

Úřední věstník

Evropské unie

C 128



České vydání

Informace a oznámení

Svazek 52

6. června 2009

Oznámení č.	Obsah	Strana
I	<i>Usnesení, doporučení a stanoviska</i>	
	STANOVISKA	
	Evropský inspektor ochrany údajů	
2009/C 128/01	Stanovisko evropského inspektora ochrany údajů k závěrečné zprávě Kontaktní skupiny EU-USA na vysoké úrovni pro sdílení informací a ochranu soukromí a osobních údajů	1
2009/C 128/02	Stanovisko evropského inspektora ochrany údajů ke sdělení Komise Evropskému parlamentu, Radě a Evropskému hospodářskému a sociálnímu výboru – Směrem k evropské strategii pro elektronické soudnictví (e-justice)	13
2009/C 128/03	Návrh stanoviska evropského inspektora ochrany údajů k návrhu směrnice Evropského parlamentu a Rady o uplatňování práv pacientů v přeshraniční zdravotní péči	20
2009/C 128/04	Druhé stanovisko evropského inspektora ochrany údajů k přezkumu směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích)	28
2009/C 128/05	Stanovisko evropského inspektora ochrany údajů k návrhu směrnice Rady, kterou se členským státům ukládá povinnost udržovat minimální zásoby ropy nebo ropných produktů	42

IV *Informace*

INFORMACE ORGÁNŮ A INSTITUCÍ EVROPSKÉ UNIE

Komise

2009/C 128/06	Směnné kurzy vůči euru	45
---------------	------------------------------	----

Tiskové opravy

2009/C 128/07	Oprava úrokové míry použité Evropskou centrální bankou pro hlavní refinanční operace (Úř. věst. C 124 ze dne 4.6.2009)	46
---------------	--	----

I

(Usnesení, doporučení a stanoviska)

STANOVISKA

EVROPSKÝ INSPEKTOR OCHRANY ÚDAJŮ

Stanovisko evropského inspektora ochrany údajů k závěrečné zprávě Kontaktní skupiny EU-USA na vysoké úrovni pro sdílení informací a ochranu soukromí a osobních údajů

(2009/C 128/01)

EVROPSKÝ INSPEKTOR OCHRANY ÚDAJŮ,

s ohledem na Smlouvu o založení Evropského společenství, a zejména na článek 286 této smlouvy,

s ohledem na Listinu základních práv Evropské unie, a zejména na článek 8 této listiny,

s ohledem na směrnici Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů,

s ohledem na 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, a zejména na článek 41 uvedeného nařízení,

PŘIJAL TOTO STANOVISKO:

I. ÚVOD - SOUVISLOSTI STANOVISKA

1. S ohledem na summit EU dne 12. června 2008 oznámilo předsednictví Rady Evropské unie dne 28. května 2008 Coreperu, že Kontaktní skupina EU-USA na vysoké úrovni (dále jen „kontaktní skupina“) pro sdílení informací a ochranu soukromí a osobních údajů dokončila zprávu. Tato zpráva byla zveřejněna dne 26. června 2008 ⁽¹⁾.

⁽¹⁾ Dokument Rady č. 9831/08, dostupný na adrese: http://ec.europa.eu/justice_home/fsj/privacy/news/index_en.htm

2. Zpráva usiluje o určení společných zásad týkajících se ochrany soukromí a údajů jakožto prvního kroku k výměně informací se Spojenými státy za účelem boje proti terorismu a závažné nadnárodní trestné činnosti.

3. Předsednictví Rady ve svém oznámení uvádí, že by uvítalo jakékoli názory, pokud jde o činnosti navazující na tuto zprávu, a zejména odezvu na doporučení ohledně dalších opatření určených ve zprávě. Evropský inspektor ochrany údajů (EIOÚ) na tuto výzvu reaguje předložením tohoto stanoviska vycházejícího ze současné situace, jak je známa, a aniž je dotčen jakýkoli další postoj, který případně zaujme na základě posouzení vývoje dané otázky.

4. EIOÚ bere na vědomí, že činnost kontaktní skupiny proběhla v souvislostech, v nichž zejména od 11. září 2001 došlo k rozvoji výměny údajů mezi USA a EU prostřednictvím mezinárodních dohod či jiných druhů nástrojů. Mezi ně patří dohody Europolu a Eurojustu se Spojenými státy i dohody o jmenné evidenci cestujících a věc Swift, které vedly k výměně dopisů mezi úředníky EU a USA v zájmu stanovení minimálních záruk ochrany údajů ⁽²⁾.

⁽²⁾ — Dohoda mezi Spojenými státy americkými a Evropským policejním úřadem ze dne 6. prosince 2001 a Dodatková dohoda mezi Europolem a USA o výměně osobních údajů a souvisejících informací zveřejněná na internetových stránkách Europolu;
— Dohoda mezi Spojenými státy americkými a Eurojustem o justiční spolupráci, 6. listopadu 2006, zveřejněná na internetové stránce Eurojustu;
— Dohoda mezi Evropskou unií a Spojenými státy americkými o zpracovávání údajů jmenné evidence cestujících (PNR) leteckými dopravci a o jejich předávání Ministerstvu vnitřní bezpečnosti Spojených států amerických (dohoda PNR 2007), podepsána v Bruselu dne 23. července 2007 a ve Washingtonu dne 26. července 2007, Úř. věst. L 204, 4.8.2007, s. 18;
— Výměna dopisů mezi úřady USA a EU ohledně programu sledování financování terorismu, 28. června 2007.

5. EU dále rovněž vyjednává a schvaluje obdobné nástroje, jimiž se stanoví výměna osobních údajů s dalšími třetími zeměmi. Nedávným příkladem je dohoda mezi Evropskou unií a Austrálií o zpracovávání údajů jmenné evidence cestujících (PNR) ze zdrojů Evropské unie leteckými dopravci a o jejich předávání Australské celní správě ⁽³⁾.
6. Z uvedených souvislostí se zdá, že okruh žádostí donucovacích orgánů třetích zemí o osobní informace je stále širší a že se z tradičních vládních databází rozšiřují i na další druhy souborů, zejména soubory údajů shromážděných soukromým sektorem.
7. Jako významnou souvislost EIOÚ rovněž připomíná skutečnost, že otázkou převodu osobních údajů do třetích zemí v rámci policejní a justiční spolupráce v trestních věcech se zabývá rámcové rozhodnutí Rady o ochraně osobních údajů zpracovávaných v rámci policejní a justiční spolupráce v trestních věcech ⁽⁴⁾, které bude pravděpodobně přijato do konce roku 2008.
8. Lze očekávat, že tato transatlantická výměna informací bude pouze vzrůstat a zasáhne i další odvětví, v nichž jsou zpracovávány osobní údaje. V této souvislosti je dialog o „transatlantickém vynucování práva“ vítán a zároveň představuje citlivou otázku. Je vítán v tom smyslu, že by mohl poskytnout jasnější rámec pro výměny údajů, které probíhají či proběhnou. Jde i o citlivou otázku, jelikož takový rámec by mohl legalizovat hromadná předávání údajů v oblasti vynucování práva, což je oblast, v níž je dopad na fyzické osoby zvláště závažný a je především zapotřebí přísných a spolehlivých ochranných opatření a záruk ⁽⁵⁾.
9. Stanovisko se bude v následující kapitole zabývat současným stavem a dalšími možnými opatřeními. Kapitola III se zaměří na oblast působnosti a povahu nástroje, který se umožnil sdílení informací. V kapitole IV bude stanovisko z obecného hlediska analyzovat právní otázky související s obsahem případné dohody. Bude se věnovat otázkám, jako jsou podmínky posouzení úrovně ochrany poskytované ve Spojených státech, a bude projednávat otázku využití regulačního rámce EU jako kritéria pro posouzení této úrovně ochrany. Uvedená kapitola bude rovněž obsahovat seznam základních požadavků, které mají být do této dohody zahrnuty. A v kapitole V stanoviska budou analyzovány zásady týkající se soukromí související se zprávou.

⁽³⁾ Úř. věst. L 213, 8.8.2008, s. 49.

⁽⁴⁾ Rámcové rozhodnutí Rady o ochraně osobních údajů zpracovávaných v rámci policejní a justiční spolupráce v trestních věcech, znění ze dne 24. června 2008 je dostupná na adrese: http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=193371

⁽⁵⁾ Pokud jde o nezbytnost jasného právního rámce, viz kapitola III a IV tohoto stanoviska.

II. Současný stav a další možná opatření

10. EIOÚ hodnotí současný stav takto. Ve vymezení společných standardů pro sdílení informací a ochranu soukromí a osobních údajů bylo dosaženo určitého pokroku.
11. Přípravné práce nejsou však dokončeny na žádném druhu dohody mezi EU a USA. Je třeba pokračovat v práci. Samotná zpráva kontaktní skupiny uvádí celou řadu nevyřešených otázek, z nichž nejvýznačnější je otázka „nápravy“. Přetrvává neshoda ohledně nezbytné oblasti působnosti soudní nápravy ⁽⁶⁾. V kapitole III zprávy bylo určeno pět dalších nevyřešených otázek. Z tohoto stanoviska navíc vyplývá, že dosud není vyřešeno mnoho dalších otázek, například oblast působnosti a povaha nástroje pro sdílení informací.
12. Vzhledem k tomu, že preferovanou možností, které dává přednost i EIOÚ, je závazná dohoda, je skutečně zapotřebí jednat uvážlivě. Než bude možné dosáhnout dohody, je třeba dalších důkladných a zevrubných příprav.
13. Podle EIOÚ by bylo nejvhodnější, kdyby dohoda byla uzavřena v rámci Lisabonské smlouvy, samozřejmě v závislosti na jejím vstupu v platnost. V rámci Lisabonské smlouvy by skutečně nedošlo k právní nejistotě ohledně dělící čáry mezi pilíři EU. Bylo by rovněž zajištěno plné zapojení Evropského parlamentu, jakož i soudní kontrola ze strany Soudního dvora.
14. Za těchto okolností by nejlepším opatřením bylo vypracovat plán pro případnou dohodu v pozdější fázi. Součástí plánu by byly tyto prvky:

— pokyny pro pokračování činnosti kontaktní skupiny (či jakékoli jiné skupiny) a časový plán;

— v počáteční fázi i jednání a případnou dohodu o základních otázkách, jako je oblast působnosti a povaha dohody;

— rozpracování zásad ochrany údajů, a to na základě společného porozumění uvedeným základním otázkám;

— zapojení zúčastněných stran v různých fázích procesu;

— pokud jde o evropskou stranu, řešení institucionálních omezení.

⁽⁶⁾ Strana 5 zprávy, pod písmenem C.

III. OBLAST PŮSOBNOSTI A POVAHA NÁSTROJE PRO SDÍLENÍ INFORMACÍ

15. Podle EIOÚ je zásadní, aby jako první krok vytvoření tohoto nástroje byla jasně vymezena oblast působnosti a povaha případného nástroje, včetně zásad ochrany údajů.

16. Pokud jde o oblast působnosti, dalšími otázkami, na něž je třeba odpovědět, jsou tyto:

— kdo jsou zúčastněné subjekty v rámci oblasti vynucování práva i mimo něj;

— co je míněno „účelem vynucování práva“ a jaký je jeho vztah k dalším účelům, jako je vnitrostátní bezpečnost, a konkrétněji hraniční kontrola a veřejné zdraví;

— jakým způsobem by nástroj zapadal do perspektivy globálního transatlantického prostoru bezpečnosti;

17. Vymezením povahy by se objasnily tyto otázky:

— v rámci kterého pilíře bude nástroj případně vyjednáván;

— zda bude nástroj závazný pro EU i pro USA;

— zda bude mít přímý účinek v tom smyslu, že pro fyzické osoby stanoví práva a povinnosti, které mohou být vymahatelné u justičního orgánu;

— zda nástroj jako takový umožní výměnu informací nebo pro ni zavede minimální standardy, které bude třeba doplnit zvláštními dohodami;

— jaký bude vztah mezi tímto nástrojem a nástroji stávajícími: bude je respektovat, nahradí je, či doplní?

III. 1. Oblast působnosti nástroje

Zúčastněné subjekty

18. Přestože ve zprávě kontaktní skupiny není jasně uvedena přesná oblast působnosti budoucího nástroje, ze zásad, které jsou v ní uvedeny, lze vyvodit, že se má vztahovat

na předávání mezi soukromými a veřejnými subjekty ⁽⁷⁾ i mezi veřejnými orgány.

- Mezi soukromými a veřejnými subjekty:

19. EIOÚ považuje uplatňování budoucího nástroje na předávání mezi soukromými a veřejnými subjekty za logické. Tento nástroj je vytvořen na základě žádostí o informace od soukromých stran, které USA vyslovila v posledních letech. EIOÚ konstatuje, že z hlediska vynucování práva se soukromé subjekty skutečně stávají systematickým zdrojem informací, a to na úrovni EU či na mezinárodní úrovni ⁽⁸⁾. Věc SWIFT představovala důležitý precedens, při němž byla soukromá společnost požádána, aby systematicky předávala hromadné údaje donucovacím orgánům třetího státu ⁽⁹⁾. Shromažďování údajů PNR od leteckých společností se řídí stejnými zásadami. EIOÚ zpochybnil oprávněnost této tendence již ve svém postoji k návrhu rámcového rozhodnutí o evropském systému PNR ⁽¹⁰⁾.

20. Existují dva další důvody, proč váhat ohledně začlenění předávání údajů mezi soukromými a veřejnými subjekty do budoucího nástroje.

21. Zprvu by začlenění mohlo mít nežádoucí dopad na území samotné EU. EIOÚ má vážné obavy, že lze-li údaje soukromých společností (jako jsou například finanční instituce) v zásadě předávat třetím zemím, mohlo by to vyvolat silný tlak, aby byl v rámci EU stejný druh údajů zpřístupněn obdobným způsobem i donucovacím orgánům. Režim PNR je příkladem takového nevídaného vývoje, který začal tím, že Spojené státy hromadně shromažďovaly údaje cestujících, a poté byl přenesen i do vnitřního evropského kontextu ⁽¹¹⁾, aniž by byla jasně prokázána nezbytnost a přiměřenost daného systému.

22. Z druhé EIOÚ v postoji k návrhu Komise o EU PNR rovněž vznesl otázku rámce pro ochranu údajů (první či třetí pilíř) použitelného na podmínky spolupráce mezi veřejnými a soukromými subjekty: měla by pravidla vycházet z povahy správce údajů (soukromý sektor), nebo ze sledovaného účelu (vynucování práva)? Dělicí

⁽⁷⁾ Viz zejména kapitola 3 zprávy „Nevyřešené otázky související s transatlantickými vztahy“, bod 1: „Důslednost v souvislosti s povinnostmi soukromých subjektů během předávání údajů“

⁽⁸⁾ Tato otázka viz postoj EIOÚ ze dne 20. prosince 2007 k návrhu rámcového rozhodnutí Rady o používání jmenné evidence cestujících pro účely vynucování práva, Úř. věst. C 110, 1.5.2008, s. 1. „Tradičně existoval jasný předěl mezi činnostmi v oblasti vynucování práva a činnostmi soukromého sektoru, kdy úkoly v oblasti vynucování práva vykonávají orgány zvláště určené, zejména policejní složky, a soukromé subjekty jsou vyžadovány pro předávání osobních údajů těmto donucovacím orgánům v jednotlivých situacích. V současné době je tu tendence žádat od soukromých subjektů systematickou spolupráci pro účely vynucování práva.“

⁽⁹⁾ Viz stanovisko Pracovní skupiny článku 29 pro ochranu údajů č. 10/2006 ze dne 22. listopadu 2006 týkající se zpracovávání osobních údajů společností SWIFT (Society for Worldwide Interbank Financial Telecommunication), pracovní dokument WP 128.

⁽¹⁰⁾ Stanovisko ze dne 20. prosince 2007, viz výše.

⁽¹¹⁾ Viz návrh rámcového rozhodnutí o používání jmenné evidence cestujících pro účely vynucování práva, uvedený v poznámce pod čarou 8, ve znění, které v současné době Rada projednává.

čára mezi prvním a třetím pilířem není zdaleka jasná v situacích, kdy povinnost zpracovávat soukromé údaje pro účely vynucování práva je uložena na soukromé subjekty. V této souvislosti je významné, že generální advokát Bot ve svém nedávném stanovisku ve věci týkající se uchovávání údajů⁽¹²⁾ navrhl v daných situacích dělit čáru, ale k tomuto návrhu dodává: „Tato dělicí čára jistě není prosta kritiky a v určitém ohledu se může zdát, že je vytvořena uměle.“ EIOÚ rovněž konstatuje, že rozsudek Soudního dvora ve věci PNR⁽¹³⁾ plně neodpovídá na otázku použitelného právního rámce. Například skutečnost, že směrnice 95/46/ES se nevztahuje na určité činnosti, automaticky neznamena, že tyto činnosti lze regulovat podle třetího pilíře. Výsledkem je, že možná ponechává právní mezeru, co se týče použitelných právních předpisů, a každopádně z ní vyplývá právní nejistota v souvislosti s právními zárukami, které mají subjekty údajů k dispozici.

23. Z tohoto hlediska EIOÚ zdůrazňuje, že je třeba zajistit, že budoucí nástroj s obecnými zásadami ochrany údajů nebude moci legalizovat transatlantické předávání osobních údajů mezi soukromými a veřejnými stranami jako takové. Toto předávání údajů může být v budoucím nástroji zahrnuto, pouze pokud:

- budoucí nástroj stanoví, že předávání údajů je možné jen tehdy, jestliže je prokázáno, že je to pro konkrétní účel nezbytně nutné, o čemž se rozhodne jednotlivě;
- předávání údajů jako takové je doprovázeno významnými opatřeními na ochranu údajů (jak je popsáno v tomto stanovisku).

EIOÚ rovněž bere na vědomí nejistotu ohledně použitelného rámce pro ochranu údajů a naléhavě proto žádá, aby v žádném případě nebylo předávání osobních údajů mezi soukromými a veřejnými stranami zahrnuto do současné podoby právních předpisů EU.

- Mezi veřejnými orgány:

24. Přesná oblast výměny informací není jasná. Při další práci na vytvoření společného nástroje by v první řadě měla být ujasněna předpokládaná oblast působnosti tohoto nástroje. Otázkou zůstává zejména:

- zda souvislosti s databázemi umístěnými v EU by se

nástroj zaměřil na centralizované databáze (částečně) spravované Evropskou unií, jako jsou například databáze Europolu a Eurojustu, nebo na decentralizované databáze spravované členskými státy, či na obojí;

- zda se oblast působnosti nástroje vztahuje i na propojené sítě, to znamená, zda se plánované záruky budou vztahovat na údaje vyměňované mezi členskými státy či agenturami v EU i v USA;
- zda by se nástroj vztahoval pouze na výměnu mezi databázemi v oblasti vynucování práva (policie, justice, případně celní úřady) nebo i mezi dalšími databázemi, jako jsou daňové databáze;
- zda by se nástroj týkal i databází vnitrostátních bezpečnostních orgánů, nebo zda by těmto orgánům umožnil přístup k databázím v oblasti vynucování práva na území jiné smluvní strany (EU do databází USA a opačně);
- zda by se nástroj vztahoval na jednotlivé případy předávání informací, či na stálý přístup ke stávajícím databázím. Tento poslední předpoklad by jistě vyvolal otázky proporcionality, jak je projednáno dále v kapitole V bodě 3.

Účel vynucování práva

25. Vymezení účelu případné dohody rovněž ponechává prostor k nejistotě. Účely vynucování práva jsou jasné uvedeny v úvodu, jakož i v první zásadě uvedené v příloze zprávy a budou dále analyzovány v kapitole IV tohoto stanoviska. EIOÚ již nyní konstatuje, že z daných prohlášení se zdá, že výměna údajů by se zaměřila na záležitosti třetího pilíře, ale bylo by zajímavé vědět, zda se jedná pouze o první krok k rozsáhlejší výměně informací. Zdá se zřejmé, že účely „veřejné bezpečnosti“ uvedené ve zprávě zahrnují boj proti terorismu, organizované trestné činnosti a jiným trestným činům. Znamená to však, že se umožní výměna údajů, pokud jde o další veřejné zájmy, jako jsou případná ohrožení veřejného zdraví?

26. EIOÚ doporučuje omezit účel na přesně stanovené předávání údajů a odůvodnit politické rozhodnutí vedoucí k danému vymezení účelu.

⁽¹²⁾ Stanovisko generálního advokáta Bota ze dne 14. října 2008, Irsko v. Evropský parlament a Rada (věc C-301/06), bod 108.

⁽¹³⁾ Rozsudek Soudního dvora ze dne 30. května 2006, Evropský parlament v. Rada Evropské unie (C-317/04) a Komise Evropských společenství (C-318/04), spojené věci C-317/04 a C-318/04, Sb. rozh. [2006], s. I-4721.

Globální transatlantický prostor bezpečnosti

27. Široká oblast působnosti této zprávy by měla být zasazena do perspektivy globálního transatlantického prostoru bezpečnosti, o kterém jednala tzv. „Skupina pro budoucnost“⁽¹⁴⁾. Zpráva této skupiny, která byla vydána v červnu roku 2008, se do určité míry zaměřuje na vnější rozměr politiky v oblasti vnitřních věcí. Uvádí, že „do roku 2014 by Evropská unie měla učinit rozhodnutí o politickém cíli, jímž je vytvoření evropsko-atlantské oblasti spolupráce se Spojenými státy v oblasti svobody, bezpečnosti a práva“. Tato spolupráce by přesahovala oblast bezpečnosti v užším slova smyslu a zahrnovala by alespoň témata, jimiž se zabývá stávající hlava IV Smlouvy o ES, jako je přistěhovalectví, víza a azyl a spolupráce v oblasti občanského práva. Je třeba zvážit, do jaké míry by dohoda o základních zásadách ochrany údajů, jako jsou zásady uvedené ve zprávě kontaktní skupiny, mohla a měla být základem pro výměnu informací v tak široké oblasti.
28. Za běžné situace nebude v roce 2014 struktura pilířů již existovat a bude jeden právní základ pro ochranu údajů v rámci EU jako takové (podle Lisabonské smlouvy článek 16 o fungování Evropské unie). Ze skutečnosti, že existuje harmonizace na úrovni EU v souvislosti s nařízením o ochraně údajů, však nevyplyvá, že by jakákoli dohoda se třetí zemí umožnila předávání jakýchkoli osobních údajů bez ohledu na účel. V závislosti na souvislostech a podmínkách zpracování údajů by pro určité oblasti, jako je vynucování práva, mohly být požadovány upravené záruky ochrany údajů. EIOÚ doporučuje, aby důsledky těchto různých hledisek byly zohledněny při přípravě budoucí dohody.

III.2. Povaha dohody*Evropský institucionální rámec*

29. V krátkodobém horizontu je každopádně nutné určit, v rámci kterého pilíře bude ujednání vyjednáváno. Je toho zapotřebí zejména vzhledem k vnitřnímu regulačnímu rámci pro ochranu údajů, na který bude mít tato dohoda dopad. Bude se jednat o rámec prvního pilíře, v zásadě o směrnici 95/45/ES se zvláštním režimem pro předávání údajů do třetích zemí, nebo o rámec třetího pilíře s méně přísným režimem pro předávání údajů do třetích zemí?⁽¹⁵⁾
30. Přestože, jak již bylo uvedeno, účely vymáhání práva převládají, zpráva kontaktní skupiny zmiňuje shromažďování údajů od soukromých subjektů a účely mohou být rovněž vykládány v širším slova smyslu, který by mohl

přesahovat pouhou bezpečnost, včetně například přistěhovalectví a otázek hraniční kontroly, ale případně i veřejného zdraví. S ohledem na tyto nejasnosti, by bylo značně vhodnější vyčkat s jasným zavedením právního rámce pro jednání a se stanovením konkrétní role evropských orgánů, zejména Evropského parlamentu a Komise, na harmonizaci pilířů v rámci právních předpisů EU, jak je stanoveno v Lisabonské smlouvě.

Závazná povaha nástroje

31. Je třeba ujasnit, zda závěry jednání vyústí v memorandum o porozumění či v jiný nezávazný nástroj, nebo zda půjde o závaznou mezinárodní dohodu.
32. EIOÚ podporuje volbu, která je upřednostňována ve zprávě, tedy závaznou dohodu. Úřední závazná dohoda je dle EIOÚ nezbytným předpokladem pro jakékoli předávání údajů mimo EU, bez ohledu na daný účel předávání údajů. Bez patřičných podmínek a ochranných opatření zahrnutých ve zvláštním (a závazném) právním rámci nemůže proběhnout žádné předání údajů třetí zemi. Jinak řečeno, memorandum o porozumění či jiný nezávazný nástroj mohou být užitečné pro nasměrování jednání o další závazné dohodě, ale nikdy nemohou nahradit nezbytnost závazné dohody.

Přímý účinek

33. Ustanovení nástroje by měla být stejně závazná pro USA i pro EU a její členské státy.
34. Rovněž je třeba zajistit, že na základě dohodnutých zásad budou fyzické osoby oprávněny vykonávat svá práva, a zejména dosáhnout nápravy. Podle EIOÚ lze tohoto výsledku nejlépe dosáhnout v případě, že podstatná ustanovení nástroje budou formulována tak, aby měla přímý účinek na osoby s bydlištěm v Evropské unii a mohla být uplatňována před soudem. V nástroji musí tedy být jasně uveden přímý účinek ustanovení mezinárodní dohody, jakož i podmínky jejího provedení do vnitřních evropských právních předpisů a do vnitrostátního práva za účelem zajištění účinnosti opatření.

Vztah k jiným nástrojům

35. Další základní otázkou rovněž je, do jaké míry je dohoda samostatným nástrojem, či zda musí být v jednotlivých případech doplněna dalšími dohodami o konkrétních výměnách údajů. Je opravdu sporné, zda by se jediná dohoda s jediným souborem standardů mohla patřičně

⁽¹⁴⁾ Zpráva neformální poradní skupiny na vysoké úrovni pro budoucnost evropské politiky v oblasti vnitřních věcí „Svoboda, bezpečnost, soukromí – evropské vnitřní věci v otevřeném světě“, červen 2008, dostupná na stránkách: register.consilium.europa.eu.

⁽¹⁵⁾ Viz články 11 a 13 rámcového rozhodnutí o ochraně údajů uvedeného v bodě 7 tohoto stanoviska.

vztahovat na rozmanitá specifika zpracovávání údajů v rámci třetího pilíře. A lze mít ještě větší pochybnosti o tom, že by bez dodatečných jednání a opatření na ochranu údajů mohla umožnit celkové schválení jakéhokoli předávání osobních údajů, bez ohledu na účel a povahu dotčených údajů. Kromě toho dohody se třetími zeměmi nemusí být trvalé, jelikož mohou souviset s konkrétními hrozbami, mohou podléhat revizi a ustanovením o skončení platnosti. Na druhé straně by společné minimální standardy uznané v závazném nástroji mohly usnadnit veškerá další jednání o převádění osobních údajů, pokud jde o konkrétní databáze či zpracovávání.

