy americkými ze dne 16. října 2006 a poté navazující dohodou podepsanou Evropskou unií dne 23. července 2007 a Spojenými státy dne 26. července 2007².

Účelem mezinárodní dohody není derogovat nebo novelizovat zákonné předpisy Evropské unie či jejích členských států. Zejména články 10 a 11 směrnice ukládají členským státům povinnost zajistit, aby správce údajů informoval subjekty, jichž se dané údaje týkají, o zamýšleném zpracování údajů. Povinnost správce informovat subjekty

¹ Úř. věst. L 281, 23.11.1995, s. 31, k nahlédnutí na této internetové adrese: http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm.

² Do všech dokumentů lze nahlédnout na internetové adrese: http://ec.europa.eu/justice_home/fsj/privacy/lawreport/index_en.htm

údajů je tudíž stanovena vnitrostátními předpisy, jež byly přijaty na základě uvedené směrnice. Pracovní skupina si je vědoma, že povinnost informovat subjekty údajů mají správci údajů a že tato povinnost musí být splněna v souladu s vnitrostátním právem státu, jímž se tyto správci řídí.

Jelikož se žádosti USA o předávání údajů PNR dotýkají obdobným způsobem všech leteckých společností, má pracovní skupina za to, že existuje skutečná potřeba sladění postupu ohledně obsahu informací, jež mají být podávány cestujícím, i času a způsobu předávání těchto informací. Za tímto účelem se pracovní skupina ve svém stanovisku ze dne 30. září 2004 (WP 97) shodla na formátu standardních informačních oznámení, která mají sloužit jako vodítko ohledně informací, jež mají být podávány cestujícím leteckých spojů mezi EU a USA.

Pracovní skupina se domnívá, že je nyní žádoucí opět projednat záležitost informací podávaných cestujícím, a to ze dvou důvodů. Za prvé je nutné aktualizovat formát sdělení cestujícím z roku 2004 tak, aby odpovídal změnám, k nimž došlo od jeho vytvoření. Za druhé letecké společnosti, cestovní kanceláře a počítačové rezervační systémy dosud neinformují jednotným a uspokojivým způsobem cestující transatlantických leteckých spojů o shromažďování a předávání jejich PNR. K řešení situace pracovní skupina ve svém stanovisku nabízí rovněž vodítko ohledně způsobu, jímž mají být tyto informace podávány.

KDO BY MĚL TYTO INFORMACE PODÁVAT?

Podle směrnice má informační povinnost správce údajů. V případě PNR se může jednat o jednu nebo několik leteckých společností. Povinnost informovat cestující mají rovněž cestovní kanceláře a počítačové rezervační systémy; to je blíže osvětleno v dalším textu.

Letecké společnosti

Údaje o cestujících jsou shromažďovány a zpracovávány proto, aby mohly letecké společnosti dostát své povinnosti dopravit cestující na místo určení. Letecká společnost určuje, proč a jak jsou osobní údaje zpracovávány a v tomto smyslu je správcem údajů. Pracovní skupina proto zastává názor, že informace mají být podávány především leteckou společností prodávající letenku.

Zvláštní případ nastane, jestliže se na sdíleném kódu podílí několik leteckých společností; je-li letenka zakoupena u jedné společnosti, ale let na dané lince ve skutečnosti provozuje společnost jiná. V uvedeném případě má pracovní skupina za to, že z hlediska ochrany údajů lze leteckou společnost, která provedla rezervaci a prodala letenku, považovat za subjekt, který určuje, proč a jak jsou dané údaje zpracovávány. Tato společnost by měla být považována za správce údajů, a mít tudíž povinnost informovat cestujícího.

Cestovní kanceláře

Podle obchodního práva členských států neplatí ve všech případech domněnka, že cestovní kanceláře vystupují jako zástupci evropských leteckých společností, ale spíše jsou považovány za zprostředkovatele mezi cestujícím a leteckou společností. Tato zprostředkovatelská činnost však v každém případě vyžaduje, aby byly cestujícím podány přesné, jasné a úplné informace o smluvních podmínkách. To zahrnuje informace o zpracovávání údajů o cestujících orgány Spojených států. Za účelem uplatnění právních pravidel o ochraně osobních údajů by měl správce údajů tyto informace poskytnout před

koupí letenky. V případě, že je letenka zakoupena od cestovní kanceláře, má povinnost informovat cestující tato kancelář, neboť jedná jménem letecké společnosti, a musí tudíž zajistit, aby letecká společnost splnila svou povinnost. Pracovní skupina má tedy za to, že by informace měly být podávány cestovní kanceláří v případech, kdy byla letenka zakoupena jejím prostřednictvím.

Počítačové rezervační systémy

V zásadě není možné, aby si cestující rezervoval letenku přímo prostřednictvím počítačových rezervačních systémů (Computer Reservation Systems – CRS), například systému Amadeus. Pokud se tak však stane, logický postup vyložený výše se v souvislosti s povinností cestovních kanceláří uplatní i v případě počítačových rezervačních systémů. Měla by se tudíž na ně vztahovat povinnost informovat cestující, kteří si rezervují letenku jejich prostřednictvím, o shromažďování a předávání údajů PNR.

V JAKÉM OKAMŽIKU BY MĚLY BÝT INFORMACE PODÁVÁNY?

Pracovní skupina se domnívá, že informace by měly být cestujícím podány nejpozději k okamžiku, kdy projeví souhlas s koupí letenky.

To je v souladu s obecnou zásadou vytyčenou v článku 6 směrnice, podle níž je údaje nutno zpracovávat řádně a v souladu s právem. Na tento požadavek řádnosti a zákonnosti se odvolávají články 10 a 11 hovořící o informaci nezbytné „pro zajištění řádného zpracování údajů vůči subjektu údajů s ohledem na zvláštní okolnosti, za kterých jsou údaje [shromažďovány nebo zpracovávány].“

Třebaže se předávání údajů PNR v praxi stalo podmínkou pro vycestování do Spojených států, cestující znají význam tohoto předávání pouze v souvislosti se zpracováním jejich osobních údajů, a to jen v případě, je-li jim tato informace podána před zakoupením letenky. Skutečnost, že tyto údaje budou předány orgánům USA, použity, zpřístupněny za jiným než původním účelem a uchovávány po dlouhou dobu, je relevantním prvkem smlouvy o letecké přepravě, zejména proto, že v jejím důsledku dochází k zásahu do základního práva cestujících na soukromí. Předchozí upozornění cestujících na tuto skutečnost před uzavřením smlouvy vychází rovněž z obecné zásady dobré víry při uzavírání smlouvy.

Navíc by tyto informace měly být podány i po koupi letenky, například tak, že budou obsaženy ve zprávě o potvrzení rezervace letu nebo na letáku přiloženém k vydané letence. To je nutné, aby se zajistilo, že cestující obdrží tyto informace v případech, kdy byla rezervace provedena třetí osobou jejich jménem (například sekretářem/sekretářkou).

JAKÉ INFORMACE BY MĚLY BÝT PODÁVÁNY?

Podávané informace by měly v souladu s články 10 a 11 směrnice obsahovat totožnost správce údajů, důvod zpracovávání a jakékoli další údaje „[...] v míře, v jaké jsou tyto doplňující informace nezbytné pro zajištění řádného zpracování údajů vůči subjektu údajů s ohledem na zvláštní okolnosti, za jakých jsou údaje shromažďovány“.

Za určení obsahu informací odpovídají, stejně jako za splnění informační povinnosti, především letecké společnosti jakožto správci údajů, aniž by tím byla dotčena vnitrostátní právní úprava, která provádí články 10 a 11 směrnice, jakož i pravomoci svěřené orgánům dozoru nad ochranou údajů k doladění podmínek informační povinnosti.

Pro sjednocení přístupu na celoevropské bázi však pracovní skupina vypracovala vzorová informační sdělení cestujícím obsažená v přílohách k tomuto stanovisku³. Tato sdělení představují vodítko pro letecké společnosti ohledně informací, které mají podávat cestujícím v souladu s povinnostmi uloženými vnitrostátními právními předpisy provádějícími uvedenou směrnici.

Informační sdělení cestujícím jsou k dispozici ve třech verzích.

Úkolem stručné verze (příloha 1) je informovat cestující o skutečnosti, že jsou údaje předávány orgánům USA, a nabídnout jim možnost dozvědět se více o podmínkách zpracovávání těchto údajů.

Delší verze (příloha 2) má podobu často kladených otázek (FAQ) a obsahuje více podrobností o podmínkách zpracovávání. Tato verze by mohla být používána v případech, kdy jsou rezervace prováděny prostřednictvím internetu nebo v kanceláři (přímo u letecké společnosti nebo v cestovní kanceláři). Pro případ, že se cestující chtějí dozvědět více o předávání svých osobních údajů orgánům USA, obsahuje toto sdělení hypertextový odkaz na mezinárodní dohodu. Obsahuje rovněž radu spojit se s leteckou společností k získání obecnějších informací o tom, jak je s jejich osobními údaji nakládáno.

Velmi stručná verze (příloha 3) má sloužit telefonickému prodeji a lze ji vytisknout přímo na letenku.

Obsah těchto sdělení byl stanoven na základě informací, které pracovní skupině a Evropské komisi poskytly orgány USA, a vychází zejména z dohody mezi EU a USA uzavřené v červenci 2007. Cílem sdělení je tudíž podat co nejpřesnější a nejucelenější přehled zpracovávání údajů PNR orgány Spojených států. Může ovšem vyvstat nutnost tato sdělení následně aktualizovat na základě změny informací poskytnutých orgány USA pracovní skupině a Evropské komisi o způsobu, jímž tyto orgány PNR zpracovávají. Existence těchto vzorových sdělení nezbavuje leteckou společnost povinnosti poskytnout cestujícím přesnější a úplnější informace, pokud takové informace mají.

JAKÝM ZPŮSOBEM BY MĚLY BÝT INFORMACE PODÁVÁNY?

Rozhodnutí o tom, jakým způsobem se informace podávají, činí subjekty, které mají informační povinnost, čili letecké společnosti a cestovní kanceláře. V každém případě musí být informace podány tak, aby si byli cestující plně vědomi skutečnosti, že jsou jejich údaje PNR shromažďovány a dále předávány.

Pracovní skupina předkládá tyto pokyny s cílem napomoci plnění požadavků vnitrostátních právních předpisů.

³ Revidováno a aktualizováno dne 24. června 2008.

Je-li rezervace provedena v cestovní kanceláři

Cestovní kanceláře by měly cestujícím poskytnout v tištěné podobě přinejmenším stručné informační sdělení. Pokud si cestující vyžádají podrobnější informace o předávání PNR, měly by jim cestovní kanceláře poskytnout výtisk delšího informačního sdělení cestujícím.

Je-li rezervace provedena telefonicky

Cestujícím by měla být přečtena velmi stručná verze informačního sdělení (příloha 3). Pokud si vyžádají podrobnější informace, letecká společnost, cestovní kancelář nebo jiná organizace by jim měly sdělit, na jakých internetových stránkách cestující naleznou delší verzi, nebo jak získat tištěnou podobu této delší verze.

Je-li rezervace provedena prostřednictvím internetu

V tomto případě se nabízí řada možností. Stručné sdělení by mělo být cestujícím prezentováno automaticky, aniž by je museli hledat. To lze provést umístěním tohoto sdělení v záhlaví internetové stránky, jejíž pomocí jsou získávány osobní údaje cestujících, nebo jiným vhodným způsobem, například tak, že se na této stránce otevírají informační okénka. Umístěním tohoto sdělení na stránce, která se otevře pouze tehdy, jestliže cestující provede nějaký volný úkon (například klepnutí na hypertextový odkaz na webové stránce), nebo jeho zařazením do obecného oddílu pojednávajícího o ochraně osobních údajů by požadavky vnitrostátních právních předpisů o ochraně osobních údajů nebyly splněny.

Právní upozornění v delší verzi si cestující může naopak vyvolat určitým úkonem, například klepnutím na hypertextový odkaz. Tento hypertextový odkaz by měl být obsažen ve stručném sdělení. Konečně by na internetové stránce mělo být právní upozornění umístěno tak, aby bylo viditelné i dostupné zcela stejně jako obecné přepravní a prodejní podmínky.

V souladu s ustanoveními čl. 30 odst. 1 písm. a) směrnice a s cílem přispět k jednotnému uplatňování vnitrostátních předpisů o ochraně osobních údajů přijatých k provedení směrnice budou vnitrostátní orgány dozoru nad ochranou údajů užívání těchto sdělení cestujícím podporovat. Budou rovněž dohlížet na to, aby letecké společnosti, cestovní kanceláře a počítačové rezervační systémy dodržovaly svou povinnost informovat cestující transatlantických letů o shromažďování a zpracovávání jejich údajů PNR.

V Bruselu dne 15. února 2007.