36. EIOÚ by tudíž před možností v podobě samostatné dohody upřednostnil vypracování minimálního souboru kritérií pro ochranu údajů, který by byl v jednotlivých případech doplněn dodatečnými zvláštními ustanoveními, jak je uvedeno ve zprávě kontaktní skupiny. Tato dodatečná zvláštní ustanovení jsou předpokladem pro umožnění předávání údajů v konkrétním případě. Toto opatření by podpořilo harmonizovaný přístup, pokud jde o ochranu údajů.

Použitelnost na stávající nástroje

37. Je třeba rovněž posoudit, jakým způsobem by případná obecná dohoda byla kombinována se stávajícími dohodami, které již byly mezi EU a USA uzavřeny. Je třeba uvést, že tyto stávající dohody nemají stejnou závaznou povahu: zejména je třeba zmínit dohodu PNR (která poskytuje největší právní jistotu), dohodu Eurojustu a dohodu Eurojustu či výměnu dopisů týkající se SWIFT⁽¹⁶⁾. Doplněval by nový všeobecný rámec tyto stávající nástroje, nebo by zůstaly beze změn, přičemž nový rámec by se použil pouze pro další budoucí výměny osobních údajů? Podle EIOÚ by právní soulad vyžadoval harmonizovaný soubor pravidel, která by se uplatňovala na stávající i budoucí dohody o předávání údajů a tyto dohody by doplňovala.
38. Výhodou použitelnosti obecné dohody v případě stávajících nástrojů by bylo posílení jejich závazné povahy. To by bylo zvláště vítáno v případě nástrojů, jež nejsou právně závazné, jako je výměna dopisů ohledně SWIFT, jelikož by tak byl alespoň zaveden soulad se souborem obecných zásad týkajících se soukromí.

IV. OBECNÉ PRÁVNÍ HODNOCENÍ

39. Tato kapitola se bude věnovat tomu, jakým způsobem je třeba se zabývat úrovní ochrany konkrétního rámce či nástroje, včetně otázky referenčních kritérií, která mají

být použita, a nezbytných základních požadavků.

Odpovídající úroveň ochrany

40. Podle EIOÚ je třeba jasně uvést, že jedním z hlavních výsledků budoucího nástroje by bylo, že by k předávání osobních údajů Spojeným státům mohlo dojít pouze tehdy, pokud by úřady ve Spojených státech zajistily odpovídající úroveň ochrany (a naopak).
41. EIOÚ se domnívá, že dostatečné záruky, pokud jde o úroveň ochrany osobních údajů, by zajistila pouze zkouška skutečné přiměřenosti. Domnívá se, že by bylo obtížné, aby obecná rámcová dohoda s natolik širokou oblastí působnosti, jako je oblast uvedená ve zprávě kontaktní skupiny, prošla jako taková zkouškou skutečné odpovídající úrovně ochrany. Odpovídající úroveň obecné dohody by bylo možné uznat, pouze pokud je zkombinována s odpovídající úrovní zvláštních dohod uzavřených v jednotlivých případech.
42. Posuzování úrovně ochrany poskytované třetími zeměmi není neobvyklé, zejména v případě Evropské komise: přiměřenost je podle prvního pilíře požadavkem pro předávání údajů. Při různých příležitostech byla podle článku 25 směrnice 95/46 měřena na základě zvláštních kritérií a Evropská komise ji potvrdila ve svých rozhodnutích⁽¹⁷⁾. V rámci třetího pilíře tento systém není výslovně stanoven: Měření odpovídající úrovně ochrany je stanoveno pouze v konkrétních situacích článku 11 a 13 dosud nepřijatého rámcového nařízení o ochraně údajů⁽¹⁸⁾ a je ponecháno na členských státech.
43. Ve stávajícím případě se rozsah opatření týká účelů vynucování práva a jednání vede Komise pod dohledem Rady. Souvislosti se od hodnocení zásad „bezpečného přístavu“ (Safe Harbour) či od odpovídající úrovně kanadských právních předpisů odlišují a více souvisejí s nedávnými jednáními se Spojenými státy a Austrálií ohledně PNR, která proběhla v právním rámci třetího pilíře. Zásady kontaktní skupiny však byly rovněž uvedeny v souvislosti s programem bezvízového styku, který se týká hranic a přistěhovalectví, a tudíž otázek prvního pilíře.
44. EIU doporučuje, aby jakékoli rozhodnutí o odpovídající úrovni podle budoucího nástroje vycházelo ze zkušeností

⁽¹⁶⁾ Viz poznámka pod čarou 2.

⁽¹⁷⁾ Rozhodnutí Komise o odpovídající úrovni ochrany osobních údajů ve třetích zemích, včetně Argentiny, Kanady, Švýcarska, Spojených států, Guernsey, Ostrova Man a Jersey, jsou dostupná na adrese: http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm.

⁽¹⁸⁾ Omezeno na případy, kdy členský stát předává třetí zemi či mezinárodnímu subjektu údaje získané od příslušného orgánu v jiném členském státě.

v těchto různých oblastech. Doporučuje rozpracování pojetí „odpovídající úrovně“ v souvislosti s budoucím nástrojem, a to na základě kritérií podobných těm, která byla užita v předchozích určováním odpovídající úrovně.

Vzájemné uznávání – vzájemnost

45. Druhá složka úrovně ochrany se týká vzájemného uznávání systémů EU a USA. Zpráva kontaktní skupiny v této souvislosti uvádí, že cílem by bylo „uznat účinnost systému, který využívá druhá strana pro ochranu soukromí a údajů, v oblastech, jichž se tyto zásady týkají“⁽¹⁹⁾ a dosáhnout „rovnocenného a vzájemného uplatňování právních předpisů v oblasti ochrany soukromí a osobních údajů“.

46. EIOÚ považuje za zřejmé, že vzájemné uznávání (neboli vzájemnost) je možné pouze tehdy, pokud je zajištěna odpovídající úroveň ochrany. Jinými slovy: budoucí nástroj by harmonizoval minimální úroveň ochrany (prostřednictvím rozhodnutí o odpovídající ochraně, přičemž by se zohlednilo, že v jednotlivých případech je třeba zvláštních dohod). Pouze za tohoto předpokladu by mohla být vzájemnost uznána.

47. Prvním prvkem, který je třeba zohlednit, je vzájemnost podstatných ustanovení o ochraně údajů. Podle EIOÚ by se dohoda měla zabývat pojetím vzájemnosti podstatných ustanovení o ochraně údajů tak, aby na jedné straně zajišťovala, že zpracovávání údajů na území EU (a USA) plně dodržuje vnitrostátní právní předpisy o ochraně údajů, a na straně druhé by zaručila, že zpracovávání mimo zemi původu údajů, které spadá do oblasti působnosti dohody, dodržuje zásady ochrany údajů, jak je uvedeno v dohodě.

48. Druhým prvkem je vzájemnost mechanismu nápravy. Je třeba zajistit, aby evropští občané měli k dispozici odpovídající nápravu, jsou-li údaje, které s nimi souvisejí, zpracovávány ve Spojených státech (bez ohledu na právní předpisy použitelné pro toto zpracovávání), a aby Evropská unie a její členské státy stejně tak poskytly rovnocenná práva občanům USA.

49. Třetím prvkem je vzájemnost týkající se přístupu donucovacích orgánů k osobním údajům. Pokud jakýkoli nástroj umožňuje orgánům Spojených států přístup k údajům pocházejícím z Evropské unie, ze vzájemnosti by vyplývalo, že orgány EU by měly mít stejný přístup, pokud jde o údaje pocházející z USA. Vzájemnost nesmí mít negativní dopad na účinnost ochrany subjektu údajů. Jedná se o podmínku pro umožnění transatlantického přístupu donucovacím orgánům. Konkrétně to znamená, že:

— přímý přístup orgánů Spojených států k údajům na území EU (a naopak) by neměl být umožněn; přístup by měl být poskytnut pouze nepřímo, za použití systému „uvolňování údajů“ (systém „push“);

— přístup by měl být poskytnut pod kontrolou orgánů ochrany údajů a justičních orgánů v zemi, kde jsou údaje zpracovávány;

— přístup orgánů Spojených států k databázím v EU by měl být v souladu s podstatnými ustanoveními ochrany údajů (viz výše) a měl by subjektu údajů zajistit plnou nápravu.

Přesnost nástroje

50. Přesné stanovení podmínek posouzení (odpovídající úroveň, rovnocennost, vzájemné uznávání) je zásadní, jelikož vymezuje obsah, pokud jde o přesnost, právní jistotu a účinnost ochrany. Obsah budoucího nástroje musí být přesný a správný.

51. Mělo by být rovněž zřejmé, že jakákoli zvláštní dohoda uzavřená v další fázi bude přesto muset zahrnovat podrobná a úplná opatření na ochranu údajů, pokud jde o subjekt plánované výměny údajů. Pouze taková dvojí úroveň konkrétních zásad ochrany údajů by zajišťovala nezbytnou „vzájemnou způsobilost“ mezi obecnou dohodou a zvláštními dohodami, jak již bylo uvedeno v bodě 35 a 36 tohoto stanoviska.

Vypracování předlohy pro další třetí země

52. Zvláštní pozornost si zaslouží míra, do jaké by se dohoda s USA mohla stát předlohou pro další třetí země. EIOÚ konstatuje, že výše uvedená zpráva Skupiny pro budoucnost uvádí jako strategického partnera EU kromě USA i Rusko. Jsou-li zásady neutrální a v souladu se základními ochrannými opatřeními EU, mohly by představovat užitečný precedens. Specifika související například s právním rámcem přijímací země či účel předávání údajů by však úplnému provedení dohody zabránily. Stejně tak rozhodující bude situace v oblasti demokracie ve třetích zemích: je třeba se ujistit, že dohodnuté zásady budou v přijímací zemi skutečně zajištěny a prováděny.

Jaká referenční kritéria použít k posouzení úrovně ochrany?

53. Implicitní i explicitní odpovídající úroveň by každopádně měla být v souladu s mezinárodním i evropským právním rámcem, a zejména se společně dohodnutými opatřeními na ochranu údajů. Tato opatření jsou zakotvena

⁽¹⁹⁾ Kapitola A. Závazná mezinárodní dohoda, s. 8.

v pokynech Organizace spojených národů, v úmluvě č. 108 Rady Evropy a v jejím dodatečném protokolu, v pokynech OECD a v rámcovém rozhodnutí o ochraně údajů, jakož i v případě aspektů prvního pilíře ve směrnici 95/46/ES⁽²⁰⁾. Všechny tyto nástroje obsahují podobné zásady, jež jsou obecněji uznány za základ ochrany osobních údajů.

54. Je proto důležité, aby výše uvedené zásady byly řádně zohledněny, přičemž byl zvážen dopad takové případné dohody, jako je dohoda uvedená ve zprávě kontaktní skupiny. Nástroj zabývající se celým odvětvím *vynucování práva* ve třetí zemi by skutečně představoval bezprecedentní situaci. Stávající rozhodnutí v rámci prvního pilíře týkající se přiměřenosti, jakož i dohody uzavřené se třetími zeměmi v rámci třetího pilíře EU (Europol, Eurojust) vždy souvisely s konkrétním předáváním údajů, zatímco tento nástroj by vzhledem k obsáhlému účelu, k němuž má sloužit (boj proti trestným činům, vnitrostátní a veřejná bezpečnost, vymáhání práva na hranicích), a vzhledem k neznámému množství příslušných databází umožnil předávání s mnohem rozsáhlejší oblastí působnosti.

Základní požadavky

55. Podmínky, jež je třeba dodržovat v souvislosti s předáváním osobních údajů třetím zemím, byly vypracovány v pracovním dokumentu Pracovní skupiny článku 29⁽²¹⁾. Jakákoli dohoda o minimálních zásadách týkajících se soukromí by měla uspět ve zkoušce souladu zajišťující účinnost opatření na ochranu údajů.

- Pokud jde o podstatu: zásady ochrany údajů by měly poskytovat vysokou úroveň ochrany a splňovat standardy v souladu se zásadami EU. Dvanáct zásad zahrnutých ve zprávě kontaktní skupiny bude

⁽²⁰⁾ — Pokyny OSN o elektronických souborech osobních údajů přijaté Valným shromážděním dne 14. prosince 1990, které jsou dostupné na adrese: www.unhcr.ch/html/menu3/b/71.htm;

— Úmluva Rady Evropy o ochraně fyzických osob v souvislosti s automatickým zpracováváním osobních údajů, 28. ledna 1981, dostupná na adrese: www.conventions.coe.int/treaty/en/Treaties/html/108.htm;

— Pokyny OECD o ochraně soukromí a přeshraničních toků osobních údajů přijaté dne 23. září 1980, které jsou dostupné na adrese: www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1_1,00.html

— Návrh rámcového rozhodnutí Rady o ochraně osobních údajů zpracovávaných v rámci policejní a justiční spolupráce v trestních věcech, který je dostupný na adrese: http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DossierId=193371

— 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, Úř. věst. L 281, 23.11.1995, s. 31.

⁽²¹⁾ Pracovní dokument ze dne 24. července 1998 o předávání osobních údajů třetím zemím: uplatnění článků 25 a 26 směrnice EU o ochraně údajů; pracovní dokument WP 12.

z tohoto hlediska dále analyzováno v kapitole V tohoto stanoviska.

- Pokud jde o specifika: v závislosti na povaze dohody, zejména pokud bude představovat úřední mezinárodní dohodu, by pravidla a postupy měly být dostatečně podrobné, aby umožnily účinné provádění.

- Pokud jde o dohled: v zájmu zajištění souladu s dohodnutými pravidly by měly být zavedeny zvláštní mechanismy kontroly, a to na úrovni vnitřní (audity) i vnější (přezkumy). Tyto mechanismy musí být stejným způsobem dostupné oběma stranám dohody. Součástí dohledu jsou mechanismy pro zajištění souladu na makroúrovni, jako jsou společné mechanismy přezkumu, jakož i na mikroúrovni, například náprava v jednotlivých případech.

56. Kromě uvedených třech základních požadavků je třeba věnovat zvláštní pozornost specifikům souvisejícím se zpracováváním osobních údajů v kontextu vynucování práva. Jedná se skutečně o oblast, v níž mohou být lidská práva určitým způsobem omezena. Je tedy třeba přijmout opatření na ochranu údajů s cílem vyrovnat omezení práv fyzických osob, zejména v souvislosti s následujícími aspekty, a to s ohledem na dopad na fyzické osoby:

- Transparentnost: pokud jde o vynucování práva, informace a přístup k osobním údajům by mohly být omezeny, a to například kvůli potřebě diskrétnosti při vyšetřování. V rámci EU je běžné zavádět dodatečné mechanismy, které vyrovnávají tato omezení základních práv (často jsou do nich zapojeny nezávislé orgány ochrany údajů), přičemž je třeba zajistit, že podobné vyrovnávací mechanismy budou k dispozici, jakmile bude informace předána třetí zemi.

- Náprava: z výše uvedených důvodů by fyzické osoby měly mít i další možnosti, jak hájit svá práva, zejména prostřednictvím nezávislého orgánu dohledu a před soudem.

- Uchovávání údajů: je možné, že by odůvodnění doby uchovávání údajů nebylo transparentní. Je třeba přijmout opatření, aby se tím subjektům údajů či orgánům dohledu nezabránilo v uplatňování jejich práv.

- Odpovědnost donucovacích orgánů: pokud neexistuje účinná transparentnost, kontrolní mechanismy fyzických osob či zúčastněných stran z institucí nemohou být v žádném případě úplné. Vzhledem k citlivosti údajů a k donucovacím opatřením, která mohou být vůči fyzickým osobám přijata na základě zpracovávání údajů, by však přesto bylo zásadně důležité takové kontroly rozhodně zavést. Odpovědnost je rozhodující, pokud jde o vnitrostátní kontrolní mechanismy přijímací země, ale i o možnosti, které má k dispozici země či region původu údajů. Tyto mechanismy přezkumu jsou stanoveny ve zvláštních dohodách, jako je dohoda PNR, a EIOÚ důrazně doporučuje zařadit je i do obecného nástroje.

V. ANALÝZA ZÁSAD

Úvod

57. Tato kapitola analyzuje dvanáct zásad zahrnutých v dokumentu kontaktní skupiny z následujícího hlediska:

- Tyto zásady ukazují, že USA a EU mají na tyto zásady určité společné názory, a to vzhledem k tomu, že si lze povšimnout podobnosti se zásadami úmluvy č. 108.
- Dohoda ohledně zásad však nepostačuje. Právní dokument by měl být dostatečně silný, aby zajistil soulad.
- EIOÚ lituje, že zásady nedoprovází důvodová zpráva.
- Dříve než se přistoupí k popisu zásad, by mělo být jasné, že obě strany chápou použité formulace stejně, například pokud jde o pojetí osobních informací či chráněných osob. Byly by vítány definice v tomto smyslu.

1. Upřesnění účelu

58. První zásada uvedená v příloze zprávy kontaktní skupiny uvádí, že osobní informace jsou zpracovávány pro zákonné účely vynucování práva. Jak bylo uvedeno, pro Evropskou unii to znamená předcházení, zadržení, vyšetřování či stíhání trestných činů. Pro USA však výklad vynucování práva přesahuje trestné činy a zahrnuje „účely vynucování práva na hranicích, veřejné bezpečnosti a vnitrostátní bezpečnosti“. Důsledky těchto rozdílů mezi uvedenými účely EU a USA nejsou jasné. Přestože zpráva zmiňuje, že účely se v praxi mohou do značné míry shodovat, je

dosud rozhodující přesně vědět, do jaké míry se neshodují. Vzhledem k dopadu opatření na fyzické osoby musí být v oblasti vynucování práva zásada omezení účely vždy přísně dodržována a uvedené účely musí být jasné a zřetelně vymezeny. Vezmeme-li v úvahu vzájemnost uvedenou ve zprávě, zdá se, že sblížení daných účelů je rovněž zásadní. Stručně řečeno, je třeba ujasnit, jak je tato zásada chápána.

2. Celistvost a kvalita údajů

59. EIOÚ vítá ustanovení požadující přesné, patřičné, včasné a úplné osobní informace nezbytné pro zákonné zpracovávání. Tato zásada je základní podmínkou jakékoli účinného zpracovávání údajů.

3. Nezbytnost a proporcionalita

60. Tato zásada stanoví jasnou vazbu mezi shromážděnými informacemi a jejich nezbytností k dosažení účelu vynucování práva stanoveného právními předpisy. Tento požadavek právního základu představuje pozitivní faktor pro zajištění zákonnosti zpracovávání. EIOÚ však konstatuje, že přestože se tím posiluje právní jistota zpracovávání, jeho právní základ spočívá v právních předpisech třetí země. Právní předpisy třetí země nemohou samy o sobě představovat zákonný základ pro předávání osobních údajů⁽²²⁾. V souvislosti se zprávou kontaktní skupiny se zdá, že je považováno za samozřejmé, aby oprávněnost právních předpisů třetí země, tedy Spojených států, byla v zásadě uznána. Je třeba mít na paměti, že jestliže takové úvahy mohou být v tomto případě opodstatněné, jelikož Spojené státy jsou demokratickým státem, stejný režim by neplatil nebo by nemohl být přenesen do vztahů se žádnou další třetí zemí.
61. Podle přílohy zprávy kontaktní skupiny musí být veškeré předávání osobních údajů náležité, nezbytné a patřičné. EIOÚ zdůrazňuje, že proto, aby zpracovávání bylo přiměřené, nesmí být nepřiměřeně rušivé a způsoby zpracovávání musí být vyvážené a musí zohledňovat práva a zájmy subjektů údajů.
62. Z tohoto důvodu by měl být přístup k informacím umožňován případ od případu, v závislosti na praktických potřebách v souvislosti s konkrétním vyšetřováním. Stálý přístup donucovacích orgánů třetí země do databází umístěných v EU by byl považován za nepřiměřený a za

⁽²²⁾ Viz zejména čl. 7 písm. c) a písm. e) směrnice 95/46/ES. Ve stanovisku 6/2002 ze dne 24. října 2002 o předávání zjevných informací o cestujících a jiných údajů od leteckých společností Spojeným státům Pracovní skupina článku 29 uvedla, že „se nezdá přijatelné, aby jednostranné rozhodnutí přijaté třetí zemí z důvodu jejího vlastního veřejného zájmu vedlo k běžnému postupu a hromadnému předávání údajů, které tato směrnice chrání“.

nedostatečně odůvodněný. EIOÚ připomíná, že i v rámci stávajících dohod o výměně údajů, například pokud jde o dohodu PNR, vychází výměna údajů z konkrétních okolností a je uzavírána na omezenou dobu ⁽²³⁾.

63. Vycházíme-li ze stejné logiky, doba uchovávání údajů by měla být regulována: údaje by měly být uchovávány, pouze pokud jsou nezbytné, přičemž by měl být zohledněn konkrétní sledovaný účel. Pokud již nemají význam pro stanovený účel, měly by být odstraněny. EIOÚ důrazně odmítá zřízení databází, v nichž by byly uloženy informace o nepodezřelých fyzických osobách pro případ, že jich bude později případně třeba.

4. Bezpečnost informací

64. Jsou vypracovány zásady týkající se opatření a postupů pro ochranu údajů proti zneužití, pozměnění a dalším rizikům, jakož i ustanovení omezující přístup neoprávněným fyzickým osobám. EIOÚ považuje tuto skutečnost za uspokojivou.
65. Zásadu by rovněž mohlo doplňovat ustanovení uvádějící, že je třeba uchovávat záznamy o subjektech, které do daných údajů nahlíží. Tím by se posílila účinnost ochranných opatření, pokud jde o omezení přístupu a předcházení zneužití údajů.
66. Pro případ narušení bezpečnosti by bylo stanoveno rovněž vzájemné informování: příjemci v USA, jakož i v EU by byli odpovědní za informování svých protějšků v případě, že obdržené údaje byly nezákonně zpřístupněny. Toto opatření přispěje k posílení odpovědnosti za bezpečné zpracovávání údajů.

5. Zvláštní kategorie osobních informací

67. Zásada zakazující zpracovávání citlivých údajů je podle EIOÚ značně oslabena výjimkou umožňující jakékoli zpracovávání citlivých údajů, pro něž vnitrostátní právní předpisy stanoví „vhodná ochranná opatření“. Právě vzhledem k citlivé povaze údajů musí být jakákoli výjimka ze zásady zákazu patřičně a přesně odůvodněna a musí se uvést seznam účelů a okolností, za nichž lze stanovený druh citlivých údajů zpracovávat, jakož i udat povahu správců oprávněných zpracovávat tento druh údajů. Co se týče ochranných opatření, která mají být přijata, EIOÚ se domnívá, že citlivé údaje jako takové by neměly předsta-

vovat prvek, jenž by mohl ohrozit vyšetřování. Za zvláštních okolností by mohly být k dispozici, ale pouze jako dodatečné informace v souvislosti se subjektem údajů, který je již vyšetřován. Ve znění zásady musí být uveden restriktivní výčet těchto ochranných opatření a podmínek.

6. Odpovědnost

68. Jak již bylo podrobněji uvedeno v bodech 55 a 56 tohoto stanoviska, je třeba účinně zajistit odpovědnost veřejných subjektů zpracovávajících osobní údaje a stanovit v dohodě způsob, jímž bude zaručena. Jde o velmi důležitou otázku, jelikož transparentnost, jež je tradičně spojována se zpracováváním osobních údajů v oblasti vynucování práva, není dostatečná. V této souvislosti není dostatečnou zárukou uvést, jako nyní v příloze, že veřejné subjekty jsou odpovědné, aniž by se dále vysvětlila podoba a důsledky této odpovědnosti. EIOÚ doporučuje, aby bylo toto vysvětlení uvedeno ve znění nástroje.

7. Nezávislý a účinný dohled

69. EIOÚ plně podporuje zařazení ustanovení o nezávislém a účinném dohledu ze strany jednoho veřejného orgánu dohledu či několika takových orgánů. Domnívá se, že by mělo být ujasněno, jakým způsobem je nezávislost vykládána, zejména na kom jsou tyto orgány nezávislé a komu podávají zprávy. V tomto ohledu je zapotřebí kritérií, jež by měla zohledňovat vzájemnou závislost institucí a činností v souvislosti s výkonnými a zákonodárnými orgány. EIOÚ připomíná, že jde o zásadní prvek pro zajištění účinného dodržování dohodnutých zásad. Pravomoc zakročit a vynucovat právo, kterou mají tyto orgány, je rovněž zásadní, pokud jde o otázku odpovědnosti veřejných subjektů zpracovávajících osobní údaje, jak již bylo uvedeno. Aby subjekty údajů mohly vykonávat svá práva, měly by být jasně informovány o tom, že tyto orgány existují a jaké jsou jejich pravomoci, zejména pokud nese odpovědnost několik orgánů v závislosti na souvislostech zpracovávání údajů.

70. EIOÚ rovněž doporučuje, aby budoucí dohoda také stanovila mechanismus spolupráce mezi orgány dohledu.

8. Přístup fyzických osob a opravy

71. Pokud jde o přístup a opravy v souvislosti s vynucováním práva, je třeba zvláštních záruk. V tomto ohledu EIOÚ vítá zásadu uvádějící, že fyzické osoby mají či měly by mít přístup a prostředky k „opravám a odstranění svých osobních informací“. Přetrvávají však určité pochybnosti v souvislosti s vymezením „fyzických osob“ (chráněny by měly být veškeré subjekty údajů, nejen občané dotčené země) a s podmínkami, za nichž by fyzické osoby mohly vznést námitky proti zpracovávání svých informací. Je

⁽²³⁾ Platnost této dohody skončí a její účinek zanikne sedm let ode dne podpisu, pokud se strany vzájemně nedohodnou na jejím nahrazení.

třeba přesněji stanovit „vhodné případy“, v nichž by bylo, nebo nebylo možné vznést námitky. Subjekty údajů by měly jasně vědět, za jakých okolností budou moci svá práva vykonávat, tedy například v závislosti na druhu orgánu, druhu vyšetřování či na jiných kritériích.

72. Pokud není možné vznášet námitky proti zpracovávání z oprávněných důvodů přímo, mělo by být k dispozici nepřímé ověřování prostřednictvím nezávislého orgánu odpovědného za dohled nad zpracováváním údajů.

9. Transparentnost a oznamování

73. EIOÚ opět zdůrazňuje význam účinné transparentnosti, aby se fyzickým osobám umožnilo vykonávat jejich práva a přispělo k obecné odpovědnosti veřejných orgánů zpracovávajících osobní údaje. Podporuje navrhované zásady, a trvá zejména na nezbytnosti obecného a individuálního oznamování fyzickým osobám. To se odráží ve znění zásady navrhované v bodě 9 přílohy.

74. Zpráva však v kapitole 2, A. B („Dohodnuté zásady“) uvádí, že v USA může transparentnost zahrnovat „jednotlivě či v kombinaci zveřejnění ve federálním rejstříku, individuální oznámení a zpřístupnění při soudním řízení“. Musí být jasné, že samotné zveřejnění v úředním věstníku pro zajištění, že subjekt údajů bude náležitě informován, nepostačuje. Kromě toho, že je třeba individuálního oznámení, EIOÚ rovněž připomíná, že informace musí být podány v podobě a v jazyce, které jsou subjektu údajů snadno srozumitelné.

10. Náprava

75. Má-li být fyzickým osobám zaručen účinný výkon jejich práv, musí být schopny podat stížnost k nezávislému orgánu ochrany údajů a musí mít možnost podat opravný prostředek k nezávislému a nestrannému soudu. Obě možnosti nápravy by měly být dostupné stejným způsobem.

76. Přístup k nezávislému orgánu ochrany údajů je nezbytný, jelikož poskytuje pružnou a méně nákladnou pomoc v určité oblasti (vynucování práva), která může být pro fyzické osoby poněkud nejasná. Orgány ochrany údajů mohou rovněž poskytnout pomoc tím, že jménem subjektů údajů uplatní právo přístupu, jestliže výjimky brání subjektům údajů v přímém přístupu k jejich osobním údajům.

77. Přístup k justičnímu systému je další dodatečnou a nepostradatelnou zárukou, že subjekty údajů mohou

usilovat o nápravu před orgánem, jenž náleží do jiné složky demokratického systému, než jsou veřejné orgány, které jejich údaje zpracovávají. Evropský soudní dvůr⁽²⁴⁾ považoval tento účinný opravný prostředek před soudem za „zásadní pro zajištění účinné ochrany práv fyzické osoby. (...) Odráží obecnou zásadu práva Společenství, která zdůrazňuje ústavní tradice společné členskými státy a jež byla zakotvena v člancích 6 a 13 Evropské úmluvy o ochraně lidských práv a základních svobod.“ Opravný prostředek je rovněž výslovně stanoven v článku 47 Listiny základních práv Evropské unie a v článku 22 směrnice 95/46/ES, aniž je dotčen jakýkoli správní opravný prostředek.

11. Automatizovaná individuální rozhodnutí

78. EIOÚ vítá ustanovení, které zavádí patřičná ochranná opatření v případě automatizovaného zpracovávání osobních informací. Konstatuje, že shoda názorů ohledně toho, co je myšleno pojmem „podstatná nepříznivá činnost týkající se příslušných zájmů fyzické osoby“, by objasnila podmínky použitelnosti této zásady.

12. Další předávání údajů

79. V případě některých dalších předávání údajů jsou příslušné podmínky nejasné. Zejména pokud další předávání musí být v souladu s mezinárodními ujednáními a dohodami mezi vysílajícími a přijímacími zeměmi, je třeba přesně stanovit, zda se jedná o dohody mezi dvěma zeměmi, které zahájily první předání údajů, nebo mezi dvěma zeměmi, které jsou zapojeny do dalšího předávání. Podle EIOÚ jsou dohody mezi dvěma zeměmi, které zahájily první předání údajů, v každém případě nezbytné.

80. EIOÚ rovněž poukazuje na velmi široké vymezení „oprávněných veřejných zájmů“, které umožňují další předávání údajů. Oblast působnosti veřejné bezpečnosti je i nadále nejasná a rozšíření předávání údajů v případě porušení etických zásad či regulovaných povolání je v souvislosti s vynucováním práva patrně neoprávněné a nadměrné.

VI. ZÁVĚRY

81. EIOÚ vítá společnou práci orgánů EU a USA v oblasti vynucování práva, v níž je ochrana údajů zásadní. Chtěl by však zdůraznit, že se jedná o složitou otázku, zejména pokud jde o přesnou oblast působnosti a povahu, a že si

⁽²⁴⁾ Věc 222/84, *Johnson*, Sb.rozh.1986, s. 1651; věc 222/86, *Heylens*, Sb.rozh. 1987, s. 4097; věc C-97/91, *Borelli*, Sb. rozh. 1992, s. I-6313.

tedy zaslouží pozornou a podrobnou analýzu. Je třeba bedlivě zvážit dopad transatlantického nástroje na ochranu údajů v souvislosti se stávajícím právním rámcem a s důsledky pro občany.

82. EIOÚ vyzývá k větší srozumitelnosti a ke konkrétnějším ustanovením, zejména ohledně těchto aspektů:

- objasnění povahy nástroje, který by měl být právně závazný za účelem poskytnutí dostatečné právní jistoty;
- propracované rozhodnutí o odpovídající úrovni vycházející ze základních požadavků ohledně aspektů režimu týkajících se podstaty, specifik a dohledu. EIOÚ se domnívá, že odpovídající úroveň obecné dohody by bylo možné uznat, pouze pokud je zkombinována s odpovídající úrovní zvláštních dohod uzavřených v jednotlivých případech;
- zřetelně vymezená oblast použitelnosti s jasným a společným vymezením dotčených účelů vynucování práva;
- přesné stanovení způsobů, jimiž se mohou soukromé subjekty zapojit do režimů předávání údajů;
- soulad se zásadou proporcionality, z níž vyplývá výměna údajů v jednotlivých případech, kdy je jí konkrétně zapotřebí;

— silný mechanismus dohledu a mechanismy nápravy dostupné subjektům údajů, včetně správních a soudních opravných prostředků;

— účinná opatření zaručující výkon práv veškerým subjektům údajů, bez ohledu na jejich národnost;

— zapojení nezávislých orgánů ochrany údajů, zejména v souvislosti s dohledem a pomocí subjektům údajů.

83. EIOÚ zdůrazňuje, že vypracování zásad není třeba uspěchat, jelikož by to vedlo pouze k neuspokojivým řešením s opačnými účinky, než jsou účinky zamýšlené v souvislosti o ochranou údajů. V tomto okamžiku by tedy nejlepším postupem bylo sestavit plán pro případné vypracování dohody v pozdější fázi.

84. EIOÚ rovněž vyzývá k větší transparentnosti, co se týče postupu vypracovávání zásad ochrany údajů. Pouze pokud se zapojí veškeré zúčastněné strany, včetně Evropského parlamentu, bude nástroj moci využít demokratické diskuse a získat nezbytnou podporu a uznání.

V Bruselu dne 11. listopadu 2008

Peter HUSTINX
Evropský inspektor ochrany údajů

Stanovisko evropského inspektora ochrany údajů ke sdělení Komise Evropskému parlamentu, Radě a Evropskému hospodářskému a sociálnímu výboru – Směrem k evropské strategii pro elektronické soudnictví (e-justice)

(2009/C 128/02)

EVROPSKÝ INSPEKTOR OCHRANY ÚDAJŮ,

s ohledem na Smlouvu o založení Evropského společenství, a zejména na článek 286 této smlouvy,

s ohledem na Listinu základních práv Evropské unie, a zejména na článek 8 této listiny,

s ohledem na směrnici Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů ⁽¹⁾,

s ohledem na 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 ⁽²⁾, a zejména na článek 41 tohoto nařízení,

PŘIJAL TOTO STANOVISKO:

I. ÚVOD

1. Dne 30. května 2008 bylo přijato sdělení Komise Evropskému parlamentu, Radě a Evropskému hospodářskému a sociálnímu výboru – „Směrem k evropské strategii pro elektronické soudnictví (e-justice)“ (dále jen sdělení). V souladu s článkem 41 nařízení (ES) č. 45/2001 evropský inspektor ochrany údajů (dále jen „EIOU“) předkládá toto stanovisko.
2. Sdělení má za cíl navrhnout strategii pro elektronické soudnictví (e-justice), která by zvýšila důvěru občanů v evropský prostor práva. Základním cílem e-justice je přispět k tomu, aby soudnictví v Evropě bylo efektivněji spravováno v zájmu občanů. Činnost EU by měla umožnit občanům přístup k informacím, aniž by jim v tom bránily jazykové, kulturní a právní bariéry spojené s existencí velkého množství systémů. Návrh akčního plánu a časový rozvrh různých projektů je uveden v příloze k tomuto sdělení.
3. Toto stanovisko EIOU vyjadřuje připomínky ke sdělení, pokud jde o zpracování osobních údajů, ochranu soukromí v oblasti elektronické komunikace a volný pohyb údajů.

II. PODKLADY A KONTEXT

4. Rada ve složení pro spravedlnost a vnější vztahy ⁽³⁾ stanovila několik priorit pro rozvoj e-justice v červnu 2007:

— zřízení evropského rozhraní (portál e-justice);

— vytvoření podmínek pro síťové propojení několika rejstříků, např. rejstříků trestů, insolvenčních, obchodních a podnikatelských rejstříků a katastrů nemovitostí;

— zahájení příprav pro využití informačních a komunikačních technologií v souvislosti s evropským platebním rozkazem;

— lepší využití videokonferenční technologie v přeshraničních řízeních, především pokud jde o dokazování;

— vytvoření pomůcek pro překlad a tlumočení.

5. Práce na problematice e-justice významně pokročila. Dle názoru Komise má tato práce zajistit, aby byla dána přednost operativním projektům a decentralizovaným strukturám, ale zároveň umožnit koordinaci na evropské úrovni, navázat na stávající právní nástroje a zlepšit jejich účinnost pomocí informačních technologií. Podporu projektu e-justice vyjádřil i Evropský parlament ⁽⁴⁾.

6. Používání moderních informačních technologií důsledně podporuje Komise, a to jak v oblasti občanské, tak trestní. Toto vedlo k nástrojům, jako je například evropský platební rozkaz. Komise spravuje od roku 2003 „portál“ Evropské soudní sítě pro občanské a obchodní věci, který je občanům přístupný ve 22 jazycích. Komise rovněž navrhla a zřídila Evropský soudní atlas. Tyto nástroje lze považovat za předchůdce budoucího evropského rámce pro e-justici. Co se týče trestních věcí, připravuje Komise nástroj, který má umožnit výměnu údajů získaných z rejstříků trestů členských států ⁽⁵⁾. Nejen Komise, ale i Eurojust vyvíjí bezpečné komunikační systémy s vnitrostátními orgány.

⁽¹⁾ Úř. věst. L 281, 23.11.1995, s. 31.

⁽²⁾ Úř. věst. L 8, 12.1.2001, s. 1.

⁽³⁾ Dokument 10393/07 JURINFO 21.

⁽⁴⁾ Viz návrh zprávy Výboru Evropského parlamentu pro právní záležitosti.

⁽⁵⁾ Viz zejména systém ECRIS, zmíněný níže.

7. E-justice hodlá v následujících letech poskytnout mnoho příležitostí k tomu, jak evropský soudní prostor přiblížit více občanům. Aby v této důležité záležitosti mohla být vypracována celková strategie, Komise přijala dané sdělení o e-justici. Sdělení stanoví objektivní kritéria pro vytyčení priorit, především pokud jde o budoucí projekty na evropské úrovni, aby bylo možné rozumném čase dosáhnout konkrétních výsledků.
8. Pracovní dokument útvarů Komise a průvodní dokument ke sdělení se souhrnem posouzení dopadů poskytují další podklady⁽⁶⁾. Při přípravě zprávy o posouzení dopadů byly zohledněny názory členských států, justičních orgánů, právnických profesí, občanů a podniků. EIOU konzultován nebyl. Zpráva o posouzení dopadů upřednostnila politickou variantu řešení problémů, která kombinuje evropský rozměr a vnitrostátní pravomoci. Ve sdělení byla zvolena tato politická varianta. Strategie se zaměří na využívání videokonferencí, vytvoření portálu e-justice, zlepšení překladatelských nástrojů vyvinutím automatických internetových pomůcek, zlepšení komunikace mezi justičními orgány, širší propojenost rejstříků jednotlivých členských států a internetové nástroje pro evropská řízení (např. evropský platební rozkaz).
9. EIOU podporuje zaměření na výše uvedené činnosti. Obecně podporuje komplexní přístup e-justice. Schvaluje trojí potřebu zlepšit přístup ke spravedlnosti, spolupráci mezi evropskými právními orgány a efektivnost soudnictví jako takového. V důsledku tohoto přístupu je ovlivněno několik institucí a osob:
- členské státy, které nesou prvotní odpovědnost za zajištění efektivního a spolehlivého soudnictví;
 - Evropská komise coby strážkyně smluv;
 - justiční orgány členských států, které potřebují propracovanější nástroje pro komunikaci, především pokud jde o přeshraniční případy;
 - právníkové profese, občané a podniky, kteří všichni podporují lepší využívání informačních technologií, protože by jim pomohly lépe reagovat na jejich potřeby v soudní oblasti.
10. Sdělení je úzce spojené s návrhem rozhodnutí Rady o vytvoření Evropského informačního systému rejstříků trestů (ECRIS). Dne 16. září 2008 přijal EIOU stanovisko k tomuto návrhu⁽⁷⁾. Podpořil návrh za předpokladu, že bude zohledněno několik faktorů. Obzvláště upozornil, že dodatečné záruky pro ochranu údajů by měly vyvážit současný nedostatek komplexního právního rámce pro ochranu údajů v oblasti spolupráce mezi policejními a justičními orgány. Zdůraznil proto, že je zapotřebí účinná koordinace dozoru nad ochranou údajů v rámci systému, na němž se podílejí orgány členských států a Komise coby poskytovatelé společné komunikační infrastruktury.
11. Za připomínku stojí některá doporučení tohoto stanoviska, například:
- Je třeba zmínit vysokou úroveň ochrany údajů jakožto prvotní podmínku pro přijetí prováděcích opatření;
 - V zájmu lepšího zajištění právní jistoty by měla být upřesněna odpovědnost Komise za společnou infrastrukturu systému i použitelnost nařízení (ES) č. 45/2001;
 - Komise, a nikoliv členské státy, by také měla být odpovědná za propojovací programové vybavení, aby se zajišťovala efektivnost výměny a umožnil lepší dozor nad systémem;
 - Použití strojových překladů by mělo být jasně stanovené a vymezené, aby napomáhalo vzájemnému pochopení trestných činů a neovlivňovalo kvalitu přenesených údajů.
12. Tato doporučení stále ilustrují kontext, ve kterém bude předložené sdělení analyzováno.
- ### III. VÝMĚNA INFORMACÍ PŘEDPOKLÁDANÁ PODLE SDĚLENÍ
13. E-justice má širokou oblast působnosti, která obecně zahrnuje používání informačních technologií při výkonu spravedlnosti v Evropské unii. Tato působnost zahrnuje

⁽⁶⁾ Pracovní dokument útvarů Komise, průvodní dokument ke sdělení „Směrem k evropské strategii pro elektronické soudnictví (e-justice)“ určenému Radě, Evropskému parlamentu a Evropskému hospodářskému a sociálnímu výboru, souhrn posouzení dopadů, 30.5.2008, dokument SEK(2008) 1944.

⁽⁷⁾ Viz stanovisko evropského inspektora ochrany údajů o zřízení Evropského informačního systému rejstříků trestů (ECRIS) podle článku 11 rámcového rozhodnutí 2008/XX/SVV, dostupného na webové stránce EIOU, www.edps.europa.eu, pod hesly „consultation“ a poté „opinions“, „2008“.

množství otázek jako například projekty, které poskytují stranám v soudním sporu informace účinnějším způsobem. Spadá sem poskytování informací na internetu o soudnictví, zákonech a judikatuře, elektronické komunikační systémy spojující strany sporu a soudy a vytvoření plně elektronických řízení. Patří sem též evropské projekty jako například používání elektronických prostředků pro nahrávání jednání soudu a projekty zahrnující výměnu informací nebo propojování.

14. I když je tato působnost velice široká, EIOÚ zaznamenal, že informace budou poskytovány o trestní řízení a o občanském a obchodním soudnictví, ale ne o správním soudnictví. Spojení bude existovat s trestním a občanským atlasem, ale ne již se správním atlasem, ačkoli by pro občany a podniky mohlo být užitečné mít přístup ke správnímu soudnictví, tj. k správnímu řízení a řízení o stížnostech. Mělo by být též zprostředkováno spojení se Sdružením státních rad. Tyto dodatky by občanům mohly usnadnit orientaci ve spletné síti, již správní právo se všemi jeho soudy často je, a zajistit, aby byli lépe informovaní o systémech správního soudnictví.

15. Z těchto důvodů EIOÚ doporučuje zahrnout správní řízení do e-justice. Jako součást tohoto nového bodu by projekt e-justice měl zajistit větší viditelnost předpisů o ochraně údajů, stejně jako vnitrostátních orgánů pro ochranu údajů, zvláště ve vztahu k typům údajů zpracovávaných v rámci e-justice. Toto by bylo v souladu s tzv. „londýnskou iniciativou“, kterou úřady pro ochranu údajů zahájily v listopadu 2006 a jejímž cílem je „komunikovat o otázkách ochrany údajů a zvýšení její účinnosti.“

IV. NOVÉ RÁMCOVÉ ROZHODNUTÍ O OCHRANĚ ÚDAJŮ V RÁMCI POLICEJNÍ A JUSTIČNÍ SPOLUPRÁCE V TRESTNÍCH VĚCECH

16. Se zvýšenou výměnou osobních údajů mezi justičními orgány, kterou sdělení předpokládá, nabírá platná právní rámec pro ochranu údajů na důležitosti. V této souvislosti EIOÚ konstatuje, že Rada Evropské unie přijala dne 27. listopadu, tři roky po původním návrhu Komise, rámcové rozhodnutí o ochraně osobních údajů v rámci policejní a justiční spolupráce v trestních věcech⁽⁸⁾. Tento nový právní předpis poskytne vedle ustanovení na ochranu údajů směrnice 95/46/ES v „prvním pilíři“ obecný právní rámec pro ochranu údajů ve věcech „třetího pilíře.“

17. EIOÚ vítá tento právní nástroj jako první důležitý krok k ochraně údajů v rámci policejní a justiční spolupráce. Úroveň ochrany údajů dosažená v konečném znění však není plně uspokojivá. Rámcové rozhodnutí se především vztahuje pouze na policejní a soudní údaje vyměňované

mezi členskými státy, orgány a systémy EU, ale nezahrnuje vnitrostátní údaje. Přijaté rámcové rozhodnutí navíc nestanoví povinnost rozlišovat mezi různými kategoriemi subjektů údajů, jako jsou podezřelé osoby, pachatelé trestných činů, svědci a oběti, aby bylo zajištěno, že jejich údaje jsou zpracovávány s odpovídajícími zárukami. Rámcové rozhodnutí není plně konzistentní se směrnicí 95/46/ES, obzvláště s ohledem na omezení účelů, pro něž mohou být osobní údaje dále zpracovávány. Nestanoví ani nezávislou skupinu příslušných vnitrostátních orgánů a orgánů EU pro ochranu údajů, která by nejen zajistila lepší koordinaci mezi orgány pro ochranu údajů, ale i podstatně přispěla k jednotnému používání rámcového rozhodnutí.

18. Toto by znamenalo, že v situaci, kdy je vynakládáno mnoho úsilí na to, aby byly vytvořeny společné systémy přeshraniční výměny osobních údajů, stále existují odlišnosti v předpisech, podle kterých jsou v jednotlivých zemích EU údaje zpracovávány a na základě kterých mohou občané uplatňovat svá práva.

19. EIOÚ znovu připomíná, že vysoká úroveň ochrany údajů v oblasti policejní a justiční spolupráce, jakož i soulad se směrnicí 95/46/ES, představují nezbytnou součást dalších předložených či plánovaných opatření za účelem usnadnění přeshraniční výměny osobních údajů při vymáhání práva. Toto vyplývá nejen z práva občanů na respektování jejich základního práva na ochranu osobních údajů, ale také z potřeby donucovacích orgánů zajistit kvalitu vyměňovaných údajů, jak potvrzuje příloha ke sdělení ve vztahu k propojení rejstříků trestů, důvěru mezi orgány jednotlivých zemí a konečně též právní platnost důkazů nashromážděných v přeshraničním kontextu.

20. Proto EIOÚ vyzývá evropské instituce, aby tyto body vzaly zvláště v úvahu nejen při provádění opatření plánovaných ve sdělení, ale též s cílem začít co nejdříve uvažovat o dalších zlepšeních právního rámce pro ochranu údajů při vymáhání práva.

V. PROJEKTY E-JUSTICE

Nástroje e-justice na evropské úrovni

21. EIOÚ uznává, že výměna osobních údajů je nutnou součástí budování prostoru svobody, bezpečnosti a práva. Z tohoto důvodu EIOÚ podporuje návrh strategie e-justice, přičemž podtrhuje význam ochrany údajů v této souvislosti. Dodržování ochrany údajů je skutečně nejen právní

⁽⁸⁾ Dosud nepublikováno v Úředním věstníku.

povinností, ale též klíčovým prvkem úspěchu navrhovaných systémů, např. pro zajištění kvality výměny údajů. Totéž platí pro instituce a orgány, které zpracovávají osobní údaje při tvorbě nových politik. Předpisy a zásady je třeba používat a následovat v praxi a obzvláště by k nim mělo být přihlíženo při návrhu a budování informačních systémů. Soukromí a ochrana údajů jsou v podstatě „klíčovými faktory úspěchu“ pro prosperující a vyváženou informační společnost. Je tedy rozumné do nich investovat a udělat to co nejdříve.

22. V této souvislosti EIOÚ zdůrazňuje, že sdělení nepředpokládá vytvoření centrální evropské databáze. Vítá volbu decentralizovaných struktur. EIOÚ údajů připomíná, že zaujal stanovisko k systému ECRIS⁽⁹⁾ a k průmskému podnětu⁽¹⁰⁾. Ve stanovisku o ECRIS evropský inspektor ochrany údajů poznamenal, že decentralizované struktury brání dodatečné duplicitě osobních údajů v centrální databázi. Ve stanovisku k „průmskému podnětu“ doporučil vzít řádně v úvahu rozsah systému při diskusích o propojení databází. Zejména by měly být stanoveny konkrétní formáty pro předávání údajů, jako např. prostřednictvím internetu podané žádosti o výpis z rejstříku trestů, které zohledňují též jazykové rozdíly, a přesnost výměn údajů by měla být neustále monitorována. Tyto body by měly být vzaty v úvahu také v souvislosti s iniciativami, které vyplývají ze strategie e-justice.

23. Evropská komise zamýšlí přispět k posílení a rozvoji nástrojů e-justice na evropské úrovni v úzké spolupráci s členskými státy a ostatními partnery. Podporuje úsilí členských států a sama má v úmyslu vypracovat řadu počítačových nástrojů ke zvýšení interoperability systémů, usnadnění přístupu občanů ke spravedlnosti a komunikace mezi justičními orgány a s cílem dosáhnout podstatných úspor z rozsahu na evropské úrovni. Pokud jde o interoperabilitu programových vybavení používaných členskými státy, ne všechny členské státy musí nezbytně používat stejné programové vybavení – ačkoli by toto byla nepraktičtější varianta – programová vybavení však musí být zcela interoperabilní.

24. EIOÚ doporučuje, aby byla v souvislosti s propojením a interoperabilitou systémů řádně vzata v úvahu zásada

omezení účelu a aby tyto systémy byly vytvářeny v rámci norem pro ochranu údajů (zásada „soukromí coby aspekt návrhu“). Jakákoli forma interakce mezi dvěma odlišnými systémy by měla být důkladně zdokumentována. Interoperabilita by nikdy neměla vést k tomu, aby orgán, kterému není povolen přístup k určitým údajům nebo jejich použití, mohl tento přístup získat prostřednictvím jiného informačního systému. EIOÚ by chtěl znovu zdůraznit, že interoperabilita by nikdy neměla sama o sobě ospravedlnit obcházení zásady omezení účelu⁽¹¹⁾.

25. Kromě toho další zásadní bod spočívá v zajištění, aby rozšířená přeshraniční výměna osobních údajů byla doprovázena zvýšeným dozorem a zvýšenou spoluprací orgánů pro ochranu údajů. EIOÚ již zdůraznil ve svém stanovisku ze dne 29. května 2006 týkajícím se rámcového rozhodnutí o výměně informací z rejstříků trestů⁽¹²⁾, že návrh rámcového rozhodnutí by se měl věnovat nejen spolupráci mezi ústředními orgány, ale i spolupráci mezi jednotlivými příslušnými orgány pro ochranu údajů. Tato potřeba je stále naléhavější vzhledem k tomu, že jednání o nedávno přijatém rámcovém rozhodnutí o ochraně osobních údajů zpracovávaných v rámci policejní a justiční spolupráce⁽¹³⁾ vedla k vypuštění ustanovení, které zřizovalo pracovní skupinu sdružující orgány EU pro ochranu údajů, jejíž úkolem měla být koordinace jejich činností v souvislosti se zpracováním údajů v rámci policejní a justiční spolupráce v trestních věcech. V zájmu zajištění účinného dohledu a zároveň vysoké kvality přeshraničního pohybu údajů pocházejících z rejstříků trestů by proto bylo potřebné vytvořit mechanismy účinné koordinace mezi příslušnými orgány pro ochranu údajů⁽¹⁴⁾. Tyto mechanismy by měly rovněž zohlednit skutečnost, že dohled nad infrastrukturou sítě s-TESTA spadá do pravomoci EIOÚ⁽¹⁵⁾. Nástroje e-justice mohou podpořit tyto mechanismy, které by mohly být vyvinuty v úzké spolupráci s orgány pro ochranu údajů.

26. Komise upozorňuje v bodě 4.2.1, že pro výměnu údajů z rejstříků trestů bude důležité, aby přesáhla rámec justiční spolupráce, aby bylo možné začlenit další cíle, např. přístup k určitým pozicím. EIOÚ zdůrazňuje, že jakékoli zpracovávání osobních údajů pro jiné účely, než pro které

⁽⁹⁾ Viz poznámka pod čarou č. 4, bod 18.

⁽¹⁰⁾ Úř. věst. C 89, 10.4.2008, s. 4.

⁽¹¹⁾ Úř. věst. C 91, 19.4.2006, s. 53. Viz též připomínky EIOÚ ke sdělení Komise o interoperabilitě evropských databází, Brusel 10.3.2006.

⁽¹²⁾ Úř. věst. C 91, 26.4.2007, s. 9.

⁽¹³⁾ Viz výše, kapitola IV.

⁽¹⁴⁾ Viz stanovisko EIOÚ k systému ECRIS, body 8, 37 a 38.

⁽¹⁵⁾ K této otázce viz níže body 27 a 28.

byly shromážděny, by mělo respektovat zvláštní podmínky stanovené v platných předpisech na ochranu údajů. Zejména by zpracovávání osobních údajů pro jiné účely mělo být dovoleno, jen pokud je to nezbytné pro dosažení cílů uvedených v předpisech Společenství na ochranu údajů ⁽¹⁶⁾ a pokud jsou stanoveny legislativními opatřeními.