*Za pracovní skupinu
předseda
Peter Schaar*

Revidováno a aktualizováno
v Bruselu dne 24. června 2008.

*Za pracovní skupinu
předseda
Alex Türk*

PŘÍLOHA I⁴**Stručné informační sdělení pro cestující spojů mezi Evropskou unií a Spojenými státy americkými**

V souladu s mezinárodní dohodou uzavřenou mezi Evropskou unií a Spojenými státy americkými předává/předávají [název letecké společnosti] Ministerstvu vnitřní bezpečnosti Spojených států (Department of Homeland Security – DHS) určité osobní údaje cestujících spojů mezi Evropskou unií a Spojenými státy obsažené ve jmenné evidenci cestujících (PNR).

Orgány USA využívají tyto údaje pro účely předcházení a potírání terorismu a jiných závažných trestných činů nadnárodní povahy. Tyto a jiné údaje mohou být použity též k porovnání se seznamy cestujících, kteří zavdávají příčinu k obavám ohledně bezpečnosti leteckého provozu.

Tyto údaje budou uchovávány po dobu patnácti let a mohou být předávány dalším orgánům. Údaje vztahující se ke konkrétnímu případu nebo vyšetřování lze uchovávat déle, dokud případ nebo vyšetřování nejsou zarchivovány.

Více informací můžete na požádání získat u své letecké společnosti či cestovní kanceláře *[letecká společnost nebo cestovní kancelář pak může poskytnout informace obsažené v delší verzi]*, nebo můžete nahlédnout do často kladených otázek (FAQ) přijatých pracovní skupinou zřízenou podle článku 29 v jejím stanovisku č. 132 (příloha 2) [hypertextový odkaz na stanovisko pracovní skupiny č. 132].

PŘÍLOHA 2⁵

Často kladené otázky týkající se předávání osobních údajů cestujících leteckých spojů mezi Evropskou unií a Spojenými státy americkými orgánům Spojených států

1. Jaké osobní údaje cestujících budou orgánům Spojených států předávány?

Zákony Spojených států vyžadují, aby letecké společnosti provozující letecké spoje na území nebo z území Spojených států (USA), nebo spoje, při nichž dochází k tranzitu přes území USA, předávaly Ministerstvu vnitřní bezpečnosti Spojených států (Department of Homeland Security – DHS) určité osobní údaje cestujících s cílem zvýšit bezpečnost letecké dopravy i bezpečnost Spojených států tím, že budou předem vyhodnocena rizika, jež mohou tito cestující představovat. Osobní údaje cestujících spadají do dvou kategorií:

- Osobní údaje obsažené ve jmenné evidenci cestujících (Passenger Name Record – PNR): tyto údaje obsahují nejrozličnější informace podané při rezervaci letenky nebo uchovávané leteckými společnostmi nebo cestovními kancelářemi, například jméno cestujícího, kontaktní údaje, podrobnosti itineráře (ku příkladu datum letu, výchozí a cílové letiště, číslo sedadla a počet zavazadel) a podrobnosti této rezervace (například název cestovní kanceláře, informace o platbě, objednání jídla nebo rezervace invalidního vozíku), popřípadě další informace (například účast v programu častých letů);
- Systém předběžné kontroly cestujících (Advanced Passenger Information – API): tato část obsahující převážně informace uvedené v cestovním pasu je často získávána při odbavení cestujícího. Tyto informace jsou předávány před příchodem cestujícího k orgánům pohraniční kontroly. Jsou užívány i ke zjišťování, zda se cestující nachází na seznamu osob, jež podle podezření uvedených orgánů představují hrozbu pro bezpečnost leteckého provozu.

Tyto často kladené otázky se týkají především údajů PNR, neboť tento předmět je upraven v souladu s mezinárodní dohodou uzavřenou dne 26. července 2007 mezi Evropskou unií a Spojenými státy americkými. Evropská unie zajistí, aby letečtí dopravci plnili tyto povinnosti. [Název letecké společnosti] musí tyto požadavky splňovat.

Podrobnější výklad způsobu, jakým DHS nakládá s údaji jmenné evidence cestujících (PNR) shromážděnými od cestujících leteckých spojů mezi Evropskou unií a USA, naleznete v mezinárodní dohodě a doprovodném dopise DHS zveřejněných v *Úředním věstníku Evropské unie* L 204 ze dne 4. srpna 2007, k nahlédnutí [zde](http://eur-lex.europa.eu/LexUriServ/site/cs/oj/2007/l_204/l_20420070804cs00180025.pdf).

http://eur-lex.europa.eu/LexUriServ/site/cs/oj/2007/l_204/l_20420070804cs00180025.pdf

2. Proč jsou údaje, které o mně byly zaneseny do jmenné evidence cestujících, předávány Ministerstvu vnitřní bezpečnosti Spojených států před přicestováním do USA nebo vycestováním z USA, popřípadě před tranzitem jejich územím?

DHS používá PNR pro lety mezi Evropskou unií a Spojenými státy pro účely prevence a potírání:

- terorismu a související trestné činnosti;

- jiných závažných trestných činů nadnárodní povahy včetně organizované trestné činnosti a
- pokusů vyhnout se zatčení nebo vzetí do vazby pro podezření ze spáchání výše zmíněných trestných činů.

PNR lze v případě nutnosti využít k ochraně životně důležitých zájmů fyzických osob, nebo v rámci případného trestního řízení nebo v jiných případech stanovených zákonem.

3. Na jakém právním základě jsou údaje PNR předávány?

Podle zákona (oddíl 49, United States Code, odstavec 44909(c)(3)) a jeho (prozatímních) prováděcích předpisů (oddíl 19, Code of Federal Regulations, odstavec 122.49b) musí každý letecký dopravce, který provozuje mezinárodní leteckou přepravu cestujících do Spojených států nebo ze Spojených států, poskytnout DHS údaje PNR v rozsahu, v němž jsou shromažďovány a obsaženy v počítačových rezervačních či odbavovacích systémech leteckých dopravců.

V dopise ze dne 26. července 2007 DHS vysvětluje způsob, jakým údaje PNR shromažďuje, používá a uchovává.

(http://eur-lex.europa.eu/LexUriServ/site/cs/oj/2007/l_204/l_20420070804cs00180025.pdf)

Tyto podmínky se týkají zejména:

- účelu, k němuž se PNR používá;
- sdílení údajů PNR s jinými stranami;
- druhu shromažďovaných informací;
- způsobu, jímž můžete nahlédnout do svých údajů a podat stížnost;
- vymáhání;
- oficiálního oznámení určeného cestující veřejnosti;
- doby uchovávání údajů;
- předávání údajů PNR;
- vzájemnosti a
- přezkumu dohody.

Na základě těchto záruk DHS uzavřely Evropská unie a Spojené státy mezinárodní dohodu podepsanou v červenci 2007 a Evropská unie nyní zajistí, aby letečtí dopravci zpřístupnili údaje PNR, tak jak to DHS vyžaduje.

4. Jsou mezi předávanými údaji PNR obsaženy i citlivé údaje?

PNR mohou v průběhu předávání DHS obsahovat i určité údaje označené jako „citlivé“. Tyto citlivé údaje PNR by mohly obsahovat i určité informace prozrazující rasový či etnický původ cestujícího, jeho politické názory, náboženské vyznání, zdravotní stav či sexuální orientaci. DHS se zaručilo, že nebude používat žádné citlivé údaje PNR, které obdrží, a instalovalo automatický filtrační program, aby se v zásadě použití citlivých údajů PNR zamezilo.

Ve výjimečných případech však lze citlivé údaje PNR použít, např. při ohrožení života či je-li fyzická osoba vystavena vážnému nebezpečí.

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

DHS může údaje PNR sdílet s dalšími vládními orgány USA s působností v oblasti boje proti terorismu, vymáhání práva nebo veřejné bezpečnosti, za účelem prevence a boje proti terorismu a nadnárodní organizované trestné činnosti a dále z důvodu veřejné bezpečnosti (včetně hrozeb, letů, fyzických osob a sledovaných tras).

DHS může sdílet údaje PNR s vládními orgány třetích zemí, avšak pouze po posouzení jejich zamýšleného použití a schopnosti tyto informace chránit. Kromě mimořádných okolností každá výměna údajů vyžaduje, aby byla zahrnuta opatření na ochranu údajů, jež jsou srovnatelná s opatřeními stanovenými v mezinárodní dohodě mezi EU a USA.

6. Jak dlouho bude Ministerstvo vnitřní bezpečnosti Spojených států údaje PNR o mé osobě uchovávat?

DHS uchovává údaje PNR po dobu patnácti let. Údaje vztahující se ke konkrétnímu případu nebo vyšetřování lze uchovávat déle, dokud případ nebo vyšetřování nejsou zarchivovány.

DHS uchovává záznam o přístupu k jakýmkoli citlivým údajům PNR a do 30 dnů po splnění účelu, za nímž byly získány, tyto údaje vymaže, pokud zákon nevyžaduje jejich uchování po delší dobu. DHS oznámí Evropské komisi (DG JLS), zpravidla do 48 hodin, že získalo k citlivým údajům přístup.

7. Mohu si vyžádat opis údajů PNR, které o mně Ministerstvo vnitřní bezpečnosti Spojených států shromáždilo, a mohu požadovat opravu svých údajů v jmenné evidenci cestujících?

Každý cestující bez ohledu na státní příslušnost či zemi pobytu může požadovat informace o svých údajích PNR a požadovat opravu nesprávných údajů.

Informace o politikách DHS týkajících se přístupu k záznamům a osobním údajům naleznete na internetové stránce http://www.dhs.gov/xfoia/editorial_0579.shtm. Více informací Vám poskytne Úřad pro ochranu soukromí DHS, program FOIA (Freedom of Information Act – zákon o svobodném přístupu k informacím):

FOIA
The Privacy Office
U.S. Department of Homeland Security
245 Murray Drive SW
STOP-0550
Washington, DC 20528-0550
Bezplatné tel. číslo: +1-866-431-0486
Tel.: +1-703-235-0790
Fax: +1-703-235-0443
E-mail: foia@dhs.gov

Politiky DHS týkající se nápravy lze nalézt na internetové stránce www.dhs.gov/trip.

Jestliže potřebujete pro podání žádosti jakoukoli pomoc, obraťte se na vnitrostátní orgán pro ochranu údajů. Kontaktní adresu orgánu pro ochranu údajů ve svém členském státě naleznete zde: [odkaz na internetovou stránku Evropa s adresami orgánů pro ochranu údajů: http://ec.europa.eu/justice_home/fsj/privacy/nationalcomm/index_en.htm]

8. Kde mohu získat další informace?

Další informace o tom, jak je nakládáno s Vašimi osobními údaji, můžete získat u své letecké společnosti.

Kontaktní údaje [letecké společnosti ...]:

[...]

PŘÍLOHA 3**Velmi stručné sdělení pro účely telefonického prodeje a pro vytištění na letence**

Platné právní předpisy vyžadují, aby byly Vaše osobní údaje zpřístupněny příslušným orgánům v EU i v jiných zemích. Více informací naleznete na našich internetových stránkách.

PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29



**1576-00-00-08/CS
WP 156**

**Stanovisko 3/2008 k návrhu Mezinárodního standardu pro ochranu soukromí v rámci
Světového antidopingového kodexu**

Přijato dne 1. srpna 2008

Tato pracovní skupina byla zřízena na základě článku 29 směrnice 95/46/ES. Jedná se o nezávislý evropský poradní orgán v oblasti 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 (Občanské soudnictví, občanská práva a občanství) Evropské komise, generální ředitelství pro spravedlnost, svobodu a bezpečnost, B-1049 Brusel, Belgie, č. kanceláře LX-46 06/80.

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

Pracovní skupina pro ochranu fyzických osob v souvislosti se zpracováním osobních údajů

zřízená podle směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995, s ohledem na článek 29 a čl. 30 odst. 1 písm. a) a čl. 30 odst. 3 uvedené směrnice a na čl.15 odst. 3 směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002, s ohledem na článek 255 Smlouvy o ES a na nařízení Evropského parlamentu a Rady č. 1049/2001 ze dne 30. května 2001 o přístupu veřejnosti k dokumentům Evropského parlamentu, Rady a Komise, s ohledem na svůj jednací řád,

přijala tento dokument.

Úvod

Generální ředitelství Evropské komise pro vzdělávání a kulturu (GR EAC) si vyžádalo stanovisko pracovní skupiny zřízené podle článku 29 (dále jen „pracovní skupina“) k návrhu mezinárodního standardu o ochraně soukromí, zpracovaného Světovou antidopingovou agenturou (dále jen „WADA“).

Návrh standardu je třeba číst ve spojení se Světovým antidopingovým kodexem (dále jen „kodex“) WADA, a zejména s článkem 14 tohoto kodexu.