27. Sdělení v souvislosti s propojením rejstříků trestů uvádí, že jako součást příprav ke vstupu rámcového rozhodnutí o výměně informací z rejstříků trestů v platnost Komise zahájí dvě studie proveditelnosti s cílem organizovat další vývoj projektu a rozšířit výměnu údajů tak, že bude zahrnovat i údaje o příslušnících třetích zemí odsouzených za trestné činy. V roce 2009 dá Komise členským státům k dispozici programové vybavení s cílem umožnit, aby výměna informací mohla v krátkém časovém intervalu probíhat mezi všemi rejstříky trestů. Tento referenční systém použitý k výměně informací v kombinaci se systémem s-TESTA umožní realizovat úspory z rozsahu tím, že členské státy nebudou muset pracovat na vývoji vlastních programů samostatně. Navíc zjednoduší fungování projektu.
28. V této souvislosti EIOÚ vítá používání infrastruktury s-TESTA, která se osvědčila jako spolehlivý systém pro výměnu údajů, a doporučuje, aby byly podrobně vymezeny statistické prvky ve vztahu k plánovaným systémům výměny údajů a aby byla řádně zohledněna potřeba zajištění dohledu nad ochranou údajů. Statistické údaje mohou například vysloveně zahrnovat prvky, jako je počet žádostí o přístup či opravu osobních údajů, délka a úplnost procesu aktualizace, druh osob, které mají přístup k těmto údajům, jakož i případy porušení bezpečnostních opatření. Kromě toho by statistické údaje a zprávy založené na těchto údajích měly být plně dostupné orgánům příslušným k ochraně údajů.

Strojový překlad a databáze překladatelů

29. Používání strojového překladu je užitečným nástrojem a může přispět k vzájemnému porozumění mezi příslušnými aktéry v členských státech. Strojový překlad by však neměl vést ke snížení kvality vyměňovaných informací, obzvláště pokud jsou tyto informace používány jako podklady pro rozhodnutí, která mají pro dotyčné osoby právní důsledky. EIOÚ poukazuje na to, že je důležité jasně stanovit a vymezit použití strojových překladů. Použití strojového překladu pro účely přenosu informací, které nebyly přesně předloženy, jako například dodatečných poznámek či upřesnění doplněných v jednotlivých případech, může mít vliv na kvalitu přenesených informací – a tím na rozhodnutí přijaté na jejich základě – a mělo by být v zásadě vyloučeno ⁽¹⁷⁾. EIOÚ navrhuje vzít toto dpo-

ručení v úvahu při přijímání opatření vyplývajících ze sdělení.

30. Sdělení usiluje o vytvoření databáze soudních předkladatelů a tlumočnicků, aby došlo ke zlepšení kvality soudních překladů a tlumočení. EIOÚ podporuje tento cíl, ale připomíná, že se na tuto databázi budou vztahovat příslušné právní normy pro ochranu údajů. Zejména pokud by databáze obsahovala údaje o hodnocení výkonu překladatelů, mohly by příslušné orgány pro ochranu údajů provádět předběžnou kontrolu.

Akční plán pro evropskou e-justici

31. V bodě 5 sdělení upozorňuje na to, že je nutné jasně rozdělit odpovědnost mezi Komisi, členské státy a další aktéry zapojené do justiční spolupráce. Komise se ujme všeobecné role koordinátora a bude podporovat výměnu osvědčených postupů a pracovat na konceptu portálu e-justice, který zprovozní, a bude koordinovat informace na něm umístěné. Kromě toho bude Komise pokračovat v práci na propojení rejstříků trestů a zůstane nadále přímo odpovědná za soudní síť pro věci občanské a bude i nadále podporovat soudní síť pro věci trestní. Členské státy budou muset aktualizovat informace o svých soudních systémech umístěné na webové stránce e-justice. Dalšími aktéry jsou soudní síť pro věci občanské a pro věci trestní a Eurojust. Budou pracovat na nástrojích, které jsou nezbytné pro účinnější justiční spolupráci, obzvláště na nástrojích pro strojový překlad a na bezpečném systému výměny, v úzké spolupráci s Komisí. Návrh akčního plánu a časový rozvrh různých projektů je uveden v příloze ke sdělení.
32. V této souvislosti EIOÚ zdůrazňuje, že na jedné straně se v systému ECRIS nevytváří žádná centrální evropská databáze a nepředpokládá se přímý přístup do databází jiných členských států, které obsahují záznamy z rejstříku trestů, zatímco na druhé straně je na vnitrostátní úrovni odpovědnost za správnost informací soustředěna v rukách ústředních orgánů členských států. V rámci tohoto mechanismu nesou členské státy odpovědnost za provoz vnitrostátních databází a za účinné provádění výměn. Není jasné, zda nesou odpovědnost za propojovací programové vybavení či nikoliv. Komise poskytne členským státům k dispozici programové vybavení s cílem umožnit, aby výměna informací mohla v krátkém časovém intervalu probíhat mezi všemi rejstříky trestů. Tento referenční systém se bude pro výměnu informací používat v kombinaci se systémem s-TESTA.
33. EIOÚ chápe, že v souvislosti s podobnými iniciativami e-justice mohou být zaváděny podobné systémy a Komise ponese odpovědnost za společnou infrastrukturu, ačkoli to

⁽¹⁶⁾ Viz zejména článek 13 směrnice 95/46 a článek 20 nařízení (ES) č. 45/2001.

⁽¹⁷⁾ Viz body 39 a 40 stanoviska EIOÚ k systému ECRIS.

není upřesněné ve sdělení. EIOÚ navrhuje z důvodu právní jistoty upřesnit tuto odpovědnost v opatřeních vycházejících ze sdělení.

Projekty e-justice

34. Příloha uvádí skupinu projektů, na kterých se bude pracovat v příštích pěti letech. První projekt, vytvoření internetových stránek e-justice, se týká portálu e-justice. Tento úkol vyžaduje studii proveditelnosti a vytvoření portálu. Dále je potřebné zavedení metod řízení a zveřejnění informací ve všech jazycích EU na internetu. Druhý a třetí projekt se týká propojování rejstříků trestů. Druhý projekt se týká propojování vnitrostátních rejstříků trestů. Třetí projekt předpokládá vytvoření evropského rejstříku odsouzených příslušníků třetích zemí na základě studie proveditelnosti a legislativního návrhu. EIOÚ konstatuje, že posledně zmíněný projekt již není uveden v pracovním programu Komise, a klade si otázku, zda to znamená změnu v plánovaných projektech Komise nebo pouhé odložení tohoto konkrétního projektu.
35. Sdělení také uvádí tři projekty v oblasti elektronické výměny a tři projekty týkající se podpory překladu. Bude zahájen pilotní projekt postupného sestavení mnohojazyčného komparativního právního slovníku. Další projekty se vztahují k vytvoření dynamických formulářů doplňujících evropské právní předpisy či na použití videokonference justičními orgány. Kromě toho se v rámci fór e-justice budou konat roční jednání o tématech e-justice a bude se rozvíjet odborná příprava právnických profesí v oblasti justiční spolupráce. EIOÚ doporučuje, aby tato jednání a odborná příprava dostatečně zohledňovaly právní předpisy a praxi v oblasti ochrany údajů.
36. Příloha tedy předpokládá vypracování široké řady evropských nástrojů s cílem usnadnit výměnu informací mezi aktéry v jednotlivých členských státech. Důležitou roli mezi těmito nástroji bude hrát portál e-justice, za který ponese odpovědnost převážně Komise.
37. Mnoha těmto nástrojům bude společné to, že informace a osobní údaje budou vyměňovány a spravovány aktéry na vnitrostátní i evropské úrovni, na něž se vztahují povinnosti ochrany údajů a kteří jsou podřízeni orgánům dozoru zřízeným na základě směrnice 95/46/ES nebo nařízení č. 45/2001. Jak již EIOÚ vysvětlil ve svém stanovisku týka-

jícím se systému pro výměnu informací o vnitřním trhu (IMI) ⁽¹⁸⁾, je v této souvislosti nezbytné zajistit, aby povinnosti spojené s dodržováním předpisů na ochranu údajů byly plněny účinně a hladce.

38. Za tímto účelem je v podstatě nutné jednak, aby byla jasně vymezena a rozdělena odpovědnost za zpracovávání osobních údajů v rámci těchto systémů, a jednak aby byly, kdykoli je to nutné, stanoveny vhodné koordinační mechanismy – zejména ve vztahu k doзору.
39. Použití nových technologií je jedním ze základních pilířů iniciativ souvisejících s e-justicí. Propojení vnitrostátních rejstříků, vytvoření elektronického podpisu, bezpečné sítě, virtuální platformy pro výměnu a rozšířené použití videokonference budou v příštích letech představovat základní prvky iniciativ v oblasti e-justice.
40. V této souvislosti je nezbytné, aby byla problematika ochrany údajů zohledněna v co možná nejranější fázi a aby byla začleněna do struktury zamýšlených nástrojů. Obzvláště důležitá je struktura systému a také zavedení vhodných bezpečnostních opatření. Tento přístup založený na zásadě „soukromí coby aspekt návrhu“ by příslušným iniciativám spojeným s e-justicí dovolil zajišťovat účinnou správu osobních údajů a zároveň by byl zárukou souladu se zásadami na ochranu údajů a bezpečnosti při výměně údajů mezi různými orgány.
41. EIOÚ dále upozorňuje, že technologické nástroje by měly být používány nejen k zajištění výměny informací, ale také k posílení práv zúčastněných osob. V tomto ohledu EIOÚ ve sdělení vítá zmínku o možnosti občanů žádat o výpis z rejstříku trestů prostřednictvím internetu a v jazyce, který si zvolí ⁽¹⁹⁾. Ve vztahu k této otázce EIOÚ připomíná, že ve svém stanovisku k návrhu Komise o výměně informací z rejstříků trestů uvítal, že dotyčná osoba může žádat o informace z rejstříku trestů, které se jí týkají, u ústředního orgánu členského státu, za předpokladu, že se jedná o osobu, která má či měla bydliště na území dožádaného nebo žádajícího členského státu a nebo je či byla jeho státním příslušníkem. Myšlenku využít jako jedno správní místo orgán, který je blíže zúčastněné osobě, vyjádřil EIOÚ též v oblasti koordinace systémů sociálního

⁽¹⁸⁾ Úř. věst. C 270, 25.10.2008, s. 1.

⁽¹⁹⁾ Viz strana 6 sdělení.

zabezpečení. EIOÚ tudíž vyzývá Komisi, aby pokračovala stejným směrem dále a posílila technologické nástroje, a zejména přístup na internet, aby tak občanům umožnila lépe nakládat s jejich osobními údaji, i pokud se pohybují mezi různými členskými státy.

VI. ZÁVĚRY

42. EIOÚ podporuje současný návrh na zřízení e-justice a doporučuje zohlednit připomínky uvedené v tomto stanovisku, mezi něž patří:

- vzít v úvahu nové rámcové rozhodnutí o ochraně osobních údajů v rámci policejní a justiční spolupráce v trestních věcech – včetně jeho nedostatků – nejen při provádění opatření zamýšlených ve sdělení, ale též s cílem začít co nejdříve uvažovat o dalším zlepšení právního rámce pro ochranu údajů při vynucování práva;
- zahrnout správní řízení do e-justice; jako součást tohoto nového bodu, by projekt e-justice měl zajistit větší viditelnost předpisů o ochraně údajů i vnitrostátních orgánů pro ochranu údajů, zvláště s ohledem na typy údajů zpracovávané v rámci projektů e-justice;
- nadále upřednostňovat decentralizované struktury;
- vzít v souvislosti s propojením a interoperabilitou systémů řádně v úvahu zásadu omezení účelu;

- jasně rozdělit odpovědnost mezi všechny aktéry, kteří zpracovávají osobní údaje v rámci plánovaných systémů, a vytvořit mechanismy účinné koordinace mezi příslušnými orgány pro ochranu údajů;
- zajistit, aby zpracovávání osobních údajů pro jiné účely, než pro které byly shromážděny, respektovalo zvláštní podmínky stanovené v platných předpisech na ochranu údajů;
- jasně stanovit a vymezit použití strojových překladů, aby napomáhalo vzájemnému pochopení trestných činů a neovlivňovalo kvalitu přenesených údajů;
- vyjasnit odpovědnost Komise za společné infrastruktury, například za systém s-TESTA;
- v souvislosti s použitím nových technologií zajistit, aby problematika ochrany údajů byla zohledněna v co možná nejranější fázi (zásada „soukromí coby aspekt návrhu“) a zároveň posílit technologické nástroje, které občanům umožní lépe nakládat s jejich osobními údaji, i pokud se pohybují mezi různými členskými státy.

V Bruselu dne 19. prosince 2008.

Peter HUSTINX
evropský inspektor ochrany údajů

Návrh stanoviska evropského inspektora ochrany údajů k návrhu směrnice Evropského parlamentu a Rady o uplatňování práv pacientů v přeshraniční zdravotní péči

(2009/C 128/03)

EVROPSKÝ INSPEKTOR OCHRANY ÚDAJŮ,

s ohledem na Smlouvu o založení Evropského společenství, a zejména na článek 286 této smlouvy,

s ohledem na Listinu základních práv Evropské unie, a zejména na článek 8 této listiny,

s ohledem na směrnici Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů,

s ohledem na 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, a zejména na článek 41 tohoto nařízení,

s ohledem na žádost o stanovisko v souladu s čl. 28 odst. 2 nařízení (ES) č. 45/2001, která byla evropskému inspektorovi ochrany údajů zaslána dne 2. července 2008,

PŘIJAL TOTO STANOVISKO:

I. ÚVOD

Návrh směrnice o uplatňování práv pacientů v přeshraniční zdravotní péči

1. Dne 2. července 2008 přijala Komise návrh směrnice Evropského parlamentu a Rady o uplatňování práv pacientů v přeshraniční zdravotní péči (nadále pouze návrh) ⁽¹⁾. Návrh zaslala Komise evropskému inspektorovi ochrany údajů ke konzultaci v souladu s čl. 28 odst. 2 nařízení (ES) č. 45/2001.

2. Cílem tohoto návrhu je stanovit rámec Společenství pro poskytování přeshraniční zdravotní péče v EU pro případy, kdy je péče, kterou pacienti vyhledávají, poskytována v jiném členském státě, než je domovská země pacienta. To se týká tří hlavních oblastí:

⁽¹⁾ KOM(2008) 414 v konečném znění. Vezměte prosím na vědomí, že ve stejný den bylo přijato rovněž doplňující sdělení o rámci Společenství pro uplatňování práv pacientů v přeshraniční zdravotní péči (KOM(2008) 415 v konečném znění). Jelikož je však toto sdělení pouze dosti obecné, evropský inspektor ochrany údajů se rozhodl, že se zaměří na navrhovanou směrnici.

— stanovení společných zásad ve všech zdravotních systémech EU, které jasné určí povinnosti členských států;

— vytvoření konkrétního rámce pro přeshraniční zdravotní péči, který vyjasní práva pacientů na poskytnutí zdravotní péče v jiném členském státě;

— podpora spolupráce EU v oblasti zdravotní péče, například uznávání předpisů vystavených v jiných zemích, evropské referenční sítě, hodnocení zdravotnických technologií, sběr údajů, kvalita a bezpečnost.

3. Cíle tohoto rámce jsou dva: dostatečně vyjasnit otázku práv týkajících se náhrady nákladů za zdravotní péči poskytnutou v jiných členských státech a zajistit, aby v případě přeshraniční péče byly dodržovány nezbytné požadavky na kvalitní, bezpečnou a účinnou zdravotní péči.

4. Uplatňování systému přeshraniční zdravotní péče vyžaduje výměnu příslušných osobních údajů týkajících se zdravotního stavu (nadále jen „údaje o zdravotním stavu“) pacientů mezi pověřenými organizacemi a zdravotníky různých členských států. Tyto údaje jsou považovány za důvěrné a vztahují se na ně přísnější pravidla ochrany údajů, jak stanoví článek 8 směrnice 95/46/ES o zvláštních kategoriích údajů.

Konzultace s evropským inspektorem ochrany údajů

5. Evropský inspektor ochrany údajů vítá, že je v této otázce konzultován a že odkaz na tuto konzultaci je uveden v preambuli návrhu, v souladu s článkem 28 nařízení (ES) č. 45/2001.

6. Je to poprvé, co byl evropský inspektor ochrany údajů formálně konzultován ohledně návrhu směrnice v oblasti zdravotní péče. V tomto stanovisku jsou tudíž některé poznámky pojaty širěji a týkají se obecných otázek ochrany osobních údajů v odvětví zdravotnictví, což by se mohlo týkat rovněž dalších příslušných právních nástrojů (závazných i nezávazných).

7. Hned zpočátku by chtěl evropský inspektor ochrany údajů vyjádřit podporu iniciativám zaměřeným na zlepšování podmínek pro přeshraniční zdravotní péči. Tento návrh je třeba ve skutečnosti vidět v souvislosti s celkovým programem ES zaměřeným na zlepšování zdraví občanů v informační společnosti. Dalšími iniciativami v tomto směru jsou Komisí připravované směrnice a sdělení o dárcovství lidských orgánů a o transplantacích ⁽¹⁾, doporučení o interoperabilitě elektronických zdravotních záznamů ⁽²⁾, jakož i plánované sdělení o telemedicině ⁽³⁾. Evropský inspektor ochrany údajů je však znepokojen tím, že všechny tyto související iniciativy nejsou těsně provázané nebo propojené v oblasti bezpečnosti soukromí a údajů, takže brání přijetí jednotného přístupu k ochraně údajů v oblasti zdravotní péče, zejména pokud jde o využívání nových informačních a komunikačních technologií. Jako příklad uveďme, že ačkoli je telemedicina výslovně uvedena v 10. bodě odůvodnění navrhované směrnice, není ve stávajícím návrhu uveden žádný odkaz na příslušný aspekt sdělení ES týkající se ochrany údajů. Ačkoli jsou elektronické zdravotní záznamy jedním z možných způsobů předávání údajů o zdravotním stavu do zahraničí, není tu navíc uveden žádný odkaz na otázky ochrany soukromí, jimiž se zabývá příslušné doporučení Komise. ⁽⁴⁾ To vzbuzuje dojem, že celkové pojetí otázky ochrany soukromí v oblasti zdravotní péče dosud není jasně definováno a v některých případech zcela chybí.

8. To je rovněž patrné ze stávajícího návrhu, u něhož evropský inspektor ochrany údajů bohužel shledává, že se konkrétně neřeší otázky související s ochranou údajů. Odkazy na ochranu údajů je v něm samozřejmě možno nalézt, ale jsou převážně všeobecné povahy a odpovídajícím způsobem neodrážejí konkrétní potřeby v oblasti soukromí a požadavky přeshraniční zdravotní péče.

9. Evropský inspektor ochrany údajů by rád zdůraznil, že jednotný a spolehlivý přístup k ochraně údajů ve všech navrhovaných nástrojích zdravotní péče nejenže zajistí základní právo občanů na ochranu údajů, ale rovněž přispěje k dalšímu rozvoji přeshraniční zdravotní péče v EU.

II. OCHRANA ÚDAJŮ V OBLASTI PŘESHRANIČNÍ ZDRAVOTNÍ PÉČE

Obecné souvislosti

10. Nejdůležitějším cílem Evropského společenství bylo vytvoření vnitřního trhu jakožto oblasti bez vnitřních hranic, v níž je zajištěn volný pohyb zboží, osob, služeb

a kapitálu. Tím, že se občanům umožnilo snadněji se stěhovat do jiných členských států, než ze kterých pocházejí, a usazovat se v nich, samozřejmě vyvstaly otázky týkající se zdravotní péče. Z toho důvodu se v devadesátých letech musel Soudní dvůr v souvislosti s vnitřním trhem zabývat otázkami možné úhrady zdravotních nákladů vzniklých v jiném členském státě. Soudní dvůr uznal, že svoboda poskytovat služby, jak je stanovena v článku 49 Smlouvy o ES, zahrnuje rovněž svobodu osob vycestovat do jiného členského státu, aby tam vyhledali lékařskou péči ⁽⁵⁾. V důsledku toho se k pacientům, kteří měli zájem o přeshraniční zdravotní péči, už nemohlo přistupovat jinak než ke státním příslušníkům v jejich zemi původu, kterým se dostalo stejné lékařské péče, aniž by překročili hranice.

11. Tato rozhodnutí Soudního dvora jsou nyní jádrem stávajícího návrhu. Jelikož je judikatura Soudního dvora založena na jednotlivých případech, je záměrem stávajícího návrhu zlepšit srozumitelnost, aby se tak zajistilo obecnější a účinnější uplatňování svobody při využívání a poskytování zdravotnických služeb. Jak už však bylo uvedeno, návrh je rovněž součástí ambicióznějšího programu, jehož cílem je zlepšit zdraví občanů v informační společnosti, kdy EU vidí velké možnosti pro zkvalitnění přeshraniční zdravotní péče prostřednictvím využívání informační technologie.

12. Stanovení pravidel přeshraniční zdravotní péče je ze zřejmých důvodů choulostivou otázkou. Dotýká se totiž citlivé oblasti, v níž si členské státy stanovily odlišné vnitrostátní systémy, například systémy pojištění a úhrady nákladů, nebo systémy organizace infrastruktury zdravotní péče včetně informačních sítí a aplikací v oblasti zdravotní péče. Ačkoli se normotvůrce Společenství ve stávajícím návrhu soustředí pouze na přeshraniční zdravotní péči, tato pravidla přinejmenším ovlivní způsob organizování systémů vnitrostátní zdravotní péče.

13. Zlepšení podmínek přeshraniční zdravotní péče bude ku prospěchu občanů. Zároveň však pro ně bude v sobě obsahovat určitá rizika. Je třeba vyřešit mnoho praktických problémů, které souvisí s přeshraniční spoluprací mezi lidmi z různých zemí hovořícími různými jazyky. Jelikož dobrý zdravotní stav je pro každého občana velice důležitý, je třeba eliminovat veškerá rizika spojená se špatnou komunikací vedoucí k nepřesnostem. Je samozřejmé, že posílení přeshraniční zdravotní péče spolu s využíváním moderní informační technologie má značné důsledky pro

⁽¹⁾ Oznámeny v pracovním programu Komise.

⁽²⁾ Doporučení Komise ze dne 2. července 2008 o přeshraniční interoperabilitě systémů elektronických zdravotních záznamů (oznámeno pod číslem dokumentu K(2008) 3282), Úř. věst. L 190, 18.7.2008, s. 37.

⁽³⁾ Oznámeno v pracovním programu Komise.

⁽⁴⁾ To je názorně doloženo i tím, že ochrana soukromí nebo údajů není zmíněna ve sdělení uvedeném v poznámce pod čarou č. 1, ačkoli jeho cílem je stanovit rámec Společenství pro uplatňování práv pacientů v přeshraniční zdravotní péči.

⁽⁵⁾ Viz věc 158/96, *Kohll*, Sb. rozh. 1998, s. I-1931, bod 34. Viz mimo jiné rovněž věc C-157/99, *Smits and Peerbooms*, Sb. rozh. 2001, s. I-5473 a věc C-385/99, *Müller-Fauré and Van Riet*, Sb. rozh. 2003, s. I-12403.

ochranu osobních údajů. Účinnější, a tudíž častější výměna údajů o zdravotním stavu, větší vzdálenost mezi osobami a příslušnými instancemi, rozdílné vnitrostátní právní předpisy uplatňující pravidla ochrany údajů, to všechno vede k otázkám týkajícím se bezpečnosti údajů a právní jistoty.

Ochrana údajů o zdravotním stavu

14. Je třeba zdůraznit, že údaje o zdravotním stavu jsou považovány za zvláštní kategorii údajů, která si zasluhuje vyšší stupeň ochrany. Jak nedávno v souvislosti s článkem 8 Evropské úmluvy o ochraně lidských práv uvedl Evropský soud pro lidská práva: „Ochrana osobních údajů, zejména zdravotních údajů, má zásadní význam pro to, aby člověk mohl využívat svého práva na respektování soukromého a rodinného života, jak je zaručuje článek 8 uvedené úmluvy“⁽¹⁾. Předtím, než budou vysvětlena přísnější pravidla zpracovávání údajů o zdravotním stavu stanovená ve směrnici 95/46/ES, věnujeme pár slov pojmu „údaje o zdravotním stavu“.
15. Směrnice 95/46/ES neobsahuje výslovné vymezení údajů o zdravotním stavu. Běžně se používá širší interpretace, kdy se údaje o zdravotním stavu často definují jako „osobní údaje, které mají jasnou a těsnou souvislost s popisem zdravotního stavu člověka“⁽²⁾. V tomto smyslu údaje o zdravotním stavu obvykle zahrnují zdravotní údaje (např. lékařská doporučení a předpisy, lékařské nálezy, laboratorní testy, rentgenové snímky atd.), jakož i správní a finanční údaje související se zdravotním stavem (např. doklady o hospitalizacích, číslo sociálního pojištění, rozpis lékařských vyšetření, faktury za poskytnutí zdravotní péče atd.). Je třeba uvést, že pojem „zdravotní údaje“⁽³⁾ se používá někdy také pro údaje týkající se zdraví, stejně jako „údaje o zdravotní péči“⁽⁴⁾. V celém tomto stanovisku se bude používat pojem „údaje o zdravotním stavu“.
16. Užitečnou definici „údajů o zdravotním stavu“ nabízí norma ISO 27799: „veškeré informace týkající se zdravotního nebo mentálního zdraví jednotlivce nebo poskytování zdravotních služeb jednotlivci, k nimž mohou patřit: a) informace o registraci jednotlivců k poskytnutí zdravotních služeb; b) informace o platbách nebo způsobilosti pro zdravotní péči s ohledem na jednotlivce; c) číslo, symbol nebo jiný kód přidělený jednotlivci pro jeho jednoznačnou identifikaci ke zdravotním účelům; d) jakékoli informace o jednotlivci shromážděné v průběhu poskytování zdravot-

ních služeb tomuto jednotlivci; e) informace získané na základě testování nebo vyšetření částí těla nebo biologického materiálu; a f) identifikace osoby (zdravotníka) jakožto poskytovatele zdravotnické služby jednotlivci“.

17. Evropský inspektor ochrany údajů v souvislosti se stávajícím návrhem velmi podporuje přijetí konkrétní definice pojmu „údaje o zdravotním stavu“, kterou by bylo možné využít rovněž v budoucnosti u dalších příslušných právních textů ES (viz níže uvedený oddíl III).
18. Článek 8 směrnice 95/46/ES stanoví pravidla zpracovávání zvláštních kategorií údajů. Tato pravidla jsou přísnější než pravidla zpracovávání jiných údajů stanovená v článku 7 směrnice 95/46/ES. To je již patrné, když čl. 8 odst. 1 výslovně uvádí, že členský stát zakáže mimo jiné i zpracování údajů týkajících se zdraví. V následujících odstavcích uvedeného článku je stanoveno několik výjimek z tohoto zákazu, ale ty jsou specifitější než důvody pro zpracovávání běžných údajů uvedených v článku 7. Zákaz například neplatí, pokud subjekt údajů udělil výslovný souhlas (čl. 8 odst. 2 písm. a)), na rozdíl od nezpochybnitelného souhlasu požadovaného v čl. 7 písm. a) směrnice 95/46/ES. Právní předpisy členských států mohou navíc stanovit, že v určitých případech nepřestává zákaz platit ani se souhlasem subjektu údajů. Třetí odstavec článku 8 je věnován pouze zpracovávání údajů týkajících se zdravotního stavu. Podle tohoto odstavce zákaz uvedený v prvním odstavci neplatí, je-li zpracování údajů nezbytné pro účely zdravotní prevence, lékařských diagnóz, lékařské péče a ošetřování nebo správy zdravotnických služeb a pokud tyto údaje zpracovává odborný zdravotnický pracovník, který je na základě vnitrostátního práva nebo právních předpisů přijatých příslušnými vnitrostátními orgány vázán povinností zachovávat profesní tajemství, nebo jiná osoba rovněž podléhající obdobné povinnosti mlčenlivosti.
19. Článek 8 směrnice 95/46/ES klade velký důraz na skutečnost, že by členské státy měly zajistit vhodná a odpovídající ochranná opatření. Čl. 8 odst. 4 například členským státům umožňuje z důvodu významného veřejného zájmu stanovit i jiné výjimky ze zákazu zpracovávání důvěrných údajů, ale s výhradou poskytnutí vhodných ochranných opatření. Tato skutečnost obecným způsobem zdůrazňuje odpovědnost členských států za to, aby věnovaly zvláštní pozornost zpracovávání důvěrných údajů, například údajů týkajících se zdravotního stavu.