Kodex požaduje, aby sportovci antidopingovým organizacím pravidelně sdělovali konkrétní údaje. Tyto údaje budou následně ukládány spolu s ostatními údaji (včetně citlivých údajů) do databáze s názvem ADAMS, nacházející se v Kanadě.

Podle závazků zamýšlených kodexem se zpracovávají také údaje o doprovodném personálu sportovců – dle definice stanovené kodexem – a o dalších kategoriích osob. Pro účely kodexu zahrnuje pojem „účastník“ sportovce i jejich doprovodný personál.

Část I – Úvod, ustanovení kodexu a definice pojmů

Bod 2 – Ustanovení kodexu

Ačkoli je názor pracovní skupiny spíše než na Světový antidopingový kodex vázán na návrh mezinárodního standardu předložený pracovní skupině dne 7. července 2008, pracovní skupina by ráda zdůraznila (odkazuje-li se v návrhu standardu na ustanovení kodexu), že některá ustanovení kodexu vzbuzují otázky o své slučitelnosti s evropskými normami o ochraně údajů.

Každá osoba účastnící se antidopingových činností má právo na respektování svého soukromí a na ochranu osobních údajů a znění článku 14 kodexu by tak mohlo být upraveno takto: „*Signatáři kodexu souhlasí s principy koordinace nakládání s antidopingovými výsledky, veřejné průhlednosti a odpovědnosti a respektování soukromých zájmů **všech osob, včetně osob obviněných z toho, že porušily antidopingová pravidla.***“

Článek 14.2 - Zveřejnění

Pracovní skupina připomíná, že zveřejňování a sdělování údajů představují způsoby zpracování údajů podléhající režimu ochrany. Pracovní skupina vítá skutečnost, že k zveřejnění rozhodnutí v případě, kdy se sportovec nedopustil porušení antidopingových předpisů, dojde pouze se souhlasem sportovce. Doporučuje však vyjasnění mezinárodního standardu v tom smyslu, aby antidopingovým organizacím bylo zřejmé, že „přiměřená snaha o získání tohoto souhlasu“ nemůže v souvislosti se zveřejněním právoplatně nahradit tento souhlas (viz článek 14.2.3).

Pracovní skupina rovněž zpochybňuje úměrnost zpracování, které spočívá ve zveřejnění rozsudku a dalších informací souvisejících se sportovci nebo jakoukoli jinou „osobou“ na internetu po dobu nejméně jednoho roku (14.2.4 – viz též část II bod 10 níže). V tomto ohledu pracovní skupina navrhuje, aby tyto „osoby“, nejedná-li se o samotné sportovce nebo jejich doprovodný personál, rovněž podléhaly tomuto standardu. V tomto případě neexistuje důvod je vyjímát z privilegia ochrany.

Článek 14.5 (databáze ADAMS)

S výjimkou několika málo řádků v článku 14.4 kodexu se návrhem standardu nijak nestanoví přesná pravidla pro zpracování údajů v souvislosti s databází ADAMS. Návrh standardu je určen pouze pro antidopingové organizace. Ustanovení na ochranu údajů v rámci boje proti dopingům je však nutno zaručit jak pro zpracování údajů prováděné antidopingovými organizacemi, tak pro užívání databáze ADAMS. Pracovní skupina zaznamenává u této databáze působnost kanadských orgánů na ochranu údajů. Nemůže se však spokojit s nízkým počtem odkazů na tuto databázi v textu standardu.

Pracovní skupina proto doporučuje buď úpravu mezinárodního standardu tak, aby se databázi ADAMS věnoval podrobněji, anebo vypracování procesních zásad WADA pro uživatele databáze ADAMS. Pokud jde o přenosy údajů z EU do Kanady, je také třeba upozornit, že by se měla věnovat pozornost provádění těchto přenosů v souladu s předpisy EU o řádném zabezpečení dalšího předávání údajů.

Článek 14.6

Pojem „třetí strana“ není definován.

Obecně by měly být stanoveny konkrétní účely zpracování údajů prováděného podle kodexu. Jediný odkaz na zpracování údajů antidopingovými organizacemi „v souvislosti se svou antidopingovou činností“ nepostačuje.

Bod 3 – Pojmy a definice**Účastník**

Pracovní skupina se domnívá, že pojetí „účastníka“ – ve smyslu definice uvedené v kodexu – je příliš restriktivní na to, aby zaručilo ochranu jakékoli osoby, jejíž údaje lze v rámci provádění kodexu zpracovávat (viz výše uvedené poznámky týkající se pojmů „osoba“ podle článku 14.2.4 a „třetí strany“ podle článku 14.6). Pracovní skupina sice uznává, že poskytovat údaje agentuře WADA budou povinni pouze sportovci a jejich doprovodný personál, jednotné užívání pojmů v mezinárodním standardu a v kodexu by však napomohlo zabránit záměnám.

V článku 3.2 návrhu standardu jsou uvedeny tři nové definice:

Osobní informace

Uvedená definice obsahuje definici „osobních údajů“ z čl. 2 písm. a) směrnice. Pracovní skupina podotýká, že s výjimkou článku 9 (Zachování bezpečnosti osobních informací) neposkytuje návrh standardu v rámci antidopingových činností další záruky ochrany zdravotních a soudních údajů.

Citlivé osobní informace

Osobní informace považované za citlivé odpovídají informacím uvedeným v článku 8 směrnice. Pracovní skupina zde odkazuje na svou připomínku k článku 6 standardu týkající se zpracování těchto údajů (viz níže).

Zpracování

Definice sice doslova neodpovídá definici uvedené v čl. 2 písm. b) směrnice, je však přijatelná.

Část – Standardy pro nakládání s osobními informacemi***Bod 4 – Zpracování osobních informací v souladu s mezinárodním standardem a příslušnými zákony***

Pracovní skupina se domnívá, že pojem „zástupci, kteří jsou třetími stranami“ zahrnuje subdodavatele ve smyslu čl. 2 písm. e) směrnice o ochraně údajů. Z tohoto předpokladu vycházejí další připomínky k tomuto pojmu (viz bod 9). Rozsah tohoto pojmu je třeba přesně vymezit.

Odstavec 4.1

Pracovní skupina se domnívá, že odstavec 4.1 by měl být upraven tak, aby jasně stanovil, že standard jsou povinni dodržovat také zástupci, kteří jsou třetími stranami, i v případě, že se tak děje v rozsahu přesahujícím ustanovení norem platných podle příslušných vnitrostátních právních předpisů.

Návrh standardu nerozlišuje mezi různými skupinami osob, na které se standard vztahuje (sportovci, doprovodný personál, třetí strana). Použití zásady proporcionality však bude záviset na kategorii, do níž daná osoba patří (jaké údaje? jaké uložené údaje?). Proto by měl být návrh standardu v tomto ohledu upraven.

Zpracovávání podstatných a přiměřených osobních informací

Článek 5.3 by měl s přihlédnutím k požadavkům podle zásad nezbytnosti a proporcionality stanovit osobní informace nebo jejich kategorie nezbytné k dosažení účelů uvedených v písmenech a), b) a c). Jak je uvedeno výše, provádění těchto zásad se bude lišit podle kategorie osob, jejichž údaje se budou zpracovávat (sportovec, doprovodný personál).

Článek 5.4 návrhu standardu stanoví, že zpracovávané osobní informace musí být přesné, úplné a aktuální. Zdá se však, že poslední věta tohoto odstavce tuto povinnost zeslabuje vůči antidopingovým organizacím. Zdá se dokonce, že přesouvá odpovědnost ze správce údajů na subjekt údajů¹. Tomuto posunu nasvědčuje také komentář. V tomto ohledu pracovní skupina zdůrazňuje, že podle čl. 6 písm. d) směrnice o ochraně údajů musí být přijata veškerá

¹ „(...) Ačkoli antidopingové organizace nejsou povinny ověřovat přesnost všech jimi zpracovávaných osobních informací, požaduje se, aby co nejdříve opravily či doplnily veškeré osobní informace, o kterých s jistotou vědí, že jsou nesprávné či nepřesné.“

nezbytná opatření, aby nepřesné nebo neúplné údaje s ohledem na účely, pro které byly shromážděny nebo později zpracovány, byly vymazány nebo opraveny. Tuto odpovědnost má v případě potřeby správce údajů na základě žádosti o opravu, předloženou subjekty údajů.

Bod 6 – Zpracování osobních informací se souhlasem

Na základě článku 7 směrnice o ochraně údajů musí veškeré zpracovávání údajů vycházet z platného právního základu. Existence tohoto právního základu má zásadní význam při zpracovávání zdravotních údajů.

Článek 6.1

Článek 6.1 návrhu standardu vyzývá antidopingové organizace, aby k zajištění zákonnosti zpracovávání údajů využívaly souhlas sportovců a členů jejich doprovodného personálu. Pracovní skupina se domnívá, že tento souhlas není v souladu s podmínkami čl. 2 písm. h) směrnice o ochraně údajů. Podle tohoto ustanovení je souhlas definován jako „*jakýkoli svobodný, výslovný a vědomý projev vůle, kterým subjekt údajů dává své svolení k tomu, aby osobní údaje, které se jej týkají, byly předmětem zpracování*“. Souhlas se zpracováním údajů shromažďovaných v souvislosti s plněním závazků podle Světového antidopingového kodexu není svobodný ani informovaný. Z důvodu sankcí spojených s případným odmítnutím účastníků podrobit se závazkům podle kodexu (sdělování údajů o pobytu, lékařské antidopingové kontroly) se pracovní skupina nemůže domnívat, že by byl souhlas jakkoli svobodný². Pracovní skupina má rovněž pochybnosti, zda by souhlas byl informovaný (viz bod níže).

Vzhledem k tomu, že není možné vycházet při zpracování údajů z čl. 7 písm. a) a čl. 8 písm. a) směrnice o ochraně údajů, bude zpracování údajů muset vycházet z jiného přijatelného právního důvodu. Pracovní skupina připomíná, že zpracování údajů související s porušením předpisů není dovoleno ani na základě souhlasu, byť informovaného, subjektu údajů (čl. 8 písm. 2) směrnice o ochraně údajů).

Pracovní skupina proto doporučuje, aby WADA zvážila jiné důvody ke zpracovávání osobních údajů ve smyslu článku 7 a citlivých osobních údajů ve smyslu článku 8 směrnice o ochraně údajů.

Možnými právními důvody pro zpracovávání mohou být různé mezinárodní antidopingové dohody, jako například Mezinárodní úmluva proti dopingu ve sportu nebo Antidopingová úmluva Rady Evropy, pokud tyto úmluvy zakládají závaznou zákonnou povinnost, které – podle čl. 7 písm. c) a čl. 8 písm. 4 směrnice o ochraně údajů na vnitrostátní úrovni – antidopingové organizace jako správci údajů podléhají.

Článek 6.2

Článek 6.2 návrhu standardu umožňuje případné zpracovávání citlivých údajů, například údajů výše uvedených v článku 3.2. Podle směrnice o ochraně údajů jsou součástí citlivých osobních údajů údaje související s rasovým či etnickým původem, politickými názory, náboženským nebo filozofickým přesvědčením, odborovou příslušností nebo sexuálním životem. Pracovní skupina má velmi vážné pochybnosti o relevantnosti zpracovávání těchto kategorií informací, zejména pokud mají být tyto údaje zahrnuty do databáze ADAMS. Proto pracovní skupina vyzývá agenturu WADA, aby poskytla další informace nebo přezkoumala relevantnost případného zpracovávání těchto údajů a aby v článku 6.2 uvedla významné

² Například bod 6.3 návrhu standardu, jímž se stanoví, že „*antidopingové organizace informují účastníky o negativních důsledcích vyplývajících z jejich odmítnutí účastnit se dopingových kontrol, včetně testování*“.

informace, které mají být v tomto rámci zpracovávány. Nadto pak definice v článku 3.2 obsahuje genetickou charakteristiku. Pracovní skupina zpochybňuje oprávněnost a potřebu zpracovávání těchto údajů a žádá agenturu WADA, aby se přesvědčila, zda je toto zpracovávání nezbytné. V každém případě však doporučuje obzvláště vysokou úroveň ochrany při jejich zpracování.

Článek 6.4

Oblast působnosti článku 6.4 by měla být rozšířena tak, aby umožnila právním zástupcům účastníků vykonávat další práva zamýšlená návrhem standardu, jako jsou například práva podrobně uvedená v bodě 11.

Bod 7 – Zajištění odpovídající informovanosti účastníků

Pracovní skupina poukazuje na požadavky článků 10 a 11 směrnice o ochraně údajů, zejména na požadavek poskytnout kromě totožnosti správce údajů také totožnost jakéhokoli jeho zástupce.

Článek 7.2 stanoví, že pokud nejsou osobní informace shromážděny od účastníka, informují se účastníci „co nejdříve“. Pro splnění požadavků směrnice o ochraně údajů (čl. 11 odst. 1) musí být tyto informace sděleny v době provádění záznamu údajů nebo, počítá-li se se sdělením údajů třetí osobě, nejpozději při jejich prvním sdělení. Za výjimečných okolností nemusí být tyto informace poskytnuty, „*ukáže-li se, zejména u zpracování pro účely statistiky nebo historických či vědeckých výzkumů, že informování subjektu údajů není možné nebo by vyžadovalo neúměrné úsilí, nebo pokud právní předpisy výslovně upravují zaznamenávání nebo sdělování údajů*“. Tato omezení je však třeba vykládat restriktivně.

Pracovní skupina dále uvádí, že podle komentáře k článku 7.2 se použitím formulace „*by měl (...) mít přiměřený přístup k informacím...*“ zřejmě oslabuje právo subjektů údajů na informace. Pracovní skupina připomíná, že právo subjektu údajů na informace je zásadní a představuje součást požadavku na průhlednost zpracování údajů.

Bod 8 – Sdělování osobních informací jiným antidopingovým organizacím a třetím stranám

Pracovní skupina zdůrazňuje, že předání z Evropského hospodářského prostoru do třetí země může proběhnout pouze tehdy, zajistí-li tato třetí země odpovídající úroveň ochrany ve smyslu čl. 25 odst. 2 směrnice o ochraně údajů nebo poskytne-li správce dostatečná ochranná opatření pro ochranu soukromí nebo zakládá-li se předání na jedné z výjimek či odchylek, s nimiž počítá čl. 26 odst. 1 směrnice o ochraně údajů.

V tomto případě sídlí databáze ADAMS v Kanadě. Pro účely čl. 25 odst. 2 směrnice o ochraně údajů se Kanada považuje za zemi poskytující odpovídající úroveň ochrany osobních údajů předávaných z Evropského společenství příjemcům podléhajících kanadskému zákonu o ochraně osobních informací a elektronických dokumentech (Personal Information Protection and Electronic Documents Act – PIPEDA)³. Pracovní skupině však není zřejmé, zda se za správce databáze ADAMS považuje WADA nebo národní antidopingový úřad v Kanadě, nebo zda správce podléhá ustanovením zákona PIPEDA. Pracovní skupina doporučuje, aby toto bylo vyjasněno a aby v případě, že by správce databáze ADAMS nepodléhal zákonu

³ 2002/2/ES: Rozhodnutí Komise ze dne 20. prosince 2001 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně osobních údajů, kterou poskytuje kanadský zákon o ochraně osobních informací a elektronických dokumentech (Personal Information Protection and Electronic Documents Act) (oznámeno pod číslem K(2001) 4539).

PIPEDA, byly podniknuty další kroky, které zajistí, aby byla u informací předávaných z Evropského společenství do databáze ADAMS poskytována odpovídající úroveň ochrany.

Pracovní skupina zdůrazňuje potřebu respektovat „zásadu konečnosti“ a požadavek na slučitelnost pokračujícího zpracovávání předávaných údajů s původním účelem, za jakým byly údaje shromážděny.

Zejména u článku 8.4 pracovní skupina opakuje již v bodě 6 uvedené připomínky k platnosti souhlasu. Pracovní skupina dále poukazuje na skutečnost, že toto ustanovení by neumožňovalo zveřejnění osobních informací o sportovcích nebo jiných osobách na internetu, jak předpokládá článek 14.2.4 Antidopingového kodexu (viz bod 2 výše – Ustanovení kodexu).

Bod 9 – Zachování bezpečnosti osobních informací

U bodu 9.1 by měly být kontaktní údaje osoby označené antidopingovou organizací neprodleně sděleny dotyčným osobám (stejně jako informace uvedené v bodě 7.1, a nikoli pouze na jejich žádost).

U subdodavatelů, na které se mohou antidopingové organizace obracet (zástupci, kteří jsou třetími stranami – bod 9.4), pracovní skupina připomíná pravidla stanovená články 16 a 17 směrnice o ochraně údajů, a zejména závazek správce údajů zvolit zpracovatele poskytujícího dostatečné záruky s ohledem na technická bezpečnostní opatření a organizační opatření usměrňující zpracování, jež má být provedeno.

Bod 10 – Uchovávání osobních informací pouze po nezbytně nutnou dobu a zajištění jejich likvidace

Pracovní skupina vítá, že se v této verzi návrhu nachází ustanovení týkající se délky uchovávání údajů a povinnosti tyto údaje vymazat, nejsou-li již s ohledem na účel, pro který byly zpracovány, zapotřebí. Vyzývá však agenturu WADA, aby u těchto údajů – nebo alespoň u některých kategorií údajů – s ohledem na zkušenosti z této oblasti pokud možno určila přiměřenou maximální dobu uchovávání údajů antidopingovými organizacemi. Bod 2 pojednávající o pravidlech zveřejnění uvedených v čl. 14.2.4 Antidopingového kodexu by zde neměl sloužit jako vzor, protože se zdá neúměrný vzhledem ke svému ustanovení, že „minimálně“ osobní informace o sportovcích nebo jiných osobách, kterým se připisuje porušení antidopingových pravidel, by se měly umístit na internetovou stránku antidopingové organizace a „ponechat zde po dobu nejméně jednoho roku.“ (viz část I výše).

Pro porozumění významu „anonymizace / anonymních údajů“ ve smyslu směrnice odkazuje pracovní skupina na své stanovisko 4/2007 o pojetí osobních údajů⁴.

Bod 11 – Práva účastníků s ohledem na osobní informace

Standard počítá s právem přístupu pro sportovce a jejich doprovodný personál. Na základě článku 12 směrnice o ochraně údajů má každá dotčená osoba zejména právo získat od správce údajů informace týkající se alespoň účelů zpracování, kategorií údajů, na které se zpracování vztahuje, a příjemců nebo kategorií příjemců, kterým jsou údaje sdělovány. S těmito prvky návrh standardu nepočítá.

⁴ http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_cs.pdf

Návrh stanoví, že v určitých případech nemají antidopingové organizace povinnost na žádosti o přístup odpovídat. Pracovní skupina v tomto ohledu konstatuje, že u výjimek, které jsou obzvláště neurčitě vyjádřeny v bodech 11.1 (*pokud by toto v konkrétním případě neznamenal střet se schopností antidopingové organizace plnit své závazky podle kodexu*) a 11.2 (*žádosti, které jsou z hlediska svého rozsahu nebo četnosti zjevně svévolné nebo přemrštěné nebo které z hlediska nákladů nebo úsilí znamenají neúměrné zatížení*), se na první pohled zdá, že nejsou v souladu s články 12 a 15 směrnice. Jakékoli omezení práva na přístup je přípustné pouze tehdy, odpovídá-li ustanovením článku 13 směrnice, jímž se členským státům povoluje přijímání legislativních opatření s cílem omezit rozsah této povinnosti, pokud je toto omezení nezbytné pro zajištění zájmů uvedených v rámci daných ustanovení.

Pracovní skupina s uspokojením konstatuje, že v případě zamítnutí výkonu práva účastníků na přístup k údajům obdrží účastníci důvody tohoto zamítnutí písemně. Připomíná však, že toto zamítnutí je přípustné pouze za podmínek článku 13 směrnice, jenž musí být vykládán restriktivně.

K článku 11.4 pracovní skupina zdůrazňuje, že na základě čl. 12 písm. c) směrnice musí správce údajů oznamovat třetí straně, které údaje byly sděleny, veškeré opravy nebo výmazy prováděné z důvodů neúplné nebo nepřesné povahy údajů, pokud se to neukáže jako nemožné nebo to nevyžaduje nepřiměřené úsilí. Pro zajištění shody s evropskou úpravou ochrany údajů by mělo být spojení „*v příslušných případech*“ vykládáno výhradně ve smyslu těchto dvou výjimek.

Doplňující ustanovení

Konečně pak pracovní skupina považuje za politováníhodné, že se v návrhu standardu neobjevuje řada klíčových zásad evropského režimu ochrany údajů. Vyzývá agenturu WADA, aby zvážila vložení určitých doplňujících ustanovení, jejichž smyslem je zaručit:

- Zákaz automatizovaných individuálních rozhodnutí (článek 15 směrnice): vzhledem k sankcím, k nimž může zpracování údajů vést, se tento zákaz jeví jako zásadní.
- Nezávislou kontrolu provádění minimálních ustanovení standardu antidopingovými organizacemi. Článek 8.3 návrhu standardu uvádí, že antidopingová organizace může agentuře WADA sdělit své znepokojení nad možným neplněním standardu jinou organizací. Pracovní skupina se domnívá, že takovýto informační mechanismus vzbuzuje pochybnosti o závazku agentury WADA zabezpečit účinné provádění a dodržování minimálních ustanovení zavedených standardem. Dále konstatuje, že nedodržování norem není spojeno s žádnými sankcemi vůči antidopingovým organizacím. Nakolik účinný tedy tento standard bude?
- Existenci práva na nápravu a práva na náhradu škody vzniklé v důsledku úkonu zpracování neslučitelného se standardem.
- Skutečnost, že národní antidopingové organizace se řídí vnitrostátním právem upravujícím zpracování osobních informací.

Pracovní skupina podporuje iniciativu agentury WADA ve věci přijetí minimálních norem na ochranu soukromí a osobních údajů sportovců a dalších zúčastněných osob v rámci boje proti doping. Pracovní skupina zřízená podle článku 29 se domnívá, že tento standard může, s přihlédnutím ke svému zeměpisnému záběru, sehrát významnou roli v oblasti zpracování údajů, které nepodléhá právním předpisům Evropské unie nebo právním předpisům

považovaným Evropskou unií za odpovídající. Tento standard také může ve všech státech – ať již u nich zpracování údajů podléhá odpovídající ochraně, či nikoli – přispět ke zvýšení informovanosti antidopingových organizací.

Pracovní skupina s potěšením registruje odkaz na směrnici o ochraně údajů uvedený v preambuli tohoto návrhu standardu. Nemůže ho však ještě plně podpořit, protože minimální požadavky v něm obsažené dosud zjevně nedosahují minimálních norem požadovaných evropskou úpravou ochrany údajů. Bude-li přihlédnuto k výše uvedeným připomínkám, může to vést k dalšímu zpřesnění informací o databázi ADAMS. Pracovní skupina proto agenturu WADA vyzývá, aby při zpracování návrhu standardu vzala tyto připomínky v úvahu, uvítá od této agentury další objasnění a souhlasí s případným setkáním s agenturou WADA konaným za tímto účelem.

Pracovní skupina si nicméně přeje být průběžně informována o následném zpracování svých připomínek a obecněji o vývoji práce agentury WADA na tomto návrhu standardu.

V Bruselu dne 1. srpna 2008

*Za pracovní skupinu
předseda
Alex TÜRK*

IV. MATERIÁLY Z ÚŘEDNÍHO VĚSTNÍKU EVROPSKÉ UNIE

III

(Akty přijaté na základě Smlouvy o EU)

AKTY PŘIJATÉ NA ZÁKLADĚ HLAVY VI SMLOUVY O EU

RÁMCOVÉ ROZHODNUTÍ RADY 2008/977/SVV

ze dne 27. listopadu 2008

o ochraně osobních údajů zpracovávaných v rámci policejní a justiční spolupráce v trestních věcech

RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o Evropské unii, a zejména na články 30 a 31 a čl. 34 odst. 2 písm. b) této smlouvy,

s ohledem na návrh Komise,

s ohledem na stanovisko Evropského parlamentu ⁽¹⁾,

vzhledem k těmto důvodům:

a justiční spolupráci v trestních věcech s ohledem na její účinnost i zákonnost a soulad se základními právy, zejména právem na ochranu soukromí a na ochranu osobních údajů. Společné standardy zpracování a ochrany osobních údajů zpracovávaných za účelem předcházení trestné činnosti a boje proti ní přispívají k dosažení obou těchto cílů.

(4) Haagský program: posílení svobody, bezpečnosti a práva v Evropské unii, který Evropská rada přijala dne 4. listopadu 2004, zdůrazňuje nutnost inovativního přístupu k přeshraniční výměně informací důležitých pro vymáhání práva za přísného dodržování klíčových podmínek v oblasti ochrany údajů a vyzývá Komisi, aby do konce roku 2005 předložila v tomto ohledu návrhy. To se odrazilo v akčním plánu Rady a Komise, kterým se provádí Haagský program o posílení svobody, bezpečnosti a práva v Evropské unii ⁽²⁾.

(1) Evropská unie si dala za cíl udržet a rozvíjet Unii jako prostor svobody, bezpečnosti a práva, ve kterém má být společným postupem členských států v oblasti policejní a justiční spolupráce v trestních věcech zajištěna vysoká úroveň bezpečnosti.