Ochrana údajů o zdravotním stavu v případech přeshraniční péče *Sdílená odpovědnost členských států*

20. Členské státy měly by si být uvedené odpovědnosti vědomy zejména v případech, kdy se jedná o otázku přeshraniční výměny údajů o zdravotním stavu. Jak již bylo uvedeno, zvyšuje přeshraniční výměna údajů o zdravotním stavu, riziko nepřesného nebo nezákonného

⁽¹⁾ Viz Evropský soud pro lidská práva dne 17. července 2008, *I v. Finsko* (žádost č. 20511/03) bod 38.

⁽²⁾ Viz Pracovní skupina článku 29, pracovní dokument věnovaný zpracovávání osobních údajů týkajících se zdraví v elektronických zdravotních záznamech, únor roku 2007, WP 131, odstavec II.2. Viz rovněž široký pojem „osobních údajů“: Pracovní skupina článku 29, stanovisko 4/2007 o pojetí osobních údajů, WP 136.

⁽³⁾ Rada Evropy, doporučení č. R(97)5 o ochraně zdravotních údajů.

⁽⁴⁾ ISO 27799:2008 „Zdravotnická informatika – Použití ISO/IEC 272002 pro management bezpečnosti informací ve zdravotnictví“.

zpracování údajů. To může mít pro subjekt údajů samozřejmě nedozírné negativní důsledky. Do tohoto procesu je zapojen jak členský stát, v němž je pacient pojištěn, tak i členský stát, v němž je poskytována léčba, a proto tuto odpovědnost sdílejí.

21. Bezpečnost údajů o zdravotním stavu je v této souvislosti důležitým problémem. Ve výše citovaném případě z nedávné doby kladl Evropský soud pro lidská práva zvláštní důraz na důvěrnost údajů o zdravotním stavu: „Zachovávání důvěrnosti údajů o zdravotním stavu je v právních systémech všech smluvních stran úmluvy velmi důležitou zásadou. Je nesmírně důležité nejen dodržovat pocit soukromí pacienta, ale rovněž udržet si jeho důvěru v lékařskou a zdravotnickou profesi a ve zdravotnické služby obecně“⁽¹⁾.
22. Pravidla ochrany údajů stanovená ve směrnici 95/46/ES dále vyžadují, aby členský stát, v němž je pacient pojištěn, poskytl pacientovi odpovídající, správné a aktuální informace o předávání jeho osobních údajů do jiného členského státu a zajistil bezpečné předávání údajů tomuto členskému státu. Členský stát, v němž je poskytována léčba, by měl rovněž zajistit bezpečné převzetí těchto údajů a poskytnout přiměřenou úroveň ochrany při vlastním zpracování údajů podle svých vnitrostátních právních předpisů týkajících se ochrany údajů.
23. Evropský inspektor ochrany údajů by si přál, aby se v tomto návrhu jasně stanovilo rozdělení odpovědnosti členských států, rovněž s ohledem na elektronický přenos údajů, zejména v souvislosti s novými aplikacemi informačních a komunikačních technologií, jak je podrobněji uvedeno níže.

Elektronické předávání údajů o zdravotním stavu

24. Ke zlepšování přeshraniční výměny údajů o zdravotním stavu slouží především používání informačních technologií. Ačkoli se výměna údajů v rámci systému přeshraniční zdravotní péče může stále uskutečňovat v papírové formě (tzn. pacient se přestěhuje do jiného členského státu a vezme si s sebou všechny své příslušné údaje o zdravotním stavu, jako jsou laboratorní vyšetření, doporučení lékaře atd.), je patrný jasný trend směrem k náhradě elektronickými prostředky. Elektronické oznamování údajů o zdravotním stavu bude podporováno informačními systémy pro účely zdravotní péče zavedenými (anebo systémy, které budou zavedeny) v členských státech (v nemocnicích, na klinikách atd.), jakož i používáním nových technologií, například aplikací elektronických zdravotních záznamů (používaných případně přes internet) a dalších

nástrojů, například zdravotních karet pacientů a lékařů. V závislosti na systémech zdravotní péče členských států je samozřejmě možné kombinovat dokumentaci v papírové a elektronické podobě.

25. Aplikace elektronického zdravotnictví a telemedicíny, které spadají do oblasti působnosti navrhované směrnice, budou záviset výlučně na výměně elektronických údajů o zdravotním stavu (jde např. o známky vitálních funkcí, snímky atd.), obvykle spolu s dalšími stávajícími elektronickými informačními systémy pro účely zdravotní péče fungujícími v členském státě, v němž je poskytována léčba, a v členském státě, v němž je pacient pojištěn. Patří sem systémy fungující jak na bázi pacient-lékař (např. monitorování a diagnostika na dálku), tak i na bázi lékař-lékař (např. telekonzultace mezi zdravotníky za účelem odborného poradenství ohledně konkrétních případů zdravotní péče). Další specifitější aplikace v oblasti zdravotní péče sloužící ke komplexnímu poskytování přeshraniční zdravotní péče mohou rovněž spočívat pouze v elektronické výměně údajů, tj. elektronický lékařský předpis (ePrescription) nebo elektronické lékařské doporučení (eReferral), které jsou v některých členských státech na vnitrostátní úrovni již zavedeny.⁽²⁾

Problematické oblasti týkající se přeshraniční výměny údajů o zdravotním stavu

26. Vezmeme-li v úvahu výše uvedené obavy a stávající rozmanitost zdravotních systémů členských států, jakož i pokračující rozvoj aplikací elektronického zdravotnictví v souvislosti s ochranou osobních údajů v přeshraniční péči vznikají dvě hlavní problematické oblasti: a) rozdílná úroveň bezpečnosti požadovaná členskými státy v oblasti ochrany osobních údajů (pokud jde o technická a organizační opatření) a b) zohlednění ochrany soukromí v aplikacích elektronického zdravotnictví, zejména v případě nových trendů. Zvláštní pozornost mohou navíc vyžadovat i jiné aspekty, jako například druhotné využívání údajů o zdravotním stavu, zejména v oblasti sestavování statistik. Tyto otázky jsou dále rozebírány v další části tohoto oddílu.

Bezpečnost údajů v členských státech

27. Navzdory tomu, že se směrnice 95/46/ES a 2002/58/ES v Evropě jednotně používají, interpretace a provádění určitých prvků se může v jednotlivých zemích lišit, zejména v oblastech, kde jsou právní předpisy obecné a jsou ponechány na členských státech. V tomto smyslu vyvolává otázky hlavně bezpečnost zpracování, tj. opatření (technická a organizační), která používají členské státy za účelem zajištění bezpečnosti údajů o zdravotním stavu.

⁽¹⁾ Viz Evropský soud pro lidská práva dne 17. července 2008, *I v. Finsko* (žádost č. 20511/03) bod 38.

⁽²⁾ Zpráva ERA o elektronickém zdravotnictví, Směrem k ustanovení evropské výzkumné oblasti týkající se elektronického zdravotnictví, Evropská Komise, informační společnost a média, březen 2007, http://ec.europa.eu/information_society/activities/health/docs/policy/ehealth-era-full-report.pdf

28. Ačkoli přísná ochrana údajů o zdravotním stavu spadá do kompetence všech členských států, neexistuje v EU v současné době žádné pro všechny přijatelné vymezení „přiměřené“ úrovně bezpečnosti zdravotní péče v rámci EU, které by bylo možné v případě přeshraniční zdravotní péče používat. Takže na základě vnitrostátně uložených předpisů týkajících se ochrany údajů může mít například nemocnice v jednom členském státě povinnost přijmout konkrétní bezpečnostní opatření (například definice bezpečnostní politiky a kodexy chování, konkrétní pravidla externího poskytování služeb a využívání externích dodavatelů, kontrolní požadavky atd.), zatímco v jiných členských státech tomu tak být nemusí. Tato nejednotnost může mít dopad na přeshraniční výměnu údajů, zejména v případě její elektronické formy, protože není možné zaručit, že budou údaje v různých členských státech zabezpečené (z technického a organizačního pohledu) ve stejné míře.
29. V této oblasti je tudíž potřeba další harmonizace ve smyslu vymezení společného souboru bezpečnostních požadavků vztahujících se na zdravotní péči, které by byly společně přijaty poskytovateli zdravotnických služeb v členských státech. Tato potřeba je zcela v souladu s obecnou potřebou vymezení společných zásad ve zdravotních systémech EU, jak je uvedeno v návrhu.
30. Tyto zásady by měly být stanoveny v obecné rovině, aniž by se členským státům nařizovaly konkrétní technická řešení, přičemž by se však stanovil základ pro vzájemné uznávání a přijímání, například v oblasti vymezení bezpečnostní politiky, identifikace a ověřování identity pacientů a zdravotníků atd. Vzorem při takovém pokusu by se mohly stát stávající evropské a mezinárodní normy (např. ISO a CEN) v oblasti zdravotní péče a bezpečnosti, jakož i všeobecně přijímané a právně podložené technické koncepty (např. elektronické podpisy⁽¹⁾).
31. Evropský inspektor ochrany údajů podporuje myšlenku harmonizace bezpečnosti zdravotní péče na úrovni EU a zastává názor, že by Komise měla přijmout příslušné iniciativy už v rámci stávajícího návrhu (viz níže uvedený oddíl III).
- Ochrana soukromí v aplikacích elektronického zdravotnictví**
32. Ochrana soukromí a bezpečnost by měly být součástí návrhu a zavedení všech systémů zdravotnické péče, zejména aplikací elektronického zdravotnictví („soukromí coby aspekt návrhu“). Tento nezpochybnitelný požadavek podpořily i další příslušné politické dokumenty⁽²⁾, a to jak obecné, tak i konkrétní, které se zabývají oblastí zdravotní péče⁽³⁾.
33. V rámci interoperability elektronického zdravotnictví, o níž se hovoří v uvedeném návrhu, by se jako základ všech předpokládaných trendů vývoje měl znovu zdůraznit pojem „soukromí coby aspekt návrhu“. Tento pojem se týká několika různých rovin: organizační, sémantické a technické.
- V organizační rovině by se soukromí mělo zohledňovat při vymezování postupů potřebných při výměně údajů o zdravotním stavu mezi zdravotnickými zařízeními příslušných členských států. To může mít přímý vliv na typ výměny a na rozsah přenášovaných údajů (např. případné používání identifikačních čísel místo skutečných jmen pacientů).
 - V sémantické rovině by měly být požadavky ochrany soukromí a bezpečnosti zahrnuty do nových norem a systémů, např. stanovení formátu elektronického lékařského předpisu, o němž se hovoří v návrhu. Mohlo by se vycházet ze stávajících technických norem v této oblasti, např. z norem týkajících se důvěrné povahy údajů a digitálního podpisu, a řešit konkrétní potřeby v oblasti zdravotní péče, jako je ověřování identity kvalifikovaných zdravotníků na základě jejich úloh.
 - V technické rovině by se strukturou systémů a uživatelskými aplikacemi měly upravit technologie zlepšující ochranu soukromí uplatňováním výše uvedených sémantických definic.
34. Evropský inspektor ochrany údajů se domnívá, že by oblast elektronických lékařských předpisů mohla sloužit jako odrazový můstek pro začlenění požadavků týkajících se ochrany soukromí a bezpečnosti už na samotném začátku vývoje (viz níže uvedený oddíl III).

Další hlediska

35. Dalším hlediskem, které by se mohlo vzít v rámci přeshraniční výměny údajů o zdravotním stavu v úvahu, je druhotné využívání údajů o zdravotním stavu, zejména pak využívání údajů pro účely statistiky, jak je již uvedeno ve stávajícím návrhu.
36. Jak již bylo uvedeno v bodě 18, čl. 8 odst. 4 směrnice 95/46/ES předpokládá možnost druhotného využívání údajů o zdravotním stavu. K tomuto dalšímu zpracování by však mělo docházet pouze z důvodů „významného veřejného zájmu“ a je nutné, aby se na ně vztahovala „vhodná ochranná opatření“ stanovená vnitrostátními právními předpisy nebo na základě rozhodnutí orgánu dozoru.⁽⁴⁾ V případě zpracování statistických údajů, rovněž zmíněného ve stanovisku evropského inspektora ochrany

⁽¹⁾ Směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy, Úř. věst. L 13, 19.1.2000, s. 12–20.

⁽²⁾ Evropský inspektor ochrany údajů a vědecký a technický rozvoj EU, politický dokument, Evropský inspektor ochrany údajů, duben 2008, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/08-04-28_PP_RTD_EN.pdf

⁽³⁾ Doporučení Komise ze dne 2. července 2008 o přeshraniční interoperabilitě systémů elektronických zdravotních záznamů (oznámeno pod číslem K(2008) 3282), Úř. věst. L 190, 18.7.2008, s. 37.

⁽⁴⁾ Viz rovněž 34. bod odůvodnění směrnice 95/46/ES. K tomuto bodu viz rovněž stanovisko Pracovní skupiny článku 29 týkající se výše uvedených elektronických zdravotních záznamů v poznámce pod čarou 8 na str. 16.

údajů k navrhovanému nařízení o statistikách Společenství v oblasti veřejného zdraví, bezpečnosti a ochrany zdraví při práci ⁽¹⁾, navíc vyplývá další riziko z toho, že při uplatňování právních předpisů v oblasti ochrany údajů na jedné straně a právních předpisů týkajících se statistiky, by mohly být pojmy „důvěrnost“ a „ochrana údajů“ vnímány odlišně.

37. Evropský inspektor ochrany údajů by výše uvedené prvky rád zdůraznil v kontextu stávajícího návrhu. Při následném využívání údajů o zdravotním stavu by se měly uvést podrobnější odkazy na požadavky ochrany údajů (viz níže uvedený oddíl III).

III. PODROBNÁ ANALÝZA NÁVRHU

Ustanovení o ochraně údajů obsažená v návrhu

38. V různých částech návrhu jsou uvedeny četné odkazy na ochranu údajů a soukromí, a to konkrétněji:

- ve 3. bodě odůvodnění se mimo jiné stanoví, že se směrnice musí provádět a uplatňovat při náležitém dodržování práva na soukromý život a ochranu osobních údajů;
- v 11. bodě odůvodnění je v souvislosti se zpracováváním osobních údajů uveden odkaz na základní právo na soukromí a na důvěrnost jakožto na dvě operační zásady společné pro systémy zdravotnictví v celém Společenství;
- v 17. bodě odůvodnění se píše o právu na ochranu osobních údajů jakožto o základním právu jednotlivců, které je třeba zabezpečit, přičemž je pozornost věnována především právu jednotlivců na přístup k údajům o zdravotním stavu – rovněž v souvislosti s přeshraniční zdravotní péčí – jak je stanoveno ve směrnici 95/46/ES;
- v článku 3, v němž se stanoví vztah uvedené směrnice k ostatním právním předpisům Společenství, je v odst. 1 písm. a) uveden odkaz na směrnice 95/46/ES a 2002/58/ES;
- v článku 5 týkajícím se povinností členských států, v němž je poskytována léčba, se v odst. 1 písm. f) za jednu z těchto povinností stanoví ochrana práva na soukromí, a to v souladu s vnitrostátními opatřeními, jimiž se provádějí směrnice 95/46/ES a 2002/58/ES;
- v článku 6 věnovaném zdravotní péči poskytované v jiném členském státě se v odstavci 5 zdůrazňuje právo pacientů, kteří cestují do jiného členského státu za účelem využití zdravotní péče, nebo pacientů, kteří vyhledávají zdravotní péči poskytovanou v jiném členském státě, na přístup ke své zdravotní dokumentaci, což je opět v souladu s vnitrostátními opatřeními, jimiž se provádějí směrnice 95/46/ES a 2002/58/ES;

— v článku 12 o vnitrostátních kontaktních místech pro přeshraniční zdravotní péči se v odst. 2 písm. a) uvádí, že by tato kontaktní místa měla být mimo jiné odpovědná za to, že budou pacientům poskytovat a dodávat informace o zárukách ochrany osobních údajů poskytovaných v jiném členském státě;

— v článku 16 týkajícím se elektronického zdravotnictví, se stanoví, že opatření pro dosažení interoperability systémů informačních a komunikačních technologií by měla respektovat základní právo na ochranu osobních údajů v souladu s platnými právními předpisy;

— nakonec je v čl. 18 odst. 1 mimo jiné uvedeno, že sběr údajů pro účely statistiky a sledování by měl probíhat v souladu s vnitrostátními právními předpisy a právními předpisy Společenství o ochraně osobních údajů.

39. Evropský inspektor ochrany údajů vítá skutečnost, že se při vypracovávání návrhu zohledňovala ochrana údajů a že je snaha ukázat celkovou potřebu ochrany soukromí v souvislosti s přeshraniční zdravotní péčí. Stávající ustanovení návrhu o ochraně údajů jsou však příliš obecná, anebo se poněkud selektivně a nesystematicky odvolávají na povinnosti členských států:

— Zejména ve 3. a 11. bodě odůvodnění a v čl. 3 odst. 1 písm. a), článku 16 a čl. 18 odst. 1 se ve skutečnosti řeší obecný právní rámec ochrany údajů (v posledních dvou z těchto článků je to v souvislosti s elektronickým zdravotnictvím a se sběrem údajů pro účely statistiky, ale bez stanovení konkrétních požadavků týkajících se soukromí).

— V čl. 5 odst. 1 písm. f) je uveden obecný odkaz na odpovědnost členských států.

— V 17. bodě odůvodnění a v čl. 6 odst. 5 je uveden konkrétnější odkaz na právo pacientů na přístup ke své lékařské dokumentaci ve členském státě, v němž je poskytována léčba.

— V čl. 12 odst. 2 písm. a) je pak ustanovení týkající se práva pacientů na informace v členském státě, v němž je pacient pojištěn (prostřednictvím vnitrostátních kontaktních míst).

Jak již bylo uvedeno v úvodu tohoto stanoviska, v návrhu navíc není uvedena žádná spojitost s aspekty týkajícími se soukromí, jimiž se zabývají jiné právní nástroje ES (závazné či nezávazné) v oblasti zdravotní péče, anebo odkaz na ně, zejména pokud jde o využívání nových aplikací informačních a komunikačních technologií (jako je telemedicina a elektronické záznamy o zdravotním stavu).

⁽¹⁾ Úř. věst. C 295, 7.12.2007, s. 1.

40. I když je ochrana soukromí obecně stanovena jakožto požadavek přeshraniční zdravotní péče, celkový obraz stále chybí, a to jak pokud jde o povinnosti členských států, tak i pokud jde o podrobnosti vyplývající z přeshraniční povahy poskytování služeb v oblasti zdravotní péče (v protikladu k vnitrostátním ustanovením týkajícím se poskytování služeb v oblasti zdravotní péče). Přesněji:

— Povinnosti členských států nejsou prezentovány uceleně, protože některé závazky (právo na přístup a informace) jsou zdůrazňovány – ačkoli v různých částech návrhu – zatímco jiné jsou zcela opominuty, například bezpečnost zpracovávání.

— Obavy ohledně nejednotnosti bezpečnostních opatření jednotlivých členských států a potřeba harmonizace bezpečnosti údajů o zdravotním stavu na evropské úrovni v souvislosti s přeshraniční zdravotní péčí nejsou vůbec zmíněny.

— Není zmíněno ani začlenění otázky soukromí do aplikací elektronického zdravotnictví. To se odpovídajícím způsobem nezohledňuje ani v případě elektronických lékařských předpisů.

41. Určité konkrétní obavy vzbuzuje navíc i článek 18, který se zabývá sběrem údajů pro statistické účely. První odstavce se týká „statistických a dalších doplňujících údajů“; dále se tu hovoří o „účelu sledování“ a následně se uvádějí oblasti, které jsou předmětem tohoto účelu sledování, zejména poskytování přeshraniční zdravotní péče, poskytovatelé péče, její poskytovatelé a pacienti, náklady a výsledky. V této souvislosti, která je již sama o sobě dosti nejasná, je uveden všeobecný odkaz na právní předpisy o ochraně údajů, avšak nejsou stanoveny žádné konkrétní požadavky na následné využívání údajů týkajících se zdravotního stavu, jak je stanoveno v čl. 8 odst. 4 směrnice 95/46/ES. Druhý odstavec navíc obsahuje bezpodmínečnou povinnost předávat velké množství údajů Komisi, a to alespoň jednou ročně. Jelikož není uveden žádný výslovný odkaz na posouzení nezbytnosti tohoto předávání, působí to dojmem, jako by normotvůrce Společenství nezbytnost tohoto předávání údajů Komisi již stanovil.

Doporučení evropského inspektora ochrany údajů

42. Evropský inspektor ochrany údajů nabízí celou řadu doporučení, jak výše uvedené problémy odpovídajícím způsobem řešit, a to na základě změn v pěti níže popsanych základních krocích.

Krok 1 – Vymezení údajů o zdravotním stavu

43. Článek 4 vymezuje základní pojmy používané v návrhu. Evropský inspektor ochrany údajů důrazně doporučuje, aby byla do tohoto článku vložena definice údajů o zdravotním stavu. Údaje o zdravotním stavu by se měly vymezit široce, například tak, jak jsou popsány v oddíle II tohoto stanoviska (body 14 a 15).

Krok 2 – Vložení zvláštního článku o ochraně údajů

44. Evropský inspektor ochrany údajů rovněž důrazně doporučuje vložit do návrhu konkrétní článek o ochraně údajů, který by mohl jasně a srozumitelně stanovit celkový rozměr ochrany soukromí. V tomto článku by měly být a) popsány veškeré povinnosti členského státu, v němž je pacient pojištěn, a členského státu, v němž je poskytována léčba, mimo jiné i nutnost bezpečnosti zpracovávání, a b) stanoveny hlavní oblasti dalšího rozvoje, např. začlenění harmonizace bezpečnosti a ochrany soukromí do elektronického zdravotnictví. Tyto záležitosti je možné řešit prostřednictvím konkrétních ustanovení (v rámci navrhovaného článku), jak je níže uvedeno v krocích 3 a 4.

Krok 3 – Konkrétní ustanovení ohledně harmonizace bezpečnosti

45. V návaznosti na změnu navrhovanou v kroku 2 doporučuje evropský inspektor ochrany údajů Komisi, aby přijala mechanismus, na jehož základě by byla s ohledem na stávající technické normy v této oblasti vymezena všeobecně přijatelná úroveň bezpečnosti údajů o zdravotní péči na vnitrostátní úrovni. To by mělo být promítnout do návrhu. Případné provádění by mohlo probíhat prostřednictvím postupu projednávání ve výboru, neboť ten je popsán již v článku 19 a vztahuje se na další části návrhu. Navíc by se k tvorbě příslušných obecných zásad mohlo využít dalších nástrojů, včetně všech příslušných zúčastněných stran, například Pracovní skupiny článku 29 a evropského inspektora ochrany údajů.

Krok 4 – Začlenění otázky ochrany soukromí do šablony elektronického lékařského předpisu

46. V článku 14 věnovaném uznávání lékařských předpisů vydaných v jiném členském státě se stanoví zavedení šablony lékařského předpisu Společenství, jímž se podpoří interoperabilita v oblasti elektronických lékařských předpisů. Toto opatření bude přijato postupem projednávání ve výboru, neboť je stanoven v čl. 19 odst. 2 návrhu.

47. Evropský inspektor ochrany údajů doporučuje, aby součástí navrhované šablony elektronického lékařského předpisu byla ochrana soukromí a bezpečnost, a to už při nejzákladnějším sémantickém vymezení této šablony. To je třeba výslovně uvést v čl. 14 odst. 2 písm. a). Také v tomto případě je nesmírně důležité zapojení všech příslušných zúčastněných stran. V této souvislosti by chtěl být evropský inspektor ochrany údajů informován o dalších opatřeních přijatých v této otázce prostřednictvím navrhovaného projednávání ve výboru a chtěl by se na nich podílet.

Krok 5 – Následné využívání údajů o zdravotním stavu pro účely statistiky a sledování

48. S cílem vyhnout se nedorozuměním vyzývá evropský inspektor ochrany údajů k objasnění pojmu „další doplňující údaje“ v čl. 18 odst. 1. Tento článek by měl být dále změněn v tom smyslu, aby se v něm jasněji odkazovalo na požadavky následného využívání údajů o zdravotním stavu, jak jsou stanoveny v čl. 8 odst. 4 směrnice 95/46/ES. Povinnost předávat veškeré údaje Komisi obsažená ve druhém odstavci by měla podmíněna posouzením nutnosti tohoto předávání k oprávněným účelům, které budou předem náležitě určeny.

IV. ZÁVĚRY

49. Evropský inspektor ochrany údajů by rád vyjádřil podporu iniciativám zaměřeným na zlepšování podmínek poskytování přeshraniční zdravotní péče. Vyjadřuje však znepokojení nad tím, že iniciativy ES související se zdravotní péčí nejsou vždy dobře koordinované, pokud jde o používání informačních a komunikačních technologií, otázku ochrany soukromí a bezpečnosti, což brání přijetí jednotného přístupu k ochraně údajů v oblasti zdravotní péče.
50. Evropský inspektor ochrany údajů vítá, že je ve stávajícím návrhu odkaz na ochranu soukromí. Jak je však vysvětleno v oddíle III tohoto stanoviska, je nutná celá řada změn, aby byly stanoveny jasné požadavky, a to jak na členský stát, v němž je pacient pojištěn, tak i na členský stát, v němž je poskytována léčba, a aby se řádným způsobem řešil aspekt ochrany údajů při přeshraniční zdravotní péči:

— Do článku 4 by se měla vložit definice údajů o zdravotním stavu, která by se vztahovala na všechny osobní údaje, které jasně a úzce souvisejí s popisem zdravotního stavu člověka. K nim by v zásadě měly patřit zdravotní údaje, ale i správní a finanční údaje související se zdravotním stavem.