(2) Společný postup v oblasti policejní spolupráce podle čl. 30 odst. 1 písm. b) Smlouvy o Evropské unii a společný postup v oblasti justiční spolupráce v trestních věcech podle čl. 31 odst. 1 písm. a) Smlouvy o Evropské unii vede k potřebě zpracovávat významné informace, které by měly podléhat vhodným předpisům o ochraně osobních údajů.

(3) Právní předpisy, které spadají do oblasti působnosti hlavy VI Smlouvy o Evropské unii, by měly posilovat policejní

(5) Výměna osobních údajů v rámci policejní a justiční spolupráce v trestních věcech, zejména podle zásady dostupnosti informací, jak je stanovena v Haagském programu, by měla být podpořena jasnými pravidly, která zlepší vzájemnou důvěru mezi příslušnými orgány a zajistí, že příslušné informace budou chráněny způsobem vylučujícím jakoukoli diskriminaci v této spolupráci mezi členskými státy při plném dodržování základních práv dotčených osob. Stávající právní předpisy na evropské úrovni nejsou pro tento účel dostačující; směrnice 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 ⁽³⁾ se nevztahuje na zpracování osobních údajů prováděné pro výkon činností mimo oblast působnosti práva Společenství, například činnosti stanovené v hlavě VI Smlouvy o Evropské unii, ani se v žádném případě nevztahuje na zpracování, jež se týká veřejné bezpečnosti, obrany, bezpečnosti státu nebo činností státu v oblasti trestního práva.

⁽¹⁾ Úř. věst. C 125 E, 22.5.2008, s. 154.

⁽²⁾ Úř. věst. C 198, 12.8.2005, s. 1.

⁽³⁾ Úř. věst. L 281, 23.11.1995, s. 31.

- (6) Toto rámcové rozhodnutí se vztahuje pouze na údaje shromažďované nebo zpracovávané příslušnými orgány za účelem předcházení trestným činům, jejich vyšetřování, odhalování nebo stíhání nebo výkonu trestů. Toto rámcové rozhodnutí by mělo ponechat na členských státech, aby na vnitrostátní úrovni přesněji určily, jaké další účely budou považovány za neslučitelné s účelem, pro který byly osobní údaje původně shromažďovány. Obecně by další zpracovávání pro historické, statistické nebo vědecké účely nemělo být považováno za neslučitelné s původním účelem zpracování.
- (7) Oblast působnosti tohoto rámcového rozhodnutí je omezena na zpracování osobních údajů předaných nebo zpřístupněných mezi členskými státy. Z tohoto omezení nelze vyvozovat žádné závěry ohledně pravomoci Unie přijímat předpisy týkající se sběru a zpracování osobních údajů na vnitrostátní úrovni nebo prospěšnost pro Unii tak činit v budoucnu.
- (8) Členské státy mají k usnadnění výměny údajů v Unii v úmyslu zajistit, aby úroveň ochrany osobních údajů dosažená při vnitrostátním zpracování údajů odpovídala úrovni stanovené tímto rámcovým rozhodnutím. Pokud jde o vnitrostátní zpracovávání údajů, nebrání toto rámcové rozhodnutí členským státům v tom, aby stanovily opatření na ochranu osobních údajů, která jsou přísnější než opatření podle tohoto rámcového rozhodnutí.
- (9) Toto rámcové rozhodnutí by se nemělo vztahovat na osobní údaje, které členský stát získal v oblasti působnosti tohoto rámcového rozhodnutí a které pocházejí z tohoto členského státu.
- (10) Sblížení právních předpisů členských států by nemělo vést k uvolnění ochrany údajů v těchto státech, ale mělo by naopak mít za cíl zajištění vysoké úrovně ochrany uvnitř Unie.
- (11) Je nezbytné upřesnit cíle ochrany údajů v rámci policejní a justiční činnosti a stanovit pravidla pro zákonnost zpracování osobních údajů s cílem zajistit, aby veškeré informace, které mohou být vyměňovány, byly zpracovávány zákonně a v souladu s platnými základními zásadami týkajícími se kvality údajů. Zároveň by neměly být žádným způsobem ohrožovány zákonné činnosti policie nebo celních, justičních a jiných příslušných orgánů.
- (12) Zásadu správnosti údajů je nutno uplatňovat s ohledem na povahu a účel daného zpracování údajů. Například zejména v soudním řízení se údaje zakládají na subjektivním vnímání jednotlivých osob a v některých případech je nelze vůbec ověřit. Požadavek na správnost se tedy nemůže týkat správnosti určitého prohlášení, ale pouze skutečnosti, že konkrétní prohlášení bylo učiněno.
- (13) Archivace v oddělených souborech údajů by měla být přípustná pouze tehdy, nejsou-li údaje již nezbytné a používané pro účely předcházení trestným činům, jejich vyšetřování, odhalování či stíhání nebo výkonu trestů. Archivace v oddělených souborech údajů by rovněž měla být přípustná, pokud jsou archivované údaje uloženy v databázi společně s jinými údaji tak, že již nemohou být použity pro účely předcházení trestným činům, jejich vyšetřování, odhalování či stíhání nebo výkonu trestů. Přiměřenost délky archivace by měla záviset na účelech archivace a oprávněných zájmech subjektů údajů. V případě archivace pro historické účely je možno počítat s velmi dlouhým obdobím.
- (14) Údaje mohou být rovněž vymazány zničením nosiče údajů.
- (15) Pokud jde o nepřesné, neúplné či již neaktuální údaje předávané nebo zpřístupňované jiným členským státům a dále zpracovávané orgány obdobnými soudům, tedy orgány, které mají pravomoc činit právně závazná rozhodnutí, měly by jejich oprava, výmaz nebo blokování probíhat v souladu s vnitrostátním právem.
- (16) Zajištění vysoké úrovně ochrany osobních údajů fyzických osob vyžaduje společná ustanovení o zjišťování zákonnosti a kvality údajů zpracovávaných příslušnými orgány v jiných členských státech.
- (17) Je vhodné na evropské úrovni stanovit podmínky, za kterých by příslušným orgánům členských států bylo povoleno předávat a zpřístupňovat osobní údaje, které obdržely od jiných členských států, orgánům a soukromým subjektům ve členských státech. V mnoha případech je předávání osobních údajů soukromým subjektům justičními, policejními nebo celními orgány nutné za účelem stíhání trestné činnosti nebo zabránění bezprostřednímu a vážnému ohrožení veřejné bezpečnosti nebo k zabránění závažnému porušení práv fyzických osob, například vydáním varování týkajících se padělání cenných papírů pro banky a úvěrové instituce nebo, v oblasti trestné činnosti týkající se vozidel, sdělením osobních údajů pojišťovně s cílem zabránit nedovolenému obchodu s využitím ukradených motorových vozidel nebo zlepšit podmínky pro znovuzískání ukradených motorových vozidel ze zahraničí. Toto není rovnocenné předávání úkolů policejních nebo justičních orgánů soukromým subjektům.

- (18) Pravidla tohoto rámcového rozhodnutí týkající se předávání osobních údajů justičními, policejními nebo celními orgány soukromým subjektům se nevztahují na sdělování údajů soukromým subjektům (například obhájcem a obětí) v trestním řízení.
- (19) Další zpracování osobních údajů obdržených od příslušného orgánu jiného členského státu nebo tímto orgánem zpřístupněných, zejména jejich další předání nebo zpřístupnění, by mělo podléhat společným pravidlům na evropské úrovni.
- (20) Mohou-li být osobní údaje dále zpracovávány na základě souhlasu členského státu, od něhož byly údaje získány, měl by mít každý členský stát možnost upravit způsoby udělování tohoto souhlasu, včetně například prostřednictvím obecného souhlasu pro kategorie informací nebo pro kategorie dalšího zpracování.
- (21) Mohou-li být osobní údaje dále zpracovávány pro účely správních řízení, zahrnují tato řízení rovněž činnosti prováděné regulačními orgány a orgány dozoru.
- (22) Zákonná činnost policejních, celních, justičních a jiných příslušných orgánů může vyžadovat, aby byly údaje zaslány orgánům ve třetích státech nebo mezinárodním subjektům, které jsou povinny předcházet trestným činům, vyšetřovat je, odhalovat nebo stíhat nebo zajišťovat výkon trestů.
- (23) Osobní údaje předávané členským státem třetím státům nebo mezinárodním subjektům by měly být v zásadě chráněny přiměřeným způsobem.
- (24) Pokud jsou osobní údaje předávány z členského státu třetím státům nebo mezinárodním subjektům, mělo by se takové předání v zásadě uskutečnit pouze poté, co členský stát, od něhož byly údaje získány, vyjádří souhlas s tímto dalším předáním. Každý členský stát by měl mít možnost upravit způsoby udělení tohoto souhlasu, včetně například prostřednictvím obecného souhlasu pro kategorie informací nebo pro určité třetí státy.
- (25) V zájmu účinné spolupráce při vymáhání práva je třeba, aby pokud je povaha ohrožení veřejné bezpečnosti členského státu nebo třetího státu tak bezprostřední, že není možné včas získat předchozí souhlas, měl příslušný orgán možnost předat příslušné osobní údaje dotčenému třetímu státu bez tohoto předchozího souhlasu. Totéž by se mohlo použít, pokud se jedná o jiné podstatné zájmy členského státu rovnocenného významu, například pokud by mohla být bezprostředně a vážně ohrožena kritická infrastruktura členského státu nebo pokud by mohl být vážně narušen finanční systém členského státu.
- (26) Může být nutné informovat subjekt údajů o zpracování jeho osobních údajů, zejména v případech závažných zásahů do jeho práv prostřednictvím tajného získávání údajů, aby se tomuto subjektu zajistila možnost účinné právní ochrany.
- (27) Členské státy by měly zajistit, aby byl subjekt údajů informován o tom, že osobní údaje by mohly být nebo jsou shromažďovány, zpracovávány nebo předávány jinému členskému státu za účelem předcházení trestným činům a jejich vyšetřování, stíhání a odhalování nebo za účelem výkonu trestů. Právo subjektu údajů být informován a výjimky z něj by mělo upravovat vnitrostátní právo. Toto informování může mít obecnou podobu, například prostřednictvím právního předpisu nebo zveřejnění seznamu činností při zpracování údajů.
- (28) Aby se zajistila ochrana osobních údajů, aniž by byl ohrožen zájem trestního vyšetřování, je nezbytné vymezit práva subjektu údajů.
- (29) Některé členské státy stanovily právo subjektu údajů na přístup v trestních věcech prostřednictvím systému, v jehož rámci má vnitrostátní orgán dozoru namísto subjektu údajů neomezený přístup ke všem osobním údajům vztahujícím se k subjektu údajů a může rovněž opravovat, mazat nebo aktualizovat nepřesné údaje. V takovém případě nepřímého přístupu může vnitrostátní právo těchto členských států stanovit, že vnitrostátní orgán dozoru pouze informuje subjekt údajů o tom, že byla provedena všechna nezbytná ověření. Tyto členské státy však rovněž pro subjekt údajů stanoví možnosti přímého přístupu v konkrétních případech, například pro přístup k soudním záznamům, pro získání kopií vlastních záznamů v rejstříku trestů nebo dokumentů o vlastních výsleších vedených policejními orgány.
- (30) Je vhodné stanovit společná pravidla o důvěrné povaze a bezpečnosti zpracování, odpovědnosti a sankcích za nezákonné využití údajů příslušnými orgány, jakož i o prostředcích právní nápravy, které má subjekt údajů k dispozici. Je však na každém členském státu, aby určil povahu pravidel pro odškodnění a sankcí použitelných v případě porušení vnitrostátních předpisů o ochraně údajů.
- (31) Toto rámcové rozhodnutí umožňuje, aby se při provádění zásad v něm stanovených brala v úvahu zásada práva na přístup veřejnosti k úředním dokumentům.