- Důrazně se doporučuje vložení zvláštního článku o ochraně údajů. V tomto článku by se měl jasně určit celkový obraz, přičemž by se popsaly povinnosti členského státu, v němž je pacient pojištěn, a členského státu, v němž je poskytována léčba, a stanovily by se hlavní oblasti dalšího rozvoje, např. harmonizace bezpečnosti a začlenění otázky soukromí, zejména do aplikací elektronického zdravotnictví.
- Doporučuje se, aby Komise v rámci tohoto návrhu přijala mechanismus, na jehož základě by byla s ohledem na stávající technické normy v této oblasti vymezena všeobecně přijatelná úroveň bezpečnosti údajů o zdravotní péči na vnitrostátní úrovni. Měly by se podporovat další nebo doplňující iniciativy, do nichž by se zapojily všechny příslušné zúčastněné strany, Pracovní skupina článku 29 a evropský inspektor ochrany údajů.
- Doporučuje se, aby byl do navrhované šablony Společenství pro elektronické lékařské předpisy vložen pojem „soukromí coby aspekt návrhu“ (a to i v sémantické rovině). To je třeba výslovně uvést v čl. 14 odst. 2 písm. a). Evropský inspektor ochrany údajů by měl být informován a chtěl by se podílet na dalších opatřeních přijatých v této otázce prostřednictvím navrhovaného postupu projednávání ve výboru.
- Doporučuje se, aby se upřesnily formulace článku 18 a aby byl v tomto článku uveden výslovnější odkaz na konkrétní požadavky související s následným využíváním údajů týkajících se zdravotního stavu, jak je stanoveno v čl. 8 odst. 4 směrnice 95/46/ES.

V Bruselu dne 2. prosince 2008.

Peter HUSTINX

evropský inspektor ochrany údajů

Druhé stanovisko evropského inspektora ochrany údajů k přezkumu směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích)

(2009/C 128/04)

EVROPSKÝ INSPEKTOR OCHRANY ÚDAJŮ,

soukromí a osobních údajů jednotlivců (dále jen „první stanovisko EIOÚ“) (2).

s ohledem na Smlouvu o založení Evropského společenství, a zejména na článek 286 této smlouvy,

s ohledem na Listinu základních práv Evropské unie, a zejména na článek 8 této listiny,

s ohledem na směrnici Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů,

s ohledem na směrnici Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací,

s ohledem na 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, a zejména na článek 41 tohoto nařízení,

PŘIJAL TOTO STANOVISKO:

I. ÚVOD

Souvislosti

1. Dne 13. listopadu 2007 Evropská komise přijala návrh, kterým se mění mimo jiné směrnice o soukromí a elektronických komunikacích, k níž se obvykle odkazuje jako ke směrnici o ochraně soukromí v odvětví elektronických komunikací (1) (dále jen „návrh“ nebo „návrh Komise“). Dne 10. dubna 2008 přijal EIOÚ stanovisko k uvedenému návrhu Komise, v němž uvedl doporučení ke zlepšení návrhu ve snaze napomoci k zajištění toho, aby navrhované změny vedly k nejlepší možné ochraně

(1) Přezkum směrnice o soukromí a elektronických komunikacích je součástí rozsáhlejšího přezkumu, jehož cílem bylo zřídit telekomunikační úřad EU, přezkoumat směrnice 2002/21/ES, 2002/19/ES, 2002/20/ES, 2002/22/ES a 2002/58/ES, jakož i nařízení (ES) č. 2006/2004 (dále jen souhrnně „přezkum telekomunikačního balíčku“).

2. EIOÚ uvítal vytvoření povinného systému oznamování narušení bezpečnosti navrhované Komisí, na jehož základě mají společnosti povinnost informovat jednotlivce v případě, že byly jejich osobní údaje ohroženy. Dále rovněž uvítal nové ustanovení umožňující právníkům osobám (např. sdružením spotřebitelů a poskytovatelům internetových služeb) podat žalobu na odesílatele nevyžádaných obchodních sdělení s cílem doplnit stávající nástroje v boji proti nevyžádaným obchodním sdělením („spam“).

3. Během projednávání v Parlamentu, které předcházelo prvnímu čtení Evropského parlamentu, poskytl EIOÚ další poradenství prostřednictvím připomínek k vybraným otázkám, které vystaly ve zprávách navržených výborů Evropského parlamentu odpovědnými za přezkum směrnice o univerzální službě (3) a směrnice o soukromí a elektronických komunikacích (dále jen „připomínky“) (4). Připomínky se v první řadě týkaly otázek souvisejících se zpracováním provozních údajů a s ochranou práv duševního vlastnictví.

4. Dne 24. září 2008 Evropský parlament přijal legislativní usnesení o směrnici o soukromí a elektronických komunikacích (dále jen „první čtení“) (5) EIOÚ se vyjádřil kladně k několika změnám Evropského parlamentu, které byly přijaty v návaznosti na stanovisko a připomínky EIOÚ uvedené výše. K důležitým změnám patřilo mimo jiné zahrnutí poskytovatelů služeb informační společnosti (tj. společností působících na internetu) do rámce povinnosti oznamovat narušení bezpečnosti. EIOÚ rovněž uvítal změnu umožňující právníkům a fyzickým osobám

(2) Stanovisko ze dne 10. dubna 2008 k návrhu směrnice, kterou se mění mimo jiné směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích), Úř. věst. C 181, 18.7.2008, s. 1.

(3) Směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací (směrnice o univerzální službě), Úř. věst. L 108, 24.4.2002, s. 51.

(4) Připomínky EIOÚ k vybraným otázkám, které vyplynuly ze zprávy Výboru pro vnitřní trh a ochranu spotřebitelů o přezkumu směrnice 2002/22/ES (o univerzální službě) a směrnice 2002/58/ES (o soukromí a elektronických komunikacích), 2. září 2008. K dispozici na adrese: www.edps.europa.eu

(5) Legislativní usnesení Evropského parlamentu ze dne 24. září 2008 o návrhu směrnice Evropského parlamentu a Rady, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci v oblasti ochrany spotřebitele (KOM(2007) 698 – C6-0420/2007 – 2007/0248(COD)).

podat žalobu na porušení kteréhokoliv ustanovení směrnice o soukromí a elektronických komunikacích (nikoliv pouze na porušení ustanovení o nevyžádaném obchodním sdělení, jak původně navrhovala Komise). Po prvním čtení Parlamentu přijala Komise pozměněný návrh směrnice o soukromí a elektronických komunikacích (dále jen „pozměněný návrh“) ⁽⁶⁾.

5. Dne 27. listopadu 2008 Rada dosáhla politické dohody o přezkumu pravidel týkajících se telekomunikačního balíčku, včetně směrnice o soukromí a elektronických komunikacích, z níž vzejde společný postoj Rady (dále jen „společný postoj“) ⁽⁷⁾. Společný postoj bude předložen Evropskému parlamentu podle čl. 251 odst. 2 Smlouvy o založení Evropského společenství, což může vést k navržení změn ze strany Evropského parlamentu.

Celkový názor na postoj Rady

6. Rada změnila základní prvky znění návrhu a nepřijala mnoho změn přijatých Evropským parlamentem. Ačkoliv společný postoj zcela určitě obsahuje pozitivní prvky, pokud jde o celek, EIOÚ je znepokojen jeho obsahem, zejména proto, že společný postoj nezahrnuje některé pozitivní změny navržené Evropským parlamentem, pozměněným návrhem nebo stanovisky EIOÚ a evropských orgánů pro ochranu údajů vydaných Pracovní skupinou zřízenou podle článku 29. ⁽⁸⁾

7. Naproti tomu byly v několika případech ustanovení pozměněného návrhu a změny Evropského parlamentu, které poskytovaly záruky občanům, vypuštěny či podstatně oslabeny. V důsledku toho je ve společném postoji úroveň ochrany poskytnutá jednotlivcům podstatně oslabena. Proto EIOÚ nyní vydává druhé stanovisko a věří, že v průběhu legislativního procesu v souvislosti se směrnicí o soukromí a elektronických komunikacích budou přijaty nové změny, které obnoví záruky v oblasti ochrany údajů.

8. Toto druhé stanovisko se zaměřuje na některé podstatné obavy a neopakuje všechny body uvedené v prvním stanovisku evropského inspektora ochrany údajů nebo v připomínkách, které platí i nadále. Toto stanovisko se věnuje především těmto otázkám:

⁽⁶⁾ Pozměněný návrh směrnice Evropského parlamentu a Rady, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci v oblasti ochrany spotřebitele, Brusel 6.11.2008 KOM(2008) 723 v konečném znění.

⁽⁷⁾ K dispozici na veřejné webové stránce Rady.

⁽⁸⁾ Stanovisko 2/2008 k přezkumu směrnice 2002/58/ES o soukromí a elektronických komunikacích (neboli *ePrivacy Directive*), které je k dispozici na webové stránce Pracovní skupiny zřízené podle článku 29.

— ustanovení o oznamování narušení bezpečnosti;

— rozsah působnosti směrnice o soukromí a elektronických komunikacích v souvislosti se soukromými a veřejně přístupnými soukromými sítěmi;

— zpracování provozních údajů pro bezpečnostní účely;

— možnost právnických osob podat žalobu na porušení směrnice o soukromí a elektronických komunikacích.

9. Při řešení výše uvedených otázek analyzuje toto stanovisko společný postoj Rady a porovnává jej s prvním čtením v Evropském parlamentu a pozměněným návrhem Komise. Stanovisko obsahuje doporučení zaměřená na zjednodušení ustanovení směrnice o soukromí a elektronických komunikacích a na zajištění toho, aby směrnice i nadále odpovídajícím způsobem chránila soukromí a osobní údaje jednotlivců.

II. USTANOVENÍ O OZNAMOVÁNÍ NARUŠENÍ BEZPEČNOSTI

10. EIOÚ podporuje přijetí režimu oznamování narušení bezpečnosti, podle něhož budou orgány a jednotlivci uvědoměni v případě, že jsou jejich osobní údaje ohroženy. ⁽⁹⁾ Oznamování o narušení bezpečnosti může pomoci jednotlivcům přijmout nezbytné kroky ke zmírnění jakýchkoliv potenciálních škod, které z tohoto ohrožení vyplývají. Povinnost zasílat oznámení informující o narušení bezpečnosti kromě toho povzbudí společnosti, aby zlepšovaly bezpečnost údajů, a posílí jejich odpovědnost, pokud jde o osobní údaje, za něž odpovídají.

11. Pozměněný návrh Komise, první čtení Evropského parlamentu a společný postoj Rady představují tři různé přístupy k oznamování narušení bezpečnosti, které se v současné době zvažují. Všechny tři přístupy mají pozitivní aspekty. EIOÚ se však domnívá, že u každého z těchto přístupů existuje prostor pro zlepšení, a doporučuje, aby při zvažování konečných kroků k přijetí režimu oznamování narušení bezpečnosti byla zohledněna doporučení popsána níže.

⁽⁹⁾ V tomto stanovisku se používá termín „ohrožený“ pro označení jakéhokoliv náhodného či nedovoleného zničení, ztráty, úpravy nebo neoprávněnému sdělování či zpřístupnění osobních údajů přenášených, uchovávaných či jinak zpracovávaných.

12. Při analýze zmíněných tří režimů oznamování narušení bezpečnosti je třeba zvážit pět kritických bodů: (i) definici narušení bezpečnosti; (ii) subjekty, na něž se vztahuje oznamovací povinnost (dále jen „zahrnuté subjekty“) (iii) kritérium pro oznamovací povinnost; (iv) určení subjektu odpovědného za stanovení, zda narušení bezpečnosti odpovídá tomuto kritériu či nikoliv a (v) příjemci oznámení.

Shrnutí přístupů Komise, Rady a Evropského parlamentu

13. Evropský parlament, Komise a Rada přijaly různé přístupy k oznamování narušení bezpečnosti. V prvním čtení Evropského parlamentu byl změněn původní režim oznamování narušení bezpečnosti stanovený v návrhu Komise.⁽¹⁰⁾ Podle přístupu Evropského parlamentu se oznamovací povinnost vztahuje nejen na poskytovatele veřejně dostupných služeb elektronických komunikací, ale rovněž na poskytovatele služeb informační společnosti. V rámci tohoto přístupu by dále byla veškerá narušení osobních údajů oznámena vnitrostátnímu regulačnímu orgánu nebo příslušným orgánům (dále jen souhrnně „orgány“) Pokud by tyto orgány stanovily, že je narušení *závažné*, požadovaly by, aby poskytovatelé veřejně dostupných služeb elektronických komunikací a poskytovatelé služeb informační společnosti neprodleně informovali dotčené osoby. V případě narušení, které představuje bezprostřední a přímé ohrožení, by poskytovatelé veřejně dostupných služeb elektronických komunikací a poskytovatelé služeb informační společnosti oznámili tuto skutečnost jednotlivcům ještě před tím, než informují orgány, a nečekali by na rozhodnutí regulačního orgánu. Výjimka z povinnosti informovat spotřebitele se vztahuje na subjekty, které mohou prokázat orgánům, že „byla zavedena náležitá opatření technologické ochrany“ činící údaje nečitelnými pro všechny, kdo nemají oprávnění k přístupu k nim.
14. Podle přístupu Rady musí být narušení také oznámeno jak účastníkům, tak orgánům, avšak pouze v případech, kdy se *zahrnuté subjekty* domnívají, že narušení představuje *závažné nebezpečí* pro soukromí účastníka (tj. krádež či podvodné zneužití totožnosti, fyzická újma, hrubá potupa či poškození pověsti).
15. V pozměněném návrhu Komise je zachována povinnost oznámit orgánům všechna narušení, kterou navrhl Evropský parlament. Avšak na rozdíl od přístupu Evropského parlamentu pozměněný návrh obsahuje výjimku z požadavku na oznamování dotčeným jednotlivcům, pokud poskytovatel veřejně dostupných služeb elektronických komunikací prokáže příslušnému orgánu, že (i) „s *přiměřenou pravděpodobností*“ nedojde v důsledku tohoto narušení k žádné škodě (např. k hospodářské ztrátě, společenské škodě nebo krádeži totožnosti) nebo (ii) pokud byla na údaje, u nichž došlo k narušení, použita „*náležitá opatření technologické ochrany*“. Z toho vyplývá, že se v přístupu Komise spojuje oznámení jednotlivcům s analýzou škod.

16. Je důležité poznamenat, že podle přístupu Evropského parlamentu⁽¹¹⁾ a Komise jsou to *orgány*, které jsou v konečném důsledku oprávněny stanovit, zda je narušení závažné nebo zda může s přiměřenou pravděpodobností způsobit škodu. Naproti tomu v přístupu Rady je rozhodnutí ponecháno na *dotčených subjektech*.

17. Přístup Rady i Komise se vztahuje pouze na poskytovatele veřejně dostupných služeb elektronických komunikací, a nikoliv, jak je tomu v případě přístupu Evropského parlamentu, na poskytovatele služeb informační společnosti.

Definice narušení bezpečnosti

18. EIOÚ vítá, že všechny tři legislativní návrhy obsahují stejnou definici oznamování narušení bezpečnosti, které je vymezeno jako „*narušení bezpečnosti, které vede k náhodnému nebo protiprávnímu zničení, ztrátě, změně či neoprávněnému vyjádření nebo zpřístupnění osobních údajů přenášených, uchovávaných nebo jinak zpracovávaných [...]*“⁽¹²⁾
19. Jak je podrobněji uvedeno níže, tato definice je vítána, protože je dostatečně široká, aby zahrnula většinu příslušných situací, v nichž by mohlo být zaručeno oznamování narušení bezpečnosti.
20. Zprvu, tato definice zahrnuje případy, kdy došlo k *neoprávněnému přístupu* k osobním údajům ze strany třetí osoby, jako je neoprávněné vniknutí na servery obsahující osobní údaje a získání takových informací.
21. Zadruhé, tato definice by rovněž zahrnula situace, v nichž došlo ke ztrátě nebo vyjádření osobních údajů, přičemž neoprávněný přístup je třeba ještě prokázat. Jednalo by se o takové situace, kdy mohlo dojít ke ztrátě osobních údajů (např. CD-ROMů, USB klíčů nebo jiných přenosných zařízení) nebo ke zveřejnění řádnými uživateli (složka s údaji zaměstnance nedopatřením a dočasně zpřístupněná pro veřejně dostupnou oblast prostřednictvím internetu). Vzhledem k tomu, že často nebude k dispozici důkaz o tom, že k těmto údajům může nebo nemůže mít v daném okamžiku přístup třetí osoba nebo že tyto údaje může využít, zdá se být vhodné zahrnout tyto případy do rozsahu této definice. Proto EIOÚ doporučuje tuto definici zachovat. EIOÚ rovněž doporučuje zahrnout definici narušení bezpečnosti do článku 2 směrnice o soukromí a elektronických komunikacích, protože by to více odpovídalo celkové struktuře směrnice a zajistilo by to větší jasnost.

⁽¹⁰⁾ Touto otázkou se zabývají zejména tyto změny Evropského parlamentu: 187, 124 až 127, 27, 21 a 32.

⁽¹¹⁾ Vyjma případů bezprostředního a přímého ohrožení; v takovém případě musí zahrnuté subjekty nejprve informovat spotřebitele.

⁽¹²⁾ Článek 2 písm. i) společného postoje a pozměněného návrhu a čl. 3 odst. 3 prvního čtení Evropského parlamentu.

Subjekty, na něž by se měla vztahovat oznamovací povinnost

22. Oznamovací povinnost v rámci přístupu Evropského parlamentu se vztahuje na poskytovatele veřejně dostupných služeb elektronických komunikací a na poskytovatele služeb informační společnosti. Avšak podle režimů Rady a Komise budou mít oznamovací povinnost vůči jednotlivcům pouze poskytovatelé veřejně dostupných služeb elektronických komunikací, jako jsou telekomunikační společnosti a poskytovatelé přístupu k internetu, a to v případě, že dojde k narušení bezpečnosti vedoucí k ohrožení osobních údajů. Jiné oblasti činnosti, jako jsou například internetové banky, internetoví maloobchodníci, internetoví poskytovatelé zdravotnických služeb a jiní nejsou touto povinností vázáni. Z níže uvedených důvodů se EIOÚ domnívá, že z hlediska veřejné politiky je nutné zajistit, aby se na služby informační společnosti, které zahrnují internetové podniky, internetové banky, internetové poskytovatele zdravotnických služeb a další, rovněž vztahovala oznamovací povinnost.
23. Zprvu, EIOÚ uvádí, že ačkoliv telekomunikační společnosti jsou jistě cílem narušení bezpečnosti, které odůvodňuje oznamovací povinnost, totéž platí pro jiné druhy společností či poskytovatelů. Pravděpodobnost narušení bezpečnosti v případě internetových maloobchodníků, internetových bank, on-line lékáren je stejná, ne-li vyšší, jako v případě telekomunikačních společností. Na základě zvážení rizik se proto nelze přiklonit k omezení rozsahu požadavku oznamovat narušení údajů na poskytovatele veřejně dostupných služeb elektronických komunikací. Potřebu širšího přístupu dokládají zkušenosti jiných zemí. Například téměř všechny státy ve Spojených státech amerických (nyní je jich více než 40) přijaly zákony o oznamování narušení bezpečnosti, které mají širší oblast působnosti a zahrnují nejen poskytovatele veřejně dostupných služeb elektronických komunikací, ale všechny subjekty mající požadované osobní údaje.
24. Zadruhé, i když je zřejmé, že narušení těch druhů osobních údajů, které jsou pravidelně zpracovávány poskytovateli veřejně dostupných služeb elektronických komunikací, může mít dopad na soukromí jednotlivců, totéž platí, ne-li ještě ve větší míře, pro druhy osobních informací zpracovávaných poskytovateli služeb informační společnosti. Banky a jiné finanční instituce mohou mít zcela jistě k dispozici vysoce důvěrné informace (např. údaje o bankovních účtech), jejichž vyzrazení může umožnit využití pro účely krádeže totožnosti. Rovněž vyzrazení velmi citlivých údajů týkajících se zdraví prostřednictvím zdravotních služeb on-line může jednotlivce velmi poškodit. Ty druhy osobních údajů, které mohou být ohroženy, proto rovněž vyžadují širší použití oznamování narušení bezpečnosti, které by zahrnovalo alespoň poskytovatele služeb informační společnosti.
25. Proti rozšíření oblasti působnosti tohoto článku, tj. subjektů, na které se vztahuje tento požadavek, byly vzneseny některé právní námitky. Zejména skutečnost, že celková oblast působnosti směrnice o soukromí a elektronických komunikacích se týká pouze poskytovatelů veřejně dostupných služeb elektronických komunikací, byla uvedena jako překážka uplatnění oznamovací povinnosti rovněž na poskytovatele služeb informační společnosti.
26. V této souvislosti by chtěl EIOÚ připomenout, že: (i) neexistuje žádná právní překážka pro zahrnutí dalších subjektů do oblasti působnosti některých ustanovení této směrnice, společně s poskytovateli veřejně dostupných služeb elektronických komunikací. To je zcela na uvážení normotvůrce Společenství. (ii) ve stávající směrnici o soukromí a elektronických komunikacích jsou jiné precedenty ohledně použití na jiné subjekty, než jsou poskytovatelé veřejně dostupných služeb elektronických komunikací.
27. Například článek 13 se použije nejen na poskytovatele veřejně dostupných služeb elektronických komunikací, ale na kteroukoliv společnost, která zasílá nevyžádaná sdělení, k čemuž je vyžadován předchozí souhlas. Kromě toho čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích, který mimo jiné zakazuje uchovávání informací, jako jsou „cookies“, v koncových zařízeních uživatelů, je závazný nejen pro poskytovatele veřejně dostupných služeb elektronických komunikací, ale rovněž pro všechny, kdo se pokoušejí ukládat informace nebo získat přístup k informacím uloženým v koncovém zařízení jednotlivců. V rámci stávajícího legislativního procesu navíc Komise dokonce navrhla rozšířit použití čl. 5 odst. 3 na případy, kdy podobné technologie (cookies/spyware) nejsou přenášeny pouze prostřednictvím systémů elektronické komunikace, ale jakýmkoliv jiným možným způsobem (přenášení stahováním z internetu nebo prostřednictvím externího paměťového média, např. CD-ROMu, USB klíče, flash disků atd.). Všechny tyto prvky jsou vítány a měly by být zachovány, ale rovněž by měly stanovit důležitý precedens pro stávající diskusi o oblasti působnosti.
28. Dále v rámci stávajícího legislativního procesu Komise a Evropský parlament a pravděpodobně i Rada navrhly nový čl. 6 odst. 6a, projednávaný níže, který se vztahuje na jiné subjekty, než jsou poskytovatelé veřejně dostupných služeb elektronických komunikací.
29. A konečně, s ohledem na obsáhlé pozitivní prvky vyplývající z povinnosti oznamovat narušení bezpečnosti budou občané s velkou pravděpodobností očekávat tyto přínosy nejen pokud byly jejich osobní údaje ohroženy ze strany poskytovatelů veřejně dostupných služeb elektronických komunikací, ale rovněž ze strany poskytovatelů služeb informační služby. Očekávání občanů nemusí být splněna, pokud například nejsou informováni v případě, že internetová banka ztratila informace o jejich bankovním účtu.

30. Souhrnně řečeno, EIOÚ je přesvědčen, že plného přínosu vyplývajícího z oznamování narušení bezpečnosti bude lépe dosaženo pouze tehdy, pokud budou do oblasti zahrnutých subjektů spadat vedle poskytovatelů veřejně dostupných služeb elektronických komunikací i poskytovatelé služeb informační společnosti.

Kritérium pro oznamovací povinnost

31. Pokud jde o podnět k oznámení, EIOÚ se domnívá, jak je dále vysvětleno níže, že kritérium „*přiměřené pravděpodobnosti poškození*“ uvedené v pozměněném návrhu jako je ze tří navrhovaných kritérií nejvhodnější. Nicméně je důležité zajistit, aby „poškození“ bylo dostatečně široké k pokrytí všech příslušných případů negativních dopadů na soukromí nebo jiné oprávněné zájmy jednotlivců. Jinak by bylo vhodnější stanovit nové kritérium, na jehož základě by oznamování bylo povinné „*pokud by narušení s přiměřenou pravděpodobností mohlo poškodit jednotlivce*“.
32. Jak bylo naznačeno v předchozí části, podmínky, za nichž musí být učiněno oznámení jednotlivcům (dále jako „podnět“ nebo „kritérium“) se liší podle přístupu Evropského parlamentu, Komise a Rady. Je zřejmé, že objem oznámení, která jednatel obdrží, bude z velké části záviset na podnětu nebo kritériu stanovených pro oznámení.
33. Podle režimů Rady a Komise musí být oznámení provedeno, pokud narušení představuje „*závažné narušení soukromí účastníka*“ (Rada) a pokud „*poškození zájmu spotřebitele je v důsledku narušení přiměřeně pravděpodobné*“ (Komise). Podle režimu Evropského parlamentu je podnětem pro oznámení jednotlivci „*závažnost narušení*“ (tj. oznámení jednotlivcům se vyžaduje, pokud je porušení považováno za „závažné“). Oznámení není nezbytné, pokud není dosaženo tohoto prahu⁽¹³⁾.
34. EIOÚ chápe, že pokud došlo k ohrožení osobních údajů, lze namítnout, že jednotlivci, jimž tyto údaje náleží, mají za všech okolností právo o této události vědět. Nicméně je však správné uvažovat o tom, zda se jedná o vhodné řešení se zřetelem na jiné zájmy a ohledy.
35. Bylo poznamenáno, že povinnost zaslat oznámení při každém ohrožení osobních údajů, jinak řečeno bez omezení, může vést k nadměrnému oznamování a „*únavě z oznamování*“, což by mohlo mít za následek ztrátu citlivosti. Jak je uvedeno níže, EIOÚ považuje tento argument za důležitý; avšak současně chce zdůraznit své

obavy týkající se nadměrného oznamování, které by mohlo být možným ukazatelem širokosáhlého selhání informačních bezpečnostních postupů.

36. Jak je uvedeno výše, EIOÚ vidí možné negativní důsledky nadměrného oznamování a chtěl by pomoci zajistit, aby právní rámec přijatý ohledně oznamovací povinnosti při narušení bezpečnosti neměl tento následek. Pokud by jednotlivcům byla zasílána častá oznámení o narušení bezpečnosti, a to i v situacích, v nichž nedochází k poškození, ztrátě nebo nesnázím, může dojít k tomu, že budou narušeny klíčové cíle poskytování oznámení, protože jednotlivci mohou paradoxně ignorovat oznámení v těch případech, v nichž ve skutečnosti musí přijmout kroky k tomu, aby se ochránili. Úsilí o nalezení správné rovnováhy při poskytování smysluplného oznámení je proto důležité, neboť pokud jednotlivci na přijatá oznámení nereagují, účinnost režimů oznamování je značně omezena.
37. S cílem přijmout odpovídající kritérium, které nepovede k nadměrnému oznamování, je třeba vedle zohlednění podnětu pro oznámení zvážit i jiné faktory, zejména definici narušení bezpečnosti a informace, na něž se vztahuje oznamovací povinnost. V tomto ohledu EIOÚ poznamenává, že podle tří navrhovaných přístupů může být objem oznámení vysoký, a to vzhledem k výše projednávané široké definici narušení bezpečnosti. Tato obava ohledně nadměrného oznamování je umocněna skutečností, že se definice narušení bezpečnosti vztahuje na všechny druhy osobních údajů. Ačkoliv se EIOÚ domnívá, že se jedná o správný přístup (neomezovat typy osobních údajů, na něž se vztahuje oznamování), narozdíl od jiných přístupů, jako jsou právní předpisy USA, v nichž se požadavky zaměřují na citlivost údajů, jedná se o faktor, který je třeba vzít v úvahu.
38. S ohledem na výše uvedené skutečnosti a při celkovém zohlednění různých proměnných EIOÚ považuje za vhodné stanovit práh nebo normu, při jejichž nedosažení není oznamování povinné.
39. Zdá se, že obě navrhovaná kritéria, tj. že narušení představuje „*vážné ohrožení soukromí*“ nebo „*přiměřeně pravděpodobné poškození*“, zahrnují například společenské poškození nebo poškození dobré pověsti a hospodářskou ztrátu. Tato kritéria by se například zaměřila na případy, kdy je jednatel vystaven krádeži totožnosti prostřednictvím zveřejnění neveřejných identifikátorů, jako jsou čísla pasů, jakož i zveřejnění informací o soukromém životě jednotlivce. EIOÚ tento přístup vítá. Je přesvědčen, že přínosů oznamovací povinnosti při narušení bezpečnosti by nebylo plně dosaženo, pokud by se režim oznamování vztahoval pouze na narušení vedoucí k hospodářské újmě.