- (32) Je-li nutné chránit osobní údaje ve vztahu ke zpracování, jež svým rozsahem nebo druhem představuje zvláštní rizika pro základní práva a svobody, například zpracování za použití nových technologií, mechanismů nebo postupů, je vhodné zajistit, aby byly před vytvořením souborů pro zpracování těchto údajů konzultovány příslušné vnitrostátní orgány dozoru.
- (33) Zřízení nezávislých orgánů dozoru v členských státech je podstatným prvkem ochrany osobních údajů zpracovávaných v rámci policejní a justiční spolupráce členských států.
- (34) Mělo by být možné, aby úkoly, které mají plnit vnitrostátní orgány dozoru zřízované podle tohoto rámcového rozhodnutí, byly rovněž svěřeny orgánům dozoru, které již byly v členských státech zřízeny na základě směrnice 95/46/ES.
- (35) Uvedené orgány dozoru by měly mít k dispozici nezbytné prostředky pro plnění svých úkolů, včetně pravomoci provádět šetření a zasahovat, zejména pokud jsou těmto orgánům podány stížnosti jednotlivých osob, nebo pravomoci podat podnět k zahájení soudního řízení. Měly by přispívat k průhlednosti zpracování údajů v členských státech, do jejichž pravomoci spadají. Jejich pravomoci by však neměly být v rozporu se zvláštními pravidly stanovenými pro trestní řízení nebo nezávislost soudů.
- (36) Článek 47 Smlouvy o Evropské unii stanoví, že se uvedená smlouva nedotýká smluv o založení Evropských společenství ani následných smluv či aktů tyto smlouvy pozměňujících nebo doplňujících. Tímto rámcovým rozhodnutím proto není dotčena ochrana osobních údajů podle práva Společenství, jak je stanoveno zejména ve směrnici 95/46/ES, v nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů ⁽¹⁾ a ve směrnici Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích) ⁽²⁾.
- (37) Tímto rámcovým rozhodnutím nejsou dotčena pravidla týkající se protiprávního přístupu k údajům, která jsou obsažena v rámcovém rozhodnutí Rady 2005/222/SVV ze dne 24. února 2005 o útocích proti informačním systémům ⁽³⁾.
- (38) Tímto rámcovým rozhodnutím nejsou dotčeny stávající povinnosti ani závazky členských států nebo Unie vyplývající z dvoustranných nebo mnohostranných dohod se třetími státy. Budoucí dohody by měly být v souladu s pravidly o výměně údajů se třetími státy.
- (39) Několik aktů přijatých na základě hlavy VI Smlouvy o Evropské unii obsahuje zvláštní ustanovení o ochraně osobních údajů vyměňovaných nebo jinak zpracovávaných podle uvedených aktů. V některých případech tvoří tato ustanovení úplný a soudržný soubor pravidel zahrnujících všechny příslušné aspekty ochrany údajů (zásady kvality údajů, pravidla o bezpečnosti údajů, úpravu práv a záruk subjektů údajů, organizaci dozoru a rozložení odpovědnosti) a upravují dané záležitosti podrobněji než toto rámcové rozhodnutí. Příslušný soubor ustanovení o ochraně údajů v těchto aktech, zejména v těch, které upravují fungování Europolu, Eurojustu, Schengenského informačního systému (SIS) a celním informačním systému (CIS), jakož i těch, které zavádějí přímý přístup pro orgány členských států k některým systémům údajů jiných členských států, by tímto rámcovým rozhodnutím neměl být dotčen. Totéž platí pro ustanovení o ochraně údajů, která upravují automatizované předávání profilů DNA, daktyloskopických údajů a vnitrostátních údajů o registraci vozidel mezi členskými státy podle rozhodnutí Rady 2008/615/SVV ze dne 23. června 2008 o posílení přeshraniční spolupráce, zejména v boji proti terorismu a přeshraniční trestné činnosti ⁽⁴⁾.
- (40) V jiných případech mají ustanovení o ochraně údajů v aktech přijatých na základě hlavy VI Smlouvy o Evropské unii omezenější oblast působnosti. Často stanoví zvláštní podmínky pro členský stát, který obdrží informace obsahující osobní údaje od jiných členských států, pokud jde o účely, ke kterým může tyto údaje použít, ale ohledně jiných aspektů ochrany údajů odkazují tato ustanovení na Úmluvu Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních dat ze dne 28. ledna 1981 nebo na vnitrostátní právo. Pokud jsou ustanovení uvedených aktů ukládající podmínky ohledně použití nebo dalšího předávání osobních údajů přijímajícím členským státům více omezující než odpovídající ustanovení tohoto rámcového rozhodnutí, neměla by být tímto rámcovým rozhodnutím dotčena. Pro všechny ostatní aspekty by se však měla použít pravidla stanovená v tomto rámcovém rozhodnutí.
- (41) Tímto rámcovým rozhodnutím není dotčena úmluva Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních dat, dodatkový protokol k uvedené úmluvě ze dne 8. listopadu 2001 ani úmluva Rady Evropy o justiční spolupráci v trestních věcech.

⁽¹⁾ Úř. věst. L 8, 12.1.2001, s. 1.

⁽²⁾ Úř. věst. L 201, 31.7.2002, s. 37.

⁽³⁾ Úř. věst. L 69, 16.3.2005, s. 67.

⁽⁴⁾ Úř. věst. L 210, 6.8.2008, s. 1.

(42) Jelikož cíle tohoto rámcového rozhodnutí, totiž určených společných pravidel na ochranu osobních údajů zpracovávaných v rámci policejní a justiční spolupráce v trestních věcech, nemůže být uspokojivě dosaženo na úrovni členských států, a proto jej může být z důvodu rozsahu a účinků opatření lépe dosaženo na úrovni Unie, může Unie přijmout opatření v souladu se zásadou subsidiarity stanovenou v článku 5 Smlouvy o založení Evropského společenství a uvedenou v článku 2 Smlouvy o Evropské unii. V souladu se zásadou proporcionality stanovenou v článku 5 Smlouvy o založení Evropského společenství nepřekračuje toto rámcové rozhodnutí rámec toho, co je nezbytné pro dosažení tohoto cíle.

(43) Spojené království se účastní tohoto rámcového rozhodnutí v souladu s článkem 5 Protokolu o začlenění schengenského *acquis* do rámce Evropské unie, připojeného ke Smlouvě o Evropské unii a Smlouvě o založení Evropského společenství, a v souladu s čl. 8 odst. 2 rozhodnutí Rady 2000/365/ES ze dne 29. května 2000 o žádosti Spojeného království Velké Británie a Severního Irsku, aby se na ně vztahovala některá ustanovení schengenského *acquis* ⁽¹⁾.

(44) Irsko se účastní tohoto rámcového rozhodnutí v souladu s článkem 5 Protokolu o začlenění schengenského *acquis* do rámce Evropské unie, připojeného ke Smlouvě o Evropské unii a Smlouvě o založení Evropského společenství, a v souladu s čl. 6 odst. 2 rozhodnutí Rady 2002/192/ES ze dne 28. února 2002 o žádosti Irsku, aby se na ně vztahovala některá ustanovení schengenského *acquis* ⁽²⁾.

(45) Pokud jde o Island a Norsko, rozvíjí toto rámcové rozhodnutí ta ustanovení schengenského *acquis* ve smyslu dohody uzavřené mezi Radou Evropské unie a Islandskou republikou a Norským královstvím o přidružení Islandské republiky a Norského království k provádění, uplatňování a rozvoji schengenského *acquis* ⁽³⁾, která spadají do oblasti uvedené v čl. 1 bodech H a I rozhodnutí Rady 1999/437/ES ⁽⁴⁾ o některých opatřeních pro uplatňování uvedené dohody

(46) Pokud jde o Švýcarsko, rozvíjí toto rámcové rozhodnutí ta ustanovení schengenského *acquis* ve smyslu Dohody mezi Evropskou unií, Evropským společenstvím a Švýcarskou konfederací o přidružení Švýcarské konfe-

derace k provádění, uplatňování a rozvoji schengenského *acquis* ⁽⁵⁾, která spadají do oblasti uvedené v čl. 1 bodech H a I rozhodnutí 1999/437/ES ve spojení s článkem 3 rozhodnutí Rady 2008/149/SVV ⁽⁶⁾ o uzavření uvedené dohody jménem Evropské unie.

(47) Pokud jde o Lichtenštejnsko, rozvíjí toto rámcové rozhodnutí ta ustanovení schengenského *acquis* ve smyslu Protokolu mezi Evropskou unií, Evropským společenstvím, Švýcarskou konfederací a Lichtenštejnským knížectvím o přistoupení Lichtenštejnského knížectví k Dohodě mezi Evropskou unií, Evropským společenstvím a Švýcarskou konfederací o přidružení Švýcarské konfederace k provádění, uplatňování a rozvoji schengenského *acquis*, která spadají do oblasti uvedené v čl. 1 bodech H a I rozhodnutí Rady 1999/437/ES ve spojení s článkem 3 rozhodnutí Rady 2008/262/SVV ⁽⁷⁾ o podpisu uvedeného protokolu jménem Evropské unie.

(48) Toto rámcové rozhodnutí ctí základní práva a zachovává zásady uznávané zejména v Listině základních práv Evropské unie ⁽⁸⁾. Snahou tohoto rámcového rozhodnutí je zajistit plné respektování práva na ochranu soukromí a práva na ochranu osobních údajů uvedených v člancích 7 a 8 Listiny,

PŘIJALA TOTO RÁMCOVÉ ROZHODNUTÍ:

Článek 1

Účel a oblast působnosti

1. Účelem tohoto rámcového rozhodnutí je zajistit vysokou úroveň ochrany základních práv a svobod fyzických osob, zejména jejich práva na soukromí, při zpracování osobních údajů v rámci policejní a justiční spolupráce v trestních věcech stanovené v hlavě VI Smlouvy o Evropské unii a současně zajistit vysokou úroveň veřejné bezpečnosti.

2. V souladu s tímto rámcovým rozhodnutím chrání členské státy základní práva a svobody fyzických osob, zejména jejich právo na soukromí, jsou-li nebo byly-li osobní údaje za účelem předcházení trestným činům, jejich vyšetřování, odhalování nebo stíhání nebo za účelem výkonu trestů

a) předávány nebo zpřístupňovány mezi členskými státy;

⁽¹⁾ Úř. věst. L 131, 1.6.2000, s. 43.

⁽²⁾ Úř. věst. L 64, 7.3.2002, s. 20.

⁽³⁾ Úř. věst. L 176, 10.7.1999, s. 36.

⁽⁴⁾ Úř. věst. L 176, 10.7.1999, s. 31.

⁽⁵⁾ Úř. věst. L 53, 27.2.2008, s. 52.

⁽⁶⁾ Úř. věst. L 53, 27.2.2008, s. 50.

⁽⁷⁾ Úř. věst. L 83, 26.3.2008, s. 5.

⁽⁸⁾ Úř. věst. C 303, 14.12.2007, s. 1.

b) předávány nebo zpřístupňovány členskými státy orgánům nebo informačním systémům zřízeným na základě hlavy VI Smlouvy o Evropské unii nebo

c) předávány nebo zpřístupňovány příslušným orgánům členských států orgány nebo informačními systémy zřízenými na základě Smlouvy o Evropské unii nebo Smlouvy o založení Evropského společenství.

3. Toto rámcové rozhodnutí se vztahuje na zcela nebo částečně automatizované zpracování osobních údajů, jakož i na neautomatizované zpracování osobních údajů, které jsou nebo mají být uloženy v souboru.

4. Tímto rámcovým rozhodnutím nejsou dotčeny podstatné zájmy národní bezpečnosti nebo zvláštní zpravodajské činnosti v oblasti národní bezpečnosti.

5. Toto rámcové rozhodnutí nebrání členským státům v tom, aby stanovily opatření na ochranu osobních údajů shromažďovaných nebo zpracovávaných na vnitrostátní úrovni, která jsou přísnější než ustanovení tohoto rámcového rozhodnutí.

Článek 2

Definice

Pro účely tohoto rámcového rozhodnutí se rozumí:

a) „osobními údaji“ veškeré informace o identifikované nebo identifikovatelné fyzické osobě („subjekt údajů“); identifikovatelnou osobou se rozumí osoba, kterou lze přímo či nepřímo identifikovat, zejména s odkazem na identifikační číslo nebo na jeden či více zvláštních prvků její fyzické, fyziologické, psychické, ekonomické, kulturní nebo sociální identity;

b) „zpracováním osobních údajů“ a „zpracováním“ jakýkoli úkon nebo soubor úkonů s osobními údaji, které jsou prováděny pomocí či bez pomoci automatizovaných postupů, jako je shromažďování, zaznamenávání, uspořádávání, uchovávání, přizpůsobování nebo pozměňování, vyhledávání, konzultace, použití, sdělení prostřednictvím přenosu, šíření nebo jakékoli jiné zpřístupnění, srovnání či kombinování, jakož i blokování, výmaz nebo zničení;

c) „blokováním“ značení uložených osobních údajů za účelem omezení jejich budoucího zpracování;

d) „souborem osobních údajů“ a „souborem“ jakýkoli uspořádaný soubor osobních údajů přístupných podle určených kritérií, ať již je centralizován, decentralizován nebo rozdělen podle funkčního či zeměpisného hlediska;

e) „zpracovatelem“ subjekt, který zpracovává osobní údaje pro správce;

f) „příjemcem“ subjekt, kterému jsou údaje sdělovány;

g) „soulasem subjektu údajů“ jakýkoli svobodný, výslovný a vědomý projev vůle, kterým subjekt údajů dává svolení k tomu, aby osobní údaje, které se jej týkají, byly předmětem zpracování;

h) „příslušnými orgány“ subjekty zřízené na základě právních aktů Rady podle hlavy VI Smlouvy o Evropské unii, jakož i policejní, celní, justiční a jiné příslušné orgány členských států, které jsou podle vnitrostátního práva oprávněny zpracovávat osobní údaje v oblasti působnosti tohoto rámcového rozhodnutí;

i) „správcem“ fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jakýkoli jiný subjekt, který sám nebo společně s jinými určuje účel a prostředky zpracování osobních údajů;

j) „označováním“ značení uložených osobních údajů, jehož účelem není omezit jejich budoucí zpracování;

k) „anonymizací“ taková změna osobních údajů, v jejímž důsledku je přiřazení jednotlivých údajů o osobních a věcných poměrech určité identifikované nebo identifikovatelné fyzické osobě nemožné nebo možné pouze za nepřiměřeného vynaložení času, nákladů a pracovního úsilí.

Článek 3

Zásady zákonnosti, proporcionality a účelu

1. Příslušné orgány smějí osobní údaje shromažďovat pouze ke stanoveným, výslovně vyjádřeným a legitimním účelům v rámci svých úkolů a zpracovávat je pouze k účelu, pro nějž byly shromažďovány. Zpracování údajů musí být zákonné a přiměřené, podstatné a nepřesahující míru s ohledem na účely, pro které jsou shromažďovány.

2. Další zpracování k jinému účelu je přípustné, pouze pokud

a) toto zpracování je slučitelné s účelem, pro nějž byly údaje shromažďovány;

b) příslušné orgány jsou zmocněny zpracovávat tyto údaje pro takový jiný účel podle platných právních předpisů a

c) toto zpracování je pro tento jiný účel nezbytné a přiměřené.

Kromě toho smějí příslušné orgány předané osobní údaje dále zpracovávat pro historické, statistické či vědecké účely za předpokladu, že členské státy stanoví vhodná ochranná opatření, například anonymizaci údajů.

Článek 4

Oprava, výmaz a blokování

1. Osobní údaje musí být opraveny, pokud jsou nesprávné, a v případě potřeby podle možnosti doplněny nebo aktualizovány.
2. Osobní údaje se vymažou nebo anonymizují, pokud již nejsou potřebné pro účely, pro které byly zákonně shromážděny nebo jsou zákonně dále zpracovávány. Toto ustanovení se nevztahuje na archivaci těchto údajů v oddělených souborech údajů po přiměřenou dobu v souladu s vnitrostátním právem.
3. Pokud existuje oprávněný důvod k domněnce, že by výmaz poškodil oprávněné zájmy subjektu údajů, osobní údaje se namísto vymazání pouze blokují. Blokování lze zpracovávat pouze k účelu, který zabránil jejich výmazu.
4. Jsou-li osobní údaje součástí soudního rozhodnutí nebo záznamu souvisejícího s vydáním soudního rozhodnutí, provádí se oprava, výmaz nebo blokování v souladu s vnitrostátními pravidly soudního řízení.

Článek 5

Stanovení lhůt pro výmaz a přezkum

Pro výmaz osobních údajů nebo pravidelný přezkum nutnosti jejich uchování se stanoví přiměřené lhůty. K dodržování těchto lhůt se stanoví procedurální opatření.

Článek 6

Zpracování zvláštních kategorií údajů

Zpracování osobních údajů, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském nebo filozofickém přesvědčení nebo o členství v odborových organizacích, jakož i zpracování údajů týkajících se zdraví nebo sexuálního života je přípustné pouze tehdy, je-li to nezbytně nutné a stanoví-li vnitrostátní právo odpovídající ochranná opatření.

Článek 7

Automatizovaná individuální rozhodnutí

Rozhodnutí, které vůči subjektu údajů zakládá nepříznivé právní účinky nebo které se jej významně dotýká a které bylo přijato výlučně na základě automatizovaného zpracování údajů určeného k hodnocení určitých rysů jeho osobnosti, je přípustné pouze tehdy, je-li povoleno právním předpisem, který rovněž upřesňuje opatření zajišťující ochranu oprávněných zájmů subjektu údajů.

Článek 8

Ověření kvality údajů, které jsou předávány nebo zpřístupňovány

1. Příslušné orgány učiní veškeré přiměřené kroky, aby nebyly předávány ani zpřístupňovány osobní údaje, které jsou

nesprávné, neúplné nebo již nejsou aktuální. Za tímto účelem příslušné orgány ověří, pokud je to proveditelné, kvalitu osobních údajů před jejich předáním nebo zpřístupněním. Při každém předání údajů se k nim pokud možno doplní dostupné informace, které přijímajícímu členskému státu umožní zhodnotit jejich správnost, úplnost, aktuálnost a spolehlivost. Jestliže byly osobní údaje předány bez předchozího vyžádání, přijímající orgán neprodleně posoudí, zda jsou tyto údaje nezbytné pro účel, pro který byly předány.

2. Zjistí-li se, že došlo k předání nesprávných údajů nebo že údaje byly předány nezákonně, je o tom příjemce neprodleně vyrozuměn. Tyto údaje jsou neprodleně opraveny, vymazány nebo blokovány v souladu s článkem 4.

Článek 9

Lhůty

1. Při předání nebo zpřístupnění údajů může předávající orgán v souladu s vnitrostátním právem a s články 4 a 5 uvést lhůty pro uchovávání údajů, po jejichž uplynutí musí příjemce údaje vymazat nebo blokovat anebo přezkoumat, zda jsou nadále potřebné. Tato povinnost neplatí, pokud jsou údaje v okamžiku uplynutí těchto lhůt potřebné pro probíhající vyšetřování, stíhání trestných činů nebo pro výkon trestů.

2. Pokud předávající orgán neuvedl žádnou lhůtu podle odstavce 1, použijí se pro účely článků 4 a 5 pro uchovávání údajů lhůty stanovené vnitrostátním právem přijímajícího členského státu.

Článek 10

Vedení protokolů a dokumentace

1. Každé předání osobních údajů musí být pro účely ověření zákonnosti zpracování údajů, vlastní kontroly a zajištění řádné neporušenosti a řádného zabezpečení údajů zaprotokolováno nebo zdokumentováno.

2. Protokol nebo dokumentace podle odstavce 1 se na požádání předají příslušnému orgánu dozoru, který provede kontrolu ochrany údajů. Příslušný orgán dozoru použije tyto informace pouze pro kontrolu ochrany údajů a pro zajištění řádného zpracování údajů, jakož i neporušenosti a zabezpečení údajů.

Článek 11

Zpracovávání osobních údajů obdržených od jiného členského státu nebo tímto státem zpřístupněných

Osobní údaje obdržené od příslušného orgánu jiného členského státu nebo tímto orgánem zpřístupněné smějí být v souladu s požadavky čl. 3 odst. 2 dále zpracovávány pouze pro tyto jiné účely, než pro které byly původně předány nebo zpřístupněny:

- a) předcházení trestným činům, jejich vyšetřování, odhalování nebo stíhání nebo výkon trestů, u kterých se nejedná o trestné činy nebo tresty, pro které byly údaje předány nebo zpřístupněny;
- b) jiná soudní a správní řízení, která přímo souvisejí s předcházením trestným činům, jejich vyšetřováním, odhalováním nebo stíháním nebo s výkonem trestů;
- c) zabránění bezprostřednímu a vážnému ohrožení veřejné bezpečnosti nebo
- d) jakýkoli jiný účel pouze s předchozím souhlasem předávajícího členského státu nebo se souhlasem subjektu údajů, je-li poskytnut v souladu s vnitrostátním právem.
- b) přijímající orgán ve třetím státě nebo přijímající mezinárodní subjekt odpovídají za předcházení trestným činům, jejich vyšetřování, odhalování nebo stíhání nebo za výkon trestů;
- c) členský stát, od něhož byly údaje získány, udělil souhlas s dalším předáním v souladu se svým vnitrostátním právem a
- d) dotyčný třetí stát nebo mezinárodní subjekt zajišťuje pro zamýšlené zpracovávání údajů odpovídající úroveň ochrany.
2. Předání údajů bez předchozího souhlasu v souladu s odst. 1 písm. c) je přípustné, pouze pokud je nezbytné pro zabránění bezprostřednímu a vážnému ohrožení veřejné bezpečnosti členského státu nebo třetího státu nebo podstatných zájmů členského státu a předchozí souhlas nelze včas získat. Orgán příslušný pro udělování souhlasu je neprodleně informován.

Kromě toho smějí příslušné orgány předané osobní údaje dále zpracovávat pro historické, statistické či vědecké účely za předpokladu, že členské státy stanoví vhodná ochranná opatření, například anonymizaci údajů.

3. Odchylně od odst. 1 písm. d) mohou být osobní údaje dále předávány, pokud

a) to stanoví vnitrostátní právo členského státu, který údaje dále předává, z důvodu

i) oprávněných zvláštních zájmů subjektu údajů nebo

ii) oprávněných převažujících zájmů, zejména důležitých veřejných zájmů, anebo

b) třetí stát nebo přijímající mezinárodní subjekt stanoví ochranná opatření, která dotyčný členský stát v souladu se svým vnitrostátním právem považuje za odpovídající.

4. Odpovídající úroveň ochrany podle odst. 1 písm. d) se posuzuje s ohledem na všechny okolnosti související s dalším předáním nebo předáváním údajů. Zejména se přihlíží k povaze údajů, účelu a trvání předpokládaného zpracování nebo předpokládaných zpracování, státu původu a státu nebo mezinárodního subjektu konečného určení údajů, k obecným i odvětvovým právním normám platným v dotyčném třetím státě nebo mezinárodním subjektu, jakož i k platným profesním předpisům a bezpečnostním opatřením.

Článek 12

Dodržování vnitrostátních omezení zpracování údajů

1. Pokud podle právních předpisů předávajícího členského státu platí pro výměnu údajů mezi příslušnými orgány uvnitř tohoto členského státu za určitých okolností zvláštní omezení zpracování údajů, předávající orgán na ně upozorní příjemce. Příjemce zajistí, aby tato omezení zpracování údajů byla dodržena.

2. Při uplatňování odstavce 1 neuplatňují členské státy jiná omezení týkající se předávání údajů jiným členskými státy nebo subjektům zřízeným na základě hlavy VI Smlouvy o Evropské unii, než která platí pro obdobné vnitrostátní předávání údajů.

Článek 13

Další předávání údajů příslušným orgánům ve třetích státech nebo mezinárodním subjektům

1. Členské státy stanoví, že osobní údaje, které předal nebo zpřístupnil příslušný orgán jiného členského státu, smějí být dále předány třetím státům nebo mezinárodním subjektům, pouze pokud

a) je to nezbytné pro účely předcházení trestným činům, jejich vyšetřování, odhalování nebo stíhání nebo výkonu trestů;

Článek 14

Předávání soukromým subjektům v členských státech

1. Členské státy stanoví, že osobní údaje, které předal nebo zpřístupnil příslušný orgán jiného členského státu, smějí být předány soukromým subjektům, pouze pokud

- a) příslušný orgán členského státu, od něhož byly údaje získány, udělil souhlas s předáním v souladu se svým vnitrostátním právem;
- b) předání nebrání žádné oprávněné zvláštní zájmy subjektu údajů a
- c) v konkrétních případech je předání pro příslušný orgán předávající údaje soukromému subjektu nutné ke

i) splnění zákonně uložené povinnosti,

ii) předcházení trestným činům, jejich vyšetřování, odhalování nebo stíhání nebo výkon trestů,

iii) zabránění bezprostřednímu a vážnému ohrožení veřejné bezpečnosti nebo

iv) předcházení závažnému porušení práv fyzických osob.

2. Příslušný orgán předávající údaje soukromému subjektu uvědomí tento subjekt o účelech, pro něž mohou být tyto údaje výlučně použity.

Článek 15

Informace vyžádané příslušným orgánem

Příjemce na žádost informuje příslušný orgán, který osobní údaje předal nebo zpřístupnil, o jejich zpracování.

Článek 16

Informování subjektu údajů

1. Členské státy zajistí, aby byl subjekt údajů informován o shromažďování nebo zpracovávání osobních údajů příslušnými orgány těchto států v souladu s vnitrostátním právem.

2. Pokud byly osobní údaje předány nebo zpřístupněny mezi členskými státy, může každý členský stát v souladu se svými vnitrostátními právními předpisy uvedenými v odstavci 1 požádat, aby druhý členský stát subjekt údajů neinformoval. V tom případě posledně uvedený členský stát neinformuje subjekt údajů bez předchozího souhlasu druhého členského státu.

Článek 17

Právo na přístup

1. Každý subjekt údajů má právo obdržet na žádosti učiněné v přiměřených intervalech bez omezení a bez nepřiměřeného prodloužení nebo nadměrných nákladů

a) alespoň potvrzení správce nebo vnitrostátního orgánu dozoru, zda údaje, které se ho týkají, byly či nebyly předávány nebo zpřístupňovány, a rovněž informace o příjemcích nebo kategoriích příjemců, jimž byly údaje předány, a sdělení o údajích, které jsou předmětem zpracování, nebo

b) alespoň potvrzení vnitrostátního orgánu dozoru, že byla provedena všechny nezbytná ověření.