⁽¹³⁾ Viz poznámka pod čarou 11 týkající se výjimky z tohoto pravidla.

40. Ze dvou navrhovaných kritérií EIOÚ upřednostňuje kritérium Komise „*přiměřeně pravděpodobné způsobení škody*“, protože by se tak zajistila vhodnější míra ochrany jednotlivců. Narušení povedou mnohem pravděpodobněji k oznamování, pokud existuje „*přiměřená pravděpodobnost způsobení škody*“ soukromí jednotlivců, než pokud mají představovat „*závažné nebezpečí*“ vzniku takové škody. Proto pokud by do oblasti působnosti byla zahrnuta pouze narušení představující závažné nebezpečí pro soukromí jednotlivců, bylo by značně omezeno množství narušení, která musí být oznámena. Zahrnutí pouze takových narušení by poskytovatelům veřejně dostupných služeb elektronických komunikací a poskytovatelům služeb informační společnosti udělilo nadměrnou pravomoc rozhodnout o tom, zda je oznámení nutné, protože by pro ně bylo mnohem snadnější odůvodnit závěr, že neexistuje žádné „*závažné nebezpečí*“, než že k nebezpečí „*s přiměřenou pravděpodobností nedojde*“. Zatímco je třeba zcela jistě zabránit nadměrnému oznamování, je třeba v případě pochybností rozhodnout ve prospěch ochrany soukromých zájmů jednotlivců a jednotlivci by měli být chráněni přinejmenším v případech, že jim narušení s přiměřenou pravděpodobností způsobí škodu. Navíc spojení „*přiměřeně pravděpodobně*“ bude účinnější v praxi, a to jak pro zahrnuté subjekty, tak pro příslušné orgány, protože vyžaduje objektivní posouzení případu a jeho příslušných souvislostí.
41. Narušení osobních údajů může dále způsobit škodu, kterou je obtížné kvantifikovat a která se může lišit. Zveřejnění stejného druhu údajů může skutečně v závislosti na konkrétních okolnostech způsobit značnou škodu jednomu jednotlivci a menší škodu jinému. Kritérium, které by vyžadovalo, aby škoda byla hmotná, významná nebo závažná, by nebylo vhodné. Například přístup Rady, který vyžaduje, aby narušení *závažně* ovlivnilo něčí soukromí, by poskytl neodpovídající ochranu jednotlivcům, neboť takové kritérium vyžaduje, aby byl dopad na soukromí „*závažný*“. Navíc vzniká prostor pro subjektivní posouzení.
42. Výše uvedené spojení „*přiměřeně pravděpodobné poškození*“ se sice zdá být vhodným kritériem pro oznamování narušení bezpečnosti, EIOÚ se však i nadále obává, že by sem nemusely spadat všechny situace, v nichž je oznámení jednotlivcům zaručeno, tj. všechny situace, v nichž existuje přiměřená pravděpodobnost negativního dopadu na soukromí nebo jiná zákonná práva jednotlivců. Z tohoto důvodu by mohla být zváženo kritérium, které by vyžadovalo oznámení, „*pokud by narušení s přiměřenou pravděpodobností poškodilo jednotlivce*“.
43. Toto alternativní kritérium má další výhodu v tom, že je v souladu s právními předpisy EU v oblasti ochrany údajů. Směrnice o ochraně údajů vskutku často odkazuje k poškození práv a svobod subjektů údajů. Například článek 18 a 49. bod odůvodnění, které se zabývají povinnostmi registrovat zpracování údajů u orgánů pro ochranu osobních údajů, opravňují členské státy k výjimce z této povinnosti v případech, v nichž zpracování „*nejdou způsobit poškození práva a svobody subjektů údajů*“. Podobné znění je použito v čl. 16 odst. 6 společného postoje s cílem umožnit právníkům osobám podat žalobu na spammy.
44. Dále by s ohledem na výše uvedené bylo možno rovněž očekávat, že zahrnuté subjekty, a zejména příslušné orgány k prosazování právních předpisů na ochranu údajů, budou důvěrněji seznámeny s výše uvedenými kritérii, což usnadní jejich posouzení toho, zda příslušné narušení odpovídá požadovanému kritériu.
- Subjekt určující, zda narušení bezpečnosti odpovídá kritériu či nikoliv*
45. Podle přístupu Evropského parlamentu (vyjma případů přímého ohrožení) a pozměněného návrhu Komise bude na orgánech členských států, aby určily, zda narušení bezpečnosti odpovídá kritériu, které je podnětem pro povinnost informovat dotčené jednotlivce.
46. EIOÚ je přesvědčen, že zapojení určitého orgánu hraje důležitou roli při určování toho, zda bylo splněno kritérium, neboť je to do určité míry zárukou správného uplatňování právních předpisů. Takový režim může zabránit tomu, aby společnosti nesprávně posuzovaly narušení jako neškodlivé či nezávažné, a tím se vyhnuly oznamování v případech, kdy je takové oznamování ve skutečnosti nezbytné.
47. Na druhé straně se EIOÚ obává, že režim, na jehož základě mají orgány provádět posouzení, může být nepraktický a jeho uskutečnění obtížné, nebo se může ukázat, že je kontraproduktivní. Dokonce tak mohou být oslabena opatření na ochranu údajů pro jednotlivce.
48. Podle tohoto přístupu budou orgány na ochranu údajů pravděpodobně zaplaveny oznámeními narušení bezpečnosti a mohou čelit závažným obtížím při provádění nezbytných posouzení. Je důležité mít na paměti, že orgánům bude třeba poskytnout dostatečné důvěrné informace, často komplexní technické povahy, které budou muset velmi rychle zpracovat za účelem posouzení toho, zda narušení bezpečnosti odpovídá kritériu. Vzhledem k obtížím s posuzováním a ke skutečnosti, že některé orgány mají omezené zdroje, se EIOÚ obává, že bude pro orgány velmi obtížné splnit tuto povinnost a že by mohla ubírat zdroje určené pro jiné důležité priority. Takový režim může dále vyvíjet na orgány nepřiměřený tlak; pokud rozhodnou, že narušení není závažné, a jednotlivci přesto utrpí škodu, orgány by skutečně mohly být považovány za odpovědné.

49. Výše uvedená obtíž je ještě závažnější, pokud zohledníme, že čas je klíčovým faktorem při minimalizaci nebezpečí vyplývajících z narušení bezpečnosti. Nejsou-li orgány schopny provést posouzení během velmi krátké doby, může dodatečná lhůta, kterou orgány vyžadují pro provedení posouzení, zvýšit škody způsobené dotčeným jednotlivcům. Tento další krok, který má zajistit větší ochranu jednotlivcům, tak může paradoxně vést k tomu, že poskytnutá ochrana bude nižší, než u systémů založených na přímém oznamování.
50. Z výše uvedených důvodů se EIOÚ domnívá, že by bylo vhodnější vytvořit systém, v němž by měly příslušné subjekty posoudit, zda narušení odpovídá kritériu či nikoliv, jak to stanoví přístup Rady.
51. Avšak aby se zabránilo nebezpečí možného zneužití, například pokud jde o subjekty odmítající učinit oznámení za okolností, v nichž se oznámení zcela jasně vyžaduje, je nanejvýš důležité zahrnout jistá bezpečnostní opatření na ochranu údajů uvedená níže.
52. Zprv, povinnost určit, zda je třeba učinit oznámení, kterou mají zahrnuté subjekty, musí být samozřejmě doplněna další povinností vyžadující povinné oznamovat orgánům všechna narušení odpovídající požadovanému kritériu. Příslušné subjekty by v takových případech měly mít povinnost informovat orgány o narušení a o důvodech jejich rozhodnutí ohledně oznámení a o obsahu jakéhokoli učiněného oznámení.
53. Z druhé, orgánům musí být udělena skutečná dozorcí úloha. Při plnění této úlohy musí být orgánům povoleno, nikoliv však přikázáno, vyšetřit okolnosti narušení a požadovat odpovídající nápravné opatření⁽¹⁴⁾. To by mělo zahrnovat nejen oznamování jednotlivcům (pokud se tak ještě nestalo), ale rovněž možnost uložení povinnosti učinit kroky k zabránění dalších narušení. Orgánům by měly být v tomto ohledu uděleny účinné pravomoci a zdroje a musí mít nezbytnou volnost k tomu, aby rozhodly, kdy je třeba reagovat na oznámení narušení bezpečnosti. Jinak řečeno, umožnilo by to orgánům, aby byly selektivní a prováděly vyšetřování například rozsáhlých a skutečně závažných narušení bezpečnosti, přičemž
- by ověřovaly a prosazovaly plnění požadavků právních předpisů.
54. S cílem dosáhnout výše uvedeného, a vedle pravomocí přiznaných v rámci směrnice o soukromí a elektronických komunikacích, jako je čl. 15a odst. 3 a směrnice o ochraně údajů, doporučuje EIOÚ vložit toto znění: „*Nebylo-li dotčenému účastníkovi nebo jednotlivci již zasláno oznámení, může příslušný vnitrostátní orgán po zvážení povahy narušení požadovat, aby tak učinili poskytovatelé veřejně dostupných služeb elektronických komunikací nebo poskytovatelé služeb informační společnosti.*“
55. EIOÚ dále doporučuje Evropskému parlamentu a Radě, aby potvrdily povinnost navrženou Evropským parlamentem (změna č. 122, čl. 4. odst. 1a), podle níž mají subjekty provádět posuzování rizik a jejich identifikaci ve svých systémech a v osobních údajích, které mají v úmyslu zpracovat. Na základě této povinnosti vypracují subjekty upravenou a přesnou definici bezpečnostních opatření, která budou použita v jejich případech a která by měly být orgánům k dispozici. Dojde-li k narušení bezpečnosti, pomůže tato povinnost zahrnutým subjektům, a případně rovněž orgánům při jejich dozorcí úloze, určit, zda ohrožení takové informace může mít za následek nepříznivý dopad na jednotlivce nebo ho může poškodit.
56. Zatřetí, povinnost zahrnutých subjektů určit, zda musí učinit oznámení jednotlivcům, musí být doplněna povinností vést podrobný a komplexní záznam interního auditu uvádějící všechna narušení, k nimž došlo, a všechna související oznámení, jakož i všechna opatření přijatá s cílem zabránit budoucím narušením. Tento záznam vnitřního auditu musí být orgánům k dispozici za účelem přezkumu a možného prošetření. Umožní to orgánům plnit jejich dozorcí úlohu. Toho by mohlo být dosaženo přijetím níže uvedeného znění: „*Poskytovatelé veřejně dostupných služeb elektronických komunikací a poskytovatelé služeb informační společnosti vedou a uchovávají komplexní záznamy podrobně uvádějící všechna narušení bezpečnosti, k nimž došlo, příslušné související technické informace a přijatá nápravná opatření. Záznamy rovněž obsahují odkaz na všechna oznámení určená dotčeným účastníkům nebo jednotlivcům a příslušným vnitrostátním orgánům, včetně jejich data a obsahu. Záznamy se na požádání poskytnou příslušnému vnitrostátnímu orgánu.*“
57. Aby byla zajištěna soudržnost při zavádění tohoto kritéria, jakož i jiné důležité aspekty rámce týkajícího se narušení bezpečnosti, jako je formát a postupy pro oznamování, bylo by samozřejmě vhodné, aby Komise po konzultaci s EIOÚ, s Pracovní skupinou zřízenou podle článku 29 a s příslušnými zúčastněnými stranami přijala technická prováděcí opatření.

⁽¹⁴⁾ Článek 15a odst. 3 uznává tuto dohlížecí pravomoc stanovením, že „členské státy zajistí, aby příslušné vnitrostátní orgány a případně další vnitrostátní orgány měly veškerou vyšetřovací pravomoc a zdroje nezbytné ke sledování a vynucování vnitrostátních předpisů přijatých podle této směrnice, včetně možnosti získat všechny příslušné informace, jež k tomu mohou potřebovat.“

Příjemci oznámení

58. Pokud jde o příjemce oznámení, EIOÚ upřednostňuje terminologii Evropského parlamentu a Komise před terminologií Rady. Evropský parlament nahradil slovo „účastníci“ slovem „uživatelé“. Komise používá pojmy „uživatelé“ a „dotčený jednotlivce“. Znění Evropského parlamentu i znění Komise by mezi příjemce oznámení nezahrnula pouze stávající účastníky, ale rovněž bývalé účastníky a třetí osoby, jako jsou uživatelé, kteří jsou ve spojení s některými zahrnutými subjekty bez toho, aniž by se stali jejich účastníky. EIOÚ tento přístup vítá a vyzývá Evropský parlament a Radu, aby jej zachovaly.

59. EIOÚ si však uvědomuje mnoho nesrovnalostí, pokud jde o terminologii v prvním čtení EP, jimiž je třeba se zabývat. Například slovo „účastníci“ bylo ve většině případů, nikoliv však ve všech, nahrazeno slovem „uživatelé“, v jiných případech slovem „spotřebitelé“. To je třeba harmonizovat.

III. OBLAST PŮSOBNOSTI SMĚRNICE O SOUKROMÍ A ELEKTRONICKÝCH KOMUNIKACÍCH: VEŘEJNÉ A SOUKROMÉ SÍTĚ

60. V čl. 3 odst. 1 stávající směrnice o soukromí a elektronických komunikacích jsou stanoveny subjekty, jichž se tato směrnice v první řadě týká, tj. ty, které zpracovávají údaje „ve spojení s“ poskytováním veřejně dostupných služeb elektronických komunikací ve veřejných sítích⁽¹⁵⁾. Příklady činností poskytovatelů veřejně dostupných služeb elektronických komunikací zahrnují poskytování přístupu k internetu, přenos informací prostřednictvím elektronických sítí, mobilní a telefonní spojení atd.

61. Evropský parlament předložil změnu č. 121, kterou se mění článek 3 původního návrhu Komise, podle níž byla oblast působnosti směrnice o soukromí a elektronických komunikacích rozšířena tak, aby zahrnula „zpracování osobních údajů ve spojení s poskytováním veřejně dostupných služeb elektronických komunikací ve veřejných a soukromých komunikačních sítích a veřejně dostupných soukromých sítí ve Společenství, [...]“ (čl. 3 odst. 1 směrnice o soukromí a elektronických komunikacích). Pro Radu a Komisi bylo bohužel obtížné přijmout tuto změnu, a proto tento přístup nezpracovaly do společného postoje ani do pozměněného návrhu.

Použití směrnice o soukromí a elektronických komunikacích na veřejně přístupné soukromé sítě

62. Z níže uvedených důvodů a s cílem podpořit shodu EIOÚ vybízí k tomu, aby byla zachována podstata změny č. 121. EIOÚ kromě toho navrhuje zahrnout změnu, která

pomůže dále objasnit druhy služeb, na něž by se vztahovala rozšířená oblast působnosti.

63. Soukromé sítě se často používají k poskytování služeb elektronických komunikací, jako je přístup k internetu určenému množství osob, které může být velké. Jedná se například o přístup na internet v internetových kavárnách a prostřednictvím přístupových bodů Wi-Fi v hotelích, restauracích, na letištích, ve vlacích a v jiných zařízeních přístupných veřejnosti, kde jsou takové služby často poskytovány jako doplněk k jiným službám (nápoje, ubytování apod.)

64. Ve všech výše uvedených příkladech jsou komunikační služby, např. přístup k internetu, poskytovány veřejnosti nikoliv prostřednictvím veřejné sítě, ale spíše prostřednictvím sítě, která může být považována za soukromou, tj. prostřednictvím soukromě provozované sítě. Ačkoliv ve výše uvedených případech jsou komunikační služby poskytovány veřejnosti, druh použité sítě je spíše soukromý než veřejný, poskytování těchto služeb proto pravděpodobně není pokryto celou směrnicí o soukromí a elektronických komunikacích nebo alespoň některými z jejích článků⁽¹⁶⁾. Základní práva jednotlivců zaručená směrnicí o soukromí a elektronických komunikacích proto nejsou v těchto případech chráněna a pro uživatele, kteří využívají téhož přístupu ke službě připojení na internet prostřednictvím veřejných telekomunikačních prostředků, vzniká ve vztahu k těm, kteří využívají přístup prostřednictvím soukromých telekomunikačních prostředků, nerovný právní stav. To vše i navzdory skutečnosti, že ohrožení soukromí jednotlivců a osobních údajů ve všech těchto případech je stejné jako v případě, že jsou k přenášení služeb použity veřejné sítě. Souhrnně řečeno, zdá se, že není důvod, který by podle této směrnice ospravedlňoval různý přístup ke komunikačním službám poskytovaným prostřednictvím soukromé sítě a k těm, které jsou poskytovány prostřednictvím veřejné sítě.

65. Proto by EIOÚ podpořil změnu, jako je změna č. 121 Evropského parlamentu, podle níž by se směrnice o soukromí a elektronických komunikacích rovněž použila na zpracování osobních údajů ve spojení s poskytováním veřejně dostupných služeb elektronické komunikace v soukromých komunikačních sítích.

66. EIOÚ však uznává, že toto znění by mohlo mít nepředvídatelné a případně nezamýšlené důsledky. Pouhý odkaz k soukromým sítím by vskutku mohl být vykládán tak, že se vztahuje na situace, na něž se tato směrnice zcela jistě

⁽¹⁵⁾ „Tato směrnice se vztahuje na zpracování osobních údajů ve spojení s poskytováním veřejně dostupných služeb elektronických komunikací ve veřejných komunikačních sítích.“

⁽¹⁶⁾ Naopak by bylo možné namítnout, že vzhledem k tomu, že jsou komunikační služby poskytovány veřejnosti, i když je síť soukromá, vztahuje se na poskytování těchto služeb stávající právní rámec, a to i navzdory skutečnosti, že síť je soukromá. Například ve Francii se zaměstnavatelé poskytující přístup k internetu svým zaměstnancům považují za rovnocenné poskytovatelům přístupu na internet, kteří nabízejí přístup k internetu na komerčním základě. Tento výklad není v široké míře přijímán.

vztahovat nemá. Například by bylo možno tvrdit, že doslovný nebo přesný výklad tohoto znění by mohl do oblasti působnosti směrnice zahrnout domácnosti⁽¹⁷⁾ vybavené připojením Wi-Fi, které umožňuje připojení komukoliv v jejich okolí (obvykle v domácnosti); i když to není cílem změny č. 121. Aby se zabránilo takovému výsledku, EIOÚ navrhuje změnu formulace změny č. 121, kterou se do oblasti působnosti směrnice o soukromí a elektronických komunikacích zahrnuje „*zpracování osobních údajů ve spojení s poskytováním veřejně dostupných služeb elektronických komunikací ve veřejných nebo veřejně přístupných soukromých komunikačních sítích ve Společenství, ...*“

67. To by pomohlo objasnit, že se směrnice o soukromí a elektronických komunikacích vztahuje pouze na soukromé sítě, které jsou veřejně přístupné. Použitím ustanovení směrnice o soukromí a elektronických komunikacích pouze na veřejně přístupné soukromé sítě (a nikoliv na všechny soukromé sítě) se použití směrnice omezí tak, aby se vztahovala pouze na služby komunikace poskytované v soukromých sítích, které jsou záměrně zpřístupňovány veřejnosti. Tato formulace pomůže ještě více zdůraznit, že dostupnost soukromé sítě široké veřejnosti je klíčovým faktorem při stanovování toho, zda se směrnice bude na daný případ vztahovat (vedle poskytování veřejně dostupných komunikačních služeb). Jinak řečeno, bez ohledu na to, zda je síť veřejná nebo soukromá, je-li síť záměrně zpřístupněná veřejnosti s cílem poskytnout službu veřejné komunikace, jako je přístup k internetu, a to i když se jedná o doplňkovou službu k jiné službě (např. ubytování v hotelu), směrnice o soukromí a elektronických komunikacích by se na tento druh služby či sítě vztahovala.

68. EIOÚ poznamenává, že výše podpořený přístup, podle něž se směrnice o soukromí a elektronických komunikacích použije na veřejně přístupné soukromé sítě, je v souladu s přístupy přijatými v několika členských státech, v nichž orgány již považují takové druhy služeb, jakož i služby poskytované prostřednictvím zcela soukromých sítí, za spadající do oblasti působnosti vnitrostátních ustanovení provádějících směrnici o soukromí a elektronických komunikacích⁽¹⁸⁾.

69. S cílem dosáhnout větší právní jistoty ohledně subjektů, na něž se vztahuje nová oblast působnosti, by mohlo být užitečné zahrnout do směrnice o soukromí a elektronických komunikacích změnu definující „*veřejně přístupnou soukromou síť*“, jež by mohla znít takto: „*veřejně přístupnou soukromou síť se rozumí soukromě provozovaná síť, k níž má široká veřejnost zpravidla neomezený přístup, za úplatu i zdarma nebo ve spojení s jinými službami nebo nabídkami, pod podmínkou přijetí platných podmínek.*“

70. V praxi by výše uvedený přístup znamenal, že by se na soukromé sítě v hotelích a jiných zařízeních, které poskytují přístup k internetu široké veřejnosti prostřednictvím soukromé sítě, směrnice vztahovala. Naproti tomu by se nevztahovala na poskytování komunikačních služeb ve zcela soukromých sítích, v nichž je služba omezena na určitou skupinu identifikovatelných jednotlivců. Proto by se například na virtuální soukromé sítě a na domácnosti spotřebitelů vybavené Wi-Fi směrnice nevztahovala. Rovněž by se nevztahovala na služby poskytované prostřednictvím výlučně korporátních sítí.

Soukromé sítě v oblasti působnosti směrnice o soukromí a elektronických komunikacích

71. Vyloučení soukromých sítí samo o sobě, jak je navrženo výše, by mělo být považováno za dočasné opatření, o němž by se mělo dále jednat. S ohledem na jedné straně na důsledky, které má vyloučení zcela soukromých sítí jako takových pro soukromí, a na druhé straně na skutečnost, že to má dopad na velký počet osob, které se obvykle připojují k internetu prostřednictvím korporátních sítí, bude možná v budoucnosti třeba tuto věc ještě jednou zvážit. Z tohoto důvodu a s cílem podpořit diskusi o tomto tématu EIOÚ doporučuje vložit do směrnice o soukromí a elektronických komunikacích bod odůvodnění, podle něhož by Komise provedla veřejnou konzultaci o použití směrnice o soukromí a elektronických komunikacích na všechny soukromé sítě, a to s použitím informací od EIOÚ, orgánů na ochranu osobních údajů a dalších příslušných zúčastněných stran. Tento bod odůvodnění by mohl dále stanovit, že v důsledku veřejné konzultace by Komise měla předložit odpovídající návrh na rozšíření nebo omezení druhů subjektů, na něž by se měla směrnice o soukromí a elektronických komunikacích vztahovat.

72. Kromě výše uvedeného by měly být jednotlivé články směrnice o soukromí a elektronických komunikacích odpovídajícím způsobem změněny tak, aby všechna provozní ustanovení výslovně odkazovala vedle veřejných sítí i k veřejně dostupným soukromým sítím.

IV. ZPRACOVÁNÍ PROVOZNÍCH ÚDAJŮ PRO BEZPEČNOSTNÍ ÚČELY

73. Během legislativního procesu týkajícího se přezkumu směrnice o soukromí a elektronických komunikacích trvaly společnosti poskytující bezpečnostní služby na tom, že je nezbytné vložit do směrnice o soukromí a elektronických komunikacích ustanovení opravňující ke shromažďování provozních údajů s cílem zaručit účinnou bezpečnost on-line.

⁽¹⁷⁾ Obvykle bezdrátové místní sítě (LAN).

⁽¹⁸⁾ Viz poznámka pod čarou 16.

74. Proto Evropský parlament vložil změnu č. 181, kterou se zavádí nový čl. 6 odst. 6a, jež by výslovně opravňoval ke zpracování provozních údajů pro bezpečnostní účely: „Aniž je dotčeno dodržování jiných ustanovení, než je článek 7 směrnice 95/46/ES a článek 5 této směrnice, provozní údaje mohou být zpracovávány v oprávněném zájmu správce údajů za účelem provádění technických opatření, která mají zajistit bezpečnost sítí a informací veřejných služeb elektronických komunikací, veřejné či soukromé sítě elektronických komunikací, služeb informační společnosti či souvisejícího koncového zařízení nebo zařízení elektronické komunikace, jak je stanoveno v čl. 4 písm. c) nařízení Evropského parlamentu a Rady (ES) č. 460/2004 ze dne 10. března 2004 o zřízení Evropské agentury pro bezpečnost sítí a informací, s výjimkou případů, kdy nad těmito zájmy převáží zájmy týkající se základních práv a svobod subjektu údajů. Toto zpracování se musí omezit pouze na skutečnosti, které jsou pro účely těchto bezpečnostních činností zcela nezbytné“.

75. Pozměněný návrh Komise tuto změnu v zásadě přijal, avšak byla odstraněna klíčová klauzule, kterou mělo být zajištěno dodržování ostatních ustanovení uvedené směrnice, znějící takto: „Aniž je dotčena [...]... této směrnice“. Rada přijala přepracovanou verzi, které ještě více oslabuje důležitou ochranu a vyvážení zájmů, které byly zapracovány do změny č. 181, a to přijetím tohoto znění: „Provozní údaje lze zpracovávat v míře nezbytně nutné k zajištění [...] bezpečnosti sítí a informací podle definice čl. 4 písm. c) nařízení Evropského parlamentu a Rady (ES) 460/2004 ze dne 10. března 2004 o zřízení Evropské agentury pro bezpečnost sítí a informací.“

76. Jak je dále objasněno níže, čl. 6 odst. 6a není nutný a může být zneužit, zejména pokud bude přijat v podobě, která neobsahuje důležitá bezpečnostní opatření, klauzule respektující jiná ustanovení uvedené směrnice a vyvážení zájmů. Proto EIOÚ doporučuje tento článek odmítnout, nebo alespoň zajistit, aby jakýkoliv takový článek týkající se této otázky obsahoval druhy bezpečnostních opatření, které byly zahrnuty do změny č. 181 ve znění přijatém EP.