2. Členské státy mohou přijmout legislativní opatření omezující přístup k informacím podle odst. 1 písm. a), pokud toto omezení, s náležitým přihlédnutím k oprávněným zájmům dotyčné osoby, představuje nezbytné a přiměřené opatření

a) s cílem zabránit maření úředních nebo právních šetření, vyšetřování nebo postupů;

b) s cílem zabránit ovlivnění předcházení trestným činům, jejich odhalování, vyšetřování a stíhání nebo výkonu trestů;

c) pro ochranu veřejné bezpečnosti;

d) pro ochranu národní bezpečnosti;

e) pro ochranu subjektu údajů nebo práv a svobod druhých.

3. Odepření či omezení přístupu musí být subjektu údajů oznámeno v písemné podobě. Přitom se sdělí věcné nebo právní důvody tohoto rozhodnutí. Od tohoto sdělení lze upustit, pokud existuje důvod podle odst. 2 písm. a) až e). Ve všech těchto případech je subjekt údajů informován o tom, že se může odvolat k příslušnému vnitrostátnímu orgánu dozoru, justičnímu orgánu nebo k soudu.

Článek 18

Právo na opravu, výmaz nebo blokování

1. Subjekt údajů má právo očekávat, že správce splní své povinnosti v souladu s články 4, 8 a 9 týkající se opravy, výmazu nebo blokování osobních údajů a vyplývající z tohoto rámcového rozhodnutí. Členské státy stanoví, zda subjekt údajů může toto právo uplatnit přímo u správce, nebo prostřednictvím příslušného vnitrostátního orgánu dozoru. Pokud správce odmítne opravu, výmaz nebo blokování provést, musí být toto odmítnutí sděleno písemně subjektu údajů, který musí být rovněž informován o možnostech, jež vnitrostátní právní předpisy stanoví pro podání stížnosti nebo soudní přezkum. Po přezkumu stížnosti nebo soudním přezkumu se subjektu údajů sdělí, zda správce jednal řádně či nikoliv. Členské státy mohou rovněž stanovit, že příslušný vnitrostátní orgán dozoru subjekt údajů informuje o tom, že přezkum byl proveden.

2. Popírá-li subjekt údajů správnost osobního údaje a nelze-li jeho správnost nebo nesprávnost zjistit, může být tento údaj označen.

Článek 19

Právo na náhradu škody

1. Kdokoli, kdo byl poškozen nezákonným zpracováním nebo jiným úkonem neslučitelným s vnitrostátními předpisy přijatými k provedení tohoto rámcového rozhodnutí, má vůči správci nebo jinému orgánu příslušnému podle vnitrostátního práva nárok na náhradu utrpěné škody.

2. Předal-li příslušný orgán členského státu osobní údaje, nemůže se příjemce ve vztahu k poškozenému zprostit podle vnitrostátního práva odpovědnosti tím, že se odvolá na nesprávnost předaných údajů. Jestliže příjemce poskytne náhradu škody v důsledku toho, že použil nesprávně předané údaje, nahradí příjemci příslušný orgán, který údaje předal, částku vyplacenou jako náhradu škody, přičemž zohlední jakoukoli možnou chybu příjemce.

Článek 20

Soudní přezkum

Aniž je dotčena možnost opravného prostředku ve správním řízení, který je možno podat před předložením věci soudu, má subjekt údajů právo v případě porušení práv, jež mu jsou zaručena vnitrostátními předpisy, předložit věc soudu.

Článek 21

Důvěrná povaha zpracování

1. Každý, kdo má přístup k osobním údajům spadajícím do oblasti působnosti tohoto rámcového rozhodnutí, je smí zpracovávat pouze jako člen příslušného orgánu nebo na pokyn příslušného orgánu, ledaže zákon stanoví jinak.

2. Osoby pracující pro příslušný orgán členského státu podléhají všem pravidlům ochrany údajů, která se vztahují na daný příslušný orgán.

Článek 22

Bezpečnost zpracování

1. Členské státy stanoví, že příslušné orgány musí přijmout vhodná technická a organizační opatření na ochranu osobních údajů proti náhodnému nebo nezákonnému zničení, náhodné ztrátě, úpravám, nezákonnému předávání nebo zpřístupnění, zejména pokud zpracování zahrnuje předávání údajů v síti nebo zpřístupňování prostřednictvím přímého automatizovaného přístupu, jakož i proti jakékoli jiné podobě jejich nezákonného zpracování. Přihlédnou přitom zejména k rizikům

vyplývajícím ze zpracování a k povaze údajů, které mají být chráněny. Tato opatření zajistí, s ohledem na stav techniky a na náklady na jejich provedení, přiměřenou úroveň bezpečnosti odpovídající rizikům vyplývajícím ze zpracování údajů a z povahy údajů, které mají být chráněny.

2. Pokud jde o automatizované zpracování údajů, přijme každý členský stát opatření, jež mají

a) zabránit neoprávněným osobám v přístupu k zařízení pro zpracování údajů využívanému pro zpracování osobních údajů (kontrola přístupu k zařízení);

b) zabránit neoprávněnému čtení, kopírování, pozměňování nebo vyjímání nosičů dat (kontrola nosičů dat);

c) zabránit neoprávněnému vkládání údajů a neoprávněnému prohlížení, pozměňování či výmazu uložených osobních údajů (kontrola uchovávání);

d) zabránit neoprávněným osobám v užívání automatizovaných systémů zpracování údajů pomocí zařízení pro přenos údajů (kontrola uživatele);

e) zajistit, aby osoby oprávněné k využívání automatizovaného systému zpracování údajů měly přístup pouze k údajům, na které se vztahuje jejich oprávnění k přístupu (kontrola přístupu k údajům);

f) zajistit, aby bylo možné ověřit a zjistit, kterým subjektům byly nebo mohou být osobní údaje předány nebo zpřístupněny za použití zařízení pro přenos údajů (kontrola předávání);

g) zajistit, aby bylo možné následně ověřit a zjistit, které osobní údaje byly vloženy do automatizovaných systémů zpracování údajů a kdo a kdy je vložil (kontrola vkládání);

h) zabránit neoprávněnému čtení, kopírování, pozměňování nebo mazání osobních údajů v průběhu přenosu osobních údajů nebo přepravy nosičů dat (kontrola přepravy);

i) zajistit, aby instalované systémy mohly být v případě výpadku obnoveny (obnova);

j) zajistit, aby systém fungoval a výskyt chyb ve funkcích byl hlášen (spolehlivost) a aby uložené údaje nebylo možné poškodit špatným fungováním systému (integrita).

3. Členské státy stanoví, že zpracovatelem může být pouze ten, kdo poskytuje záruku, že bude dodržovat nezbytná technická a organizační opatření uvedená v odstavci 1 a že se bude řídit pokyny podle článku 21. Příslušný orgán nad zpracovatelem v těchto otázkách vykonává dozor.

4. Zpracovatel může osobní údaje zpracovávat pouze na základě právního aktu nebo písemné smlouvy.

Článek 23

Předchozí konzultace

Členské státy zajistí, aby byly příslušné vnitrostátní orgány doзору konzultovány před zpracováním osobních údajů, které budou součástí nového souboru, jenž má být vytvořen, pokud

- a) mají být zpracovávány zvláštní kategorie údajů uvedené v článku 6 nebo
- b) z druhu zpracování, zejména při využití nových technologií, mechanismů nebo postupů, jinak vyplývají zvláštní rizika pro základní práva a svobody subjektu údajů, zejména pro právo na soukromí.

Článek 24

Sankce

Členské státy přijmou vhodná opatření, kterými zajistí řádné provedení tohoto rámcového rozhodnutí, a zejména určí účinné, přiměřené a odrazující sankce, které se uplatní v případě porušení předpisů přijatých na základě tohoto rámcového rozhodnutí.

Článek 25

Vnitrostátní orgány doзору

1. Každý členský stát pověří jeden nebo více orgánů veřejné moci na svém území poskytováním poradenství a sledováním uplatňování předpisů přijatých členskými státy na základě tohoto rámcového rozhodnutí. Tyto orgány vykonávají svěřené funkce zcela nezávisle.
2. Každý orgán doзору má zejména
 - a) pravomoci provádět šetření, zahrnující například právo přístupu k údajům, které jsou předmětem zpracování, a oprávnění shromažďovat veškeré informace nezbytné pro splnění svých dozorčích povinností;
 - b) pravomoci účinně zasáhnout, jako například možnost vydávat stanoviska před provedením zpracování a zajistit náležitě zveřejnění těchto stanovisek, pravomoc nařít

blokování, výmaz nebo zničení údajů nebo dočasně nebo trvale zakázat zpracování, pravomoc zaslat správci upozornění či napomenutí nebo pravomoc obrátit se s věcí na vnitrostátní parlamenty či jiné politické orgány;

- c) pravomoc dát podnět k zahájení soudního řízení v případě porušení vnitrostátních předpisů přijatých k provedení tohoto rámcového rozhodnutí nebo pravomoc toto porušení justičnímu orgánu oznámit. Rozhodnutí orgánu doзору, která dala podnět ke stížnostem, je možné napadnout u soudu.

3. Na orgán doзору se může obrátit každá osoba se žádostí týkající se ochrany jejích práv a svobod v souvislosti se zpracováním osobních údajů. Dotčená osoba je informována o způsobu vyřízení své žádosti.

4. Členské státy stanoví, že členové a zaměstnanci orgánů doзору jsou vázáni ustanoveními o ochraně údajů platnými pro příslušný orgán a že podléhají povinnosti dodržovat profesní tajemství v souvislosti s důvěrnými informacemi, ke kterým mají přístup, a to i po ukončení svého pracovního poměru.

Článek 26

Vztah k dohodám se třetími státy

Tímto rámcovým rozhodnutím nejsou dotčeny povinnosti ani závazky členských států nebo Unie vyplývající z dvoustranných nebo mnohostranných dohod se třetími státy existujících v době přijetí tohoto rámcového rozhodnutí.

Při použití těchto dohod se předání osobních údajů, které byly získány z jiného členského státu, třetímu státu provádí v souladu s čl. 13 odst. 1 písm. c) nebo odst. 2.

Článek 27

Hodnocení

1. Členské státy informují do 27. listopadu 2013 Komisi o vnitrostátních opatřeních, která přijaly k zajištění plného souladu s tímto rámcovým rozhodnutím, a zejména ve vztahu k těm ustanovením, jež je třeba dodržovat již během sběru údajů. Komise zejména přezkoumá důsledky těchto ustanovení pro oblast působnosti tohoto rámcového rozhodnutí podle čl. 1 odst. 2.
2. Komise do jednoho roku předloží Evropskému parlamentu a Radě zprávu o výsledku hodnocení podle odstavce 1, kterou doplní případnými vhodnými návrhy změn tohoto rámcového rozhodnutí.

Článek 28**Vztah k dříve přijatým aktům Unie**

Pokud byly v aktech přijatých podle hlavy VI Smlouvy o Evropské unii přede dnem vstupu tohoto rámcového rozhodnutí v platnost, které upravují výměnu osobních údajů mezi členskými státy nebo přístup určených orgánů členských států k informačním systémům zavedeným podle Smlouvy o založení Evropského společenství, zavedeny zvláštní podmínky pro použití těchto údajů přijímajícím členským státem, použijí se uvedené podmínky přednostně před ustanoveními tohoto rámcového rozhodnutí o používání údajů obdržených od jiného členského státu nebo jím zpřístupněných.

Článek 29**Provádění**

1. Členské státy přijmou opatření nezbytná pro dosažení souladu s tímto rámcovým rozhodnutím do 27. listopadu 2010.

2. K témuž datu členské státy sdělí generálnímu sekretariátu Rady a Komisi znění předpisů, kterými ve svém vnitrostátním právu provádějí povinnosti, jež pro ně vyplývají z tohoto rámcového rozhodnutí, jakož i informace o orgánech dozoru uvedených v článku 25. Na základě zprávy vypracované s pomocí těchto údajů Komisi posoudí Rada do 27. listopadu 2011, do jaké míry dosáhly členské státy souladu s tímto rámcovým rozhodnutím.

Článek 30**Vstup v platnost**

Toto rámcové rozhodnutí vstupuje v platnost dvacátým dnem po vyhlášení v *Úředním věstníku Evropské unie*.

V Bruselu dne 27. listopadu 2008.

Za Radu
předsedkyně
M. ALLIOT-MARIE

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 Nejedly, tel.: 234 665 232, fax: 234 665 505

e-mail: posta@uoou.cz

internetová adresa: www.uoou.cz

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

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

ISSN 1213-3442