Právní důvody pro zpracování provozních údajů použitelné na služby elektronických komunikací a na jiné správce údajů podle stávajících právních předpisů o ochraně údajů

77. Rozsah, v němž poskytovatelé veřejně dostupných služeb elektronických komunikací mohou zákonně zpracovat provozní údaje, je upraven podle článku 6 směrnice o soukromí a elektronických komunikacích, který omezuje zpracování provozních údajů na omezené účely, jako je účtování, propojení a marketing. Toto zpra-

cování může být provedeno pouze za zvláštních podmínek, jako je souhlas jednotlivců v případě marketingu. Kromě toho mohou jiní správci údajů, jako jsou poskytovatelé služeb informační společnosti, zpracovávat provozní údaje podle článku 7 směrnice o ochraně údajů, který stanoví, že správci údajů mohou zpracovávat osobní údaje, pokud je splněn alespoň jeden z právních základů uvedených na seznamu, přičemž na tyto právní základy se rovněž odkazuje jako na právní důvody.

78. Příkladem jednoho takového právního základu je čl. 7 písm. a) směrnice na ochranu údajů, který vyžaduje souhlas subjektu údajů. Například pokud si intranetový maloobchodní prodejce přeje zpracovat provozní údaje pro účely zaslání reklamních či marketingových materiálů, musí obdržet souhlas jednotlivce. Jiný právní základ stanovený v článku 7 může v některých případech umožnit zpracování provozních údajů pro bezpečnostní účely například bezpečnostními společnostmi nabízejícími bezpečnostní služby. To je založeno na čl. 7 písm. f), který stanoví, že správci údajů mohou zpracovat osobní údaje, pokud je to „nezbytné pro uskutečnění oprávněných zájmů správce nebo třetí osoby či osob, kterým jsou údaje sdělovány, za podmínky, že nepřevyšují zájem na základních právech a svobodách subjektu údajů“. Směrnice na ochranu údajů blíže nestanoví případy, v nichž by zpracování osobních údajů splňovalo tento požadavek. Toto určení provádějí správci údajů pro každý případ zvlášť, často se souhlasem vnitrostátních orgánů na ochranu údajů a jiných orgánů.

79. Je třeba zvážit souvislost mezi článkem 7 směrnice o ochraně údajů a navrhovaným čl. 6 odst. 6a směrnice o soukromí a elektronických komunikacích. Navrhovaný článek 6 odst. 6a stanoví okolnosti, za nichž by byly splněny požadavky čl. 7 písm. f) uvedené výše. Tím, že povoluje zpracování provozních údajů s cílem pomoci zajistit bezpečnost sítí a informací, čl. 6 odst. 6a samozřejmě umožňuje takové zpracování pro účely oprávněného zájmu sledovaného správcem údajů.

80. Jak je podrobněji objasněno níže, EIOÚ se domnívá, že navrhovaný čl. 6 odst. 6a není nezbytný ani užitečný. Z právního hlediska je totiž v zásadě zbytečné stanovit, zda konkrétní druh činnosti související se zpracováním údajů, v tomto případě zpracování provozních údajů pro bezpečnostní účely, splňuje nebo nesplňuje požadavky čl. 7 písm. f) směrnice o ochraně údajů, a v takovém případě může být souhlas jednotlivce nezbytný podle čl. 7 písm. a). Jak je uvedeno výše, toto posouzení obvykle provedou správci údajů, tj. společnosti, a to na úrovni provádění a za konzultace s orgány na ochranu údajů; v případě potřeby toto posouzení provádějí soudy. Obecně řečeno, EIOÚ se domnívá, že ve zvláštních případech oprávněné zpracování údajů pro bezpečnostní účely

prováděné bez ohrožení základních práv a svobod jednotlivců pravděpodobně splní požadavky čl. 7 písm. f) směrnice o ochraně údajů, a proto je možno je provádět. Navíc v oblasti ochrany údajů a směrnice o soukromí a elektronických komunikacích není jiný precedent pro specifikování nebo poskytnutí zvláštního přístupu k některým druhům činností zpracování údajů, které by splnily požadavky čl. 7 písm. f), a nebylo prokázáno, že je takové výjimky zapotřebí. Naopak, jak je uvedeno výše, se zdá, že v mnoha případech by tento druh činnosti bylo možno bez obtíží zařadit do rámce stávajícího znění. Proto je právní ustanovení, které potvrzuje toto posouzení, v zásadě zbytečné.

Znění čl. 6 odst. 6a podle Evropského parlamentu, Rady a Komise

81. Jak je uvedeno výše, ačkoliv je to zbytečné, je třeba zdůraznit, že změna č. 181 ve znění přijatém Evropským parlamentem byla navržena v určité míře s ohledem na zásady pro ochranu soukromí a údajů zakotvené v právních předpisech o ochraně údajů. Změna Evropského parlamentu č. 181 by se mohla více zabývat zájmem na ochraně údajů a soukromí, například vložení slov „ve zvláštních případech“ s cílem zajistit selektivní uplatňování tohoto článku nebo začleněním období zachovávaného stávající stav.
82. Změna 181 obsahuje některé pozitivní prvky. Potvrzuje, že zpracování by mělo být ve shodě se všemi ostatními zásadami pro ochranu údajů, které se vztahují na zpracování osobních údajů („Aniž je dotčeno...dodržování ustanovení [...] směrnice 95/46/ES a [...] této směrnice“). Dále ačkoliv změna č. 181 dovoluje zpracování provozních údajů z bezpečnostních důvodů, usiluje o rovnováhu mezi zájmy subjektu, který zpracovává provozní údaje, a zájmy jednotlivců, jejichž údaje jsou zpracovávány tak, že takové zpracování údajů může být provedeno pouze tehdy, pokud nad zájmy ohledně základních práv a svobod jednotlivců nepřeváží zájmy subjektu zpracovávajícího údaje („s výjimkou případů, kdy nad těmito zájmy převáží zájmy týkající se základních práv a svobod subjektu údajů“). Tento požadavek je důležitý, protože může umožnit zpracování provozních údajů pro zvláštní účely, avšak neumožní subjektu zpracovávajícímu údaje zpracovat provozní údaje hromadně.
83. Přepřísádané znění této změny předložené Radou obsahuje vítané prvky, jako je zachování slov „zcela nezbytné“, což zdůrazňuje omezenou oblast působnosti tohoto článku. Nicméně ze znění Rady byla vypuštěna ochrana údajů a ochrana soukromí uvedené výše. Zatímco se v zásadě použijí obecná ustanovení na ochranu údajů, bez ohledu na to, zda je v každém případě učiněn zvláštní odkaz, znění čl. 6 odst. 6a navržené Radou může být interpretováno tak, že poskytuje pravomoc ke zpracování provozních údajů podle uvážení, aniž by se na ně vztahovala jakákoliv ochrana údajů a ochrana soukromí, jež se vztahuje na každé zpracování provozních údajů. Proto by

bylo možno argumentovat, že provozní údaje je možno shromažďovat, uchovávat a dále využívat, aniž by musely být splněny zásady pro ochranu údajů a zvláštní povinnosti, které se jinak použijí na odpovědné strany, jako je zásada kvality nebo povinnost spravedlivého a zákonného zpracování a zachování důvěrnosti a bezpečnosti údajů. Vzhledem k tomu, že není učiněn žádný odkaz na použitelné zásady pro ochranu údajů, které stanoví časové lhůty pro uchovávání informací nebo zvláštní časové lhůty v rámci tohoto článku, znění Rady je možno vykládat tak, že umožňuje shromažďování a zpracování provozních údajů pro bezpečnostní účely na nestanovené časové období.

84. Rada navíc v některých částech znění zmírnila ochranu soukromí možným rozšířením formulace. Například byl odstraněn odkaz na „oprávněný zájem správce údajů“, čímž vznikly pochybnosti ohledně druhů subjektů, které by mohly využít této výjimky. Je nanejvýš důležité zabránit uživatelům nebo právním subjektům, aby této změny využili.
85. Nedávné zkušenosti v Evropském parlamentu a Radě ukazují, že je obtížné zákonem stanovit rozsah a podmínky, za nichž může být zpracování údajů pro bezpečnostní účely zákonně provedeno. Je nepravděpodobné, že by kterýkoliv stávající nebo budoucí článek odstranil zjevné riziko příliš širokého použití výjimky z jiných důvodů než z výlučně bezpečnostních nebo použití ze strany subjektů, které by neměly mít možnost využít této výjimky. To neznamená, že k takovému zpracování nemůže nikdy dojít. Avšak to, zda a do jaké míry může být prováděno, lze lépe posoudit na úrovni provádění. Subjekty, které si přejí účastnit se takového zpracování, by měly projednat rozsah a podmínky s orgány na ochranu údajů a případně s Pracovní skupinou článku 29. Nebo by směrnice o soukromí a elektronických komunikacích mohla zahrnovat článek umožňující zpracování provozních údajů pro bezpečnostní účely, po výslovném schválení ze strany orgánů na ochranu údajů.
86. Při současném zohlednění nebezpečí, které čl. 6 odst. 6a představuje pro základní právo na ochranu údajů a soukromí jednotlivců, a skutečnosti, že z právního hlediska je tento článek zbytečný, jak je uvedeno ve stanovisku, EIOÚ dospěl k závěru, že nejlepší řešení by bylo, kdyby byl čl. 6 odst. 6a celý vypuštěn.
87. Mělo-li by být vedle znění stávajícího čl. 6 odst. 6a přijato nějaké znění odporující doporučení EIOÚ, mělo by v každém případě obsahovat výše projednané opatření na ochranu údajů. Rovněž by mělo být řádně začleněno do stávající struktury článku 6, nejlépe jako nový odstavec 2a.

**V. MOŽNOST PRÁVNÍCH OSOB PODAT ŽALOBU NA
PORUŠENÍ SMĚRNICE O SOUKROMÍ
A ELEKTRONICKÝCH KOMUNIKACÍCH**

88. Evropský parlament předložil změnu č. 133 umožňující poskytovatelům přístupu k internetu a jiným právním subjektům, jako jsou sdružení spotřebitelů, podat žalobu na porušení některého z ustanovení směrnice o soukromí a elektronických komunikacích⁽¹⁹⁾. Bohužel ji Komise ani Rada nepřijaly. EIOÚ považuje tuto změnu za velmi pozitivní a doporučuje její zachování.
89. Pro pochopení důležitosti této změny je třeba si uvědomit, že v oblasti ochrany soukromí a údajů škoda způsobená jednotlivé osobě obvykle sama o sobě nedostačuje k podání žaloby k soudu. Jednotlivci se obvykle samostatně neobrací na soud kvůli spamům nebo kvůli tomu, že jejich jméno bylo neoprávněně zaneseno do seznamu. Tato změna by umožnila sdružením spotřebitelů a odborům zastupujícím zájmy spotřebitelů podat jejich jménem hromadnou žalobu k soudu. Větší rozmanitost donucovacích mechanismů pravděpodobně rovněž podpoří větší shodu, a je proto v zájmu účinného použití ustanovení směrnice o soukromí a elektronických komunikacích.
90. V právních rámcích některých členských států jsou právní precedenty, které již předpokládají možnost kolektivního odškodnění s cílem umožnit spotřebitelům nebo zájmovým skupinám požadovat náhradu škody od strany, která škodu způsobila.
91. Soutěžní právo některých členských států⁽²⁰⁾ navíc opravňuje spotřebitele, zájmové skupiny (vedle *poškozeného konkurenta*) podat žalobu proti subjektu, který se dopouští porušování. Důvodem tohoto přístupu je, že ze situace pravděpodobně těží společnosti jednající v rozporu se soutěžním právem, protože spotřebitelé, kteří utrpěli pouze nepatrnou škodu, obvykle žalobu nepodávají. Tento důvod je možno obdobně použít v oblasti ochrany údajů a soukromí.
92. Důležitější je, jak je uvedeno výše, že právo právních subjektů, jako jsou sdružení spotřebitelů a poskytovatelé veřejně dostupných služeb elektronických komunikací, podávat žaloby posiluje postavení spotřebitelů a podporuje celkovou shodu s právními předpisy na ochranu údajů. Jsou-li společnosti, které se dopouštějí porušování, vystaveny většímu riziku soudního řízení, pravděpodobně budou více investovat do zajištění souladu s právními předpisy v oblasti ochrany údajů, což z dlouhodobého hlediska zlepší úroveň ochrany soukromí a spotřebitele. Ze všech těchto důvodů EIOÚ vyzývá Evropský parlament a Radu k přijetí ustanovení, které

právním subjektům umožní podat žalobu na porušení kteréhokoliv ustanovení směrnice o soukromí a elektronických komunikacích.

VI. ZÁVĚR

93. Společný postoj Rady, první čtení v Evropském parlamentu a pozměněný návrh Komise obsahují v různé míře pozitivní prvky, které slouží k posílení ochrany soukromí a osobních údajů jednotlivce.
94. Avšak EIOÚ se domnívá, že existuje prostor pro zlepšení, zejména pokud jde o společný postoj Rady, který bohužel nezachoval některé změny Evropského parlamentu, které mají za cíl pomoci zajistit odpovídající ochranu soukromí a osobních údajů jednotlivce. EIOÚ naléhavě vyzývá Evropský parlament a Radu k opětovnému začlenění opatření na ochranu soukromí obsažených v prvním čtení Evropského parlamentu.
95. EIOÚ se dále domnívá, že by bylo vhodné zjednodušit některá ustanovení této směrnice. To zejména platí v případě ustanovení týkajících se narušení bezpečnosti, protože EIOÚ se domnívá, že oznamování narušení bude mít největší přínos, bude-li právní rámec stanoven od samého počátku. EIOÚ se v neposlední řadě domnívá, že by bylo vhodné zlepšit a objasnit znění některých ustanovení této směrnice.
96. S ohledem na výše uvedené EIOÚ naléhavě vyzývá Evropský parlament a Radu, aby zvýšily úsilí ke zlepšení a objasnění některých ustanovení směrnice o soukromí a elektronických komunikacích a současně aby znovu začlenily změny přijaté v prvním čtení Evropského parlamentu zaměřené na poskytování ochrany soukromí a údajů na odpovídající úrovni. Za tímto účelem jsou v níže uvedených bodech 97, 98, 99 a 100 shrnuta příslušná témata a předloženy některá z doporučení a návrhů. EIOÚ vyzývá všechny zúčastněné strany, aby je zohlednily, protože projednávání směrnice o soukromí a elektronických komunikacích směřuje ke konečnému přijetí.

Narušení bezpečnosti

97. Evropský parlament, Komise i Rada přijaly různé přístupy k oznamování narušení bezpečnosti. Mezi těmito třemi modely jsou rozdíly mimo jiné pokud jde o subjekty, na něž se vztahuje povinnost, kritérium nebo podnět pro oznámení, subjekty údajů oprávněné k tomu, aby jim bylo podáno oznámení, atd. Je třeba, aby Evropský parlament a Rada učinily vše pro vypracování pevného právního rámce pro případy narušení bezpečnosti. Za tímto účelem by Evropský parlament a Rada měly:

⁽¹⁹⁾ Článek 13 odst. 6 prvního čtení Evropského parlamentu.

⁽²⁰⁾ Viz například § 8 německého zákona o nekalé soutěži (UWG).

- zachovat definici narušení bezpečnosti ve zněních Evropského parlamentu, Rady a Komise, protože je dostatečně široká k tomu, aby zahrnula většinu situací, v nichž by mělo být oznámení narušení bezpečnosti zaručeno;
 - zahrnout poskytovatele služeb informační společnosti, s ohledem na oblast působnosti subjektů, na něž se vztahuje navržený požadavek na oznamování. Pravděpodobnost, že u internetových maloobchodníků, internetových bank a on-line lékáren dojde k narušení bezpečnosti, je stejná, ne-li vyšší, jako v případě telekomunikačních společností. Občané budou očekávat, že jim bude podáno oznámení nejen v případě, že se poskytovatelé přístupu k internetu stanou předmětem narušení bezpečnosti, ale zejména tehdy, stane-li se to jejich internetovým bankám a on-line lékárnám.
 - Pokud jde o podnět k oznámení, kritérium „*přiměřená pravděpodobnost poškození*“ uvedené v pozměněném návrhu je vhodným kritériem, které zajistí funkčnost režimu. Nicméně je důležité zajistit, aby pojem „poškození“ byl dostatečně široký k pokrytí všech příslušných případů negativních dopadů na soukromí nebo jiné oprávněné zájmy jednotlivců. V opačném případě by bylo vhodnější stanovit nové kritérium, na jehož základě by oznamování bylo povinné „*pokud by narušení s přiměřenou pravděpodobností mohlo poškodit jednotlivce*“. Přístup Rady, který vyžaduje, aby narušení závažně narušilo něčí soukromí, by poskytl jednotlivcům nedostatečnou ochranu, protože takové kritérium vyžaduje, aby byl dopad na soukromí „závažný“. Navíc vzniká prostor pro subjektivní posouzení.
 - I když má účast orgánu na stanovení, zda musí dotčený subjekt podat oznámení jednotlivcům, zcela jistě pozitivní účinky, v praxi může být obtížné účast orgánu zajistit a rovněž by to mohlo odebírat zdroje z jiných důležitých priorit. Nemohou-li orgány reagovat velmi rychle, EIOÚ se obává, že takový systém může dokonce oslabit ochranu jednotlivců a vyvinout nepřiměřený tlak na orgány. EIOÚ proto doporučuje vytvořit systém, v němž je na dotčených subjektech, aby posoudily, zda musí provést oznámení.
 - Provést níže uvedená ochranná opatření s cílem umožnit orgánům výkon dozoru nad posouzením učiněným zahrnutými subjekty ohledně toho, zda učinit oznámení:
 - zajistit, aby takové subjekty byly povinny podat oznámení orgánům o všech narušeních, které odpovídají požadovanému kritériu;
 - pověřit orgány dozorčí úlohou, která jim umožní postupovat selektivně, a být tak efektivní. Za účelem dosažení výše uvedeného je třeba vložit toto znění: „*Nebylo-li dotčenému účastníkovi nebo jednotlivci již učiněno oznámení, může příslušný vnitrostátní orgán, po zvážení povahy narušení, požadovat po poskytovatelích veřejně dostupných služeb elektronických komunikací nebo poskytovatelích služeb informační společnosti, aby tak učinili.*“
 - přijmout nové ustanovení požadující po subjektech, aby vedly podrobné a komplexní záznamy vnitřního auditu. Toho by mohlo být dosaženo přijetím tohoto znění: „*Poskytovatelé veřejně dostupných služeb elektronických komunikací a poskytovatelé služeb informační společnosti vedou a uchovávají komplexní záznamy podrobně uvádějící všechna narušení bezpečnosti, k nimž došlo, příslušné technické informace s nimi související a přijatá nápravná opatření. Záznamy rovněž obsahují odkaz ke všem oznámením vydaným dotčeným účastníkům nebo jednotlivcům a příslušným vnitrostátním orgánům, včetně jejich data a obsahu. Záznamy budou na požádání poskytnuty příslušnému vnitrostátnímu orgánu.*“
 - Umožnit Komisi přijmout technická prováděcí opatření, a to po předchozí konzultaci s EIOÚ, Pracovní skupinou zřízenou podle článku 29 a dalšími příslušnými zúčastněnými stranami, aby se zajistila soudržnost při provádění rámce týkajícího se narušení bezpečnosti.
 - Pokud jde o jednotlivce, kterým má být podáno oznámení, použít terminologii Komise nebo Evropského parlamentu „dotčení jednotlivci“ nebo „poškození uživatelé“, protože zahrnuje všechny jednotlivce, jejichž osobní údaje byly ohroženy.
- Veřejně dostupné soukromé sítě*
98. Služby komunikace jsou často zpřístupňovány veřejnosti nikoliv prostřednictvím veřejných sítí, ale prostřednictvím soukromě provozovaných sítí (např. přístupové body Wi-Fi v hotelích a na letištích), na něž se směrnice patrně nevztahuje. Evropský parlament přijal změnu č. 121 (článek 3) rozšiřující oblast působnosti této směrnice tak, aby byly zahrnuty veřejné a soukromé komunikační sítě, jakož i veřejně přístupné soukromé sítě. V tomto ohledu by Evropský parlament a Rada měly:
- zachovat podstatu změny č. 121, ale přeformulovat znění tak, aby do oblasti působnosti směrnice o soukromí a elektronických komunikacích spadalo pouze „*zpracování osobních údajů ve spojení s poskytováním veřejně dostupných služeb elektronických komunikací ve veřejných nebo veřejně přístupných komunikačních sítích ve Společenství*“. Výslovně zahrnuty by nebyly pouze soukromě provozované sítě (na rozdíl od veřejně přístupných soukromých sítí);

- změnit odpovídajícím způsobem všechna operativní ustanovení tak, aby se společně s veřejnými sítěmi výslovně odkazovalo k veřejně přístupným soukromým sítím;
- zahrnout změnu definující „veřejně přístupnou soukromou síť, kterou se rozumí soukromě provozovaná síť, k níž má široká veřejnost zpravidla neomezený přístup, za úplatu i zdarma nebo ve spojení s jinými službami nebo nabídkami, pod podmínkou přijetí platných podmínek“. Tím se zajistí větší právní jistota, pokud jde o subjekty, na něž se vztahuje nová oblast působnosti;
- přijmout nový bod odůvodnění, jehož prostřednictvím by Komise prováděla veřejnou konzultaci o použití směrnice o soukromí a elektronických komunikacích na všechny soukromé sítě, a to s použitím informací od EIOÚ, Pracovní skupiny zřízené podle článku 29 a jiných zúčastněných stran. Dále je třeba upřesnit, že v návaznosti na veřejné konzultace by Komise měla předložit odpovídající návrh na rozšíření nebo omezení druhů subjektů, na něž by se měla směrnice o soukromí a elektronických komunikacích vztahovat.

Zpracování provozních údajů pro bezpečnostní účely

99. V prvním čtení Evropského parlamentu byla přijata změna č. 181 (čl. 6 odst. 6a opravňující ke zpracování provozních údajů pro bezpečnostní účely. Ve společném postoji Rady bylo přijato nové znění oslabující některá opatření na ochranu soukromí. V tomto ohledu EIOÚ doporučuje Evropskému parlamentu a Radě:
- zamítnout tento článek jako celek, protože je zbytečný, a pokud by byl zneužit, mohl by příliš ohrozit ochranu údajů a soukromí jednotlivců;
 - nebo, v případě, že bude přijata nějaká změna stávajícího znění čl. 6 odst. 6a, začlenit opatření na ochranu

údajů projednávána v tomto stanovisku (podobná těm, která jsou uvedena ve změně Evropského parlamentu).

Podání žaloby na porušení směrnice o soukromí a elektronických komunikacích

100. Parlament přijal změnu č. 133 (čl. 13 odst. 6) umožňující právním subjektům podat žalobu na porušení kteréhokoliv ustanovení uvedené směrnice. Rada tuto změnu bohužel nezachovala. Rada a Evropský parlament by měly:
- potvrdit ustanovení umožňující právním subjektům, jako jsou sdružení spotřebitelů a odborová sdružení, využít práva na podání žaloby na porušení kteréhokoliv ustanovení této směrnice (nejen na porušení ustanovení o spamech, jak stanoví stávající přístup obsažený ve společném postoji a v pozměněném návrhu). Větší různorodost donucovacích mechanismů podpoří vyšší úroveň shody a účinné používání směrnice o soukromí a elektronických komunikacích jako celku.

Plnění úkolů

101. Ve všech výše uvedených záležitostech musí Evropský parlament a Rada vypracovat řádná pravidla a ustanovení, která jsou proveditelná i funkční a zároveň dodržují právo na soukromí a ochranu údajů jednotlivců. EIOÚ věří, že zúčastněné strany učiní maximum, aby tento úkol splnily, a doufá, že toto stanovisko k jejich úsilí přispěje.

V Bruselu dne 9. ledna 2009.

Peter HUSTINX
Evropský inspektor na ochranu údajů

Stanovisko evropského inspektora ochrany údajů k návrhu směrnice Rady, kterou se členským státům ukládá povinnost udržovat minimální zásoby ropy nebo ropných produktů

(2009/C 128/05)

EVROPSKÝ INSPEKTOR OCHRANY ÚDAJŮ,

nebo ropných produktů a zavedení nezbytných postupů k nápravě případných vážných nedostatků.

s ohledem na Smlouvu o založení Evropského společenství, a zejména na článek 286 této smlouvy,

s ohledem na Listinu základních práv Evropské unie, a zejména na článek 8 této listiny,

s ohledem na směrnici Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů ⁽¹⁾,

s ohledem na 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, a zejména na článek 41 uvedeného nařízení ⁽²⁾,

s ohledem na žádost o stanovisko v souladu s čl. 28 odst. 2 nařízení (ES) č. 45/2001 zaslanou evropskému inspektorovi ochrany údajů dne 14. listopadu 2008,

PŘIJAL TOTO STANOVISKO:

I. ÚVOD

1. Komise přijala dne 13. listopadu 2008 návrh směrnice Rady, kterou se členským státům ukládá povinnost udržovat minimální zásoby ropy a/nebo ropných produktů (dále jen: „návrh“) ⁽³⁾.
2. Cílem návrhu je zajištění vysoké úrovně bezpečnosti dodávek ropy ve Společenství prostřednictvím spolehlivých a transparentních mechanismů založených na solidaritě mezi členskými státy, udržování minimálních zásob ropy

3. Komise návrh zaslala dne 14. listopadu 2008 evropskému inspektorovi ochrany údajů ke konzultaci v souladu s čl. 28 odst. 2 nařízení (ES) č. 45/2001. Evropský inspektor ochrany údajů vítá, že je v této otázce konzultován, a konstatuje, že odkaz na tuto konzultaci je uveden v preambuli návrhu, v souladu s článkem 28 nařízení (ES) č. 45/2001.

4. Před přijetím návrhu Komise neformálně konzultovala evropského inspektora ochrany údajů ohledně konkrétního článku návrhu (stávající článek 19). Evropský inspektor ochrany údajů tuto neformální konzultaci uvítal, jelikož mu umožnila poskytnout určité podněty předtím, než Komise návrh přijala.

II. ANALÝZA NÁVRHU

Obecná analýza

5. Současná záležitost slouží jako dobrý příklad toho, že je třeba mít neustále na paměti pravidla pro ochranu údajů. V situaci, která se týká členských států a jejich povinnosti udržovat nouzové zásoby ropy, jejichž vlastníky jsou především právní subjekty, není zpracovávání osobních údajů zcela zjevné, ale i přestože se jako takové nepředpokládá, může k němu dojít. V každém případě je třeba zvážit možnost, že ke zpracovávání osobních údajů dojde a podle toho jednat.
6. V současném stavu směrnice stanoví v zásadě dvě činnosti, které by mohly zahrnovat zpracovávání osobních údajů. První je shromažďování informací o zásobách ropy členskými státy a následné předávání těchto informací Komisi. Druhá činnost se vztahuje k pravomoci Komise provádět kontroly v členských státech. Shromažďování informací o vlastních zásobách ropy by mohlo zahrnovat osobní údaje, jako jsou jména ředitelů společností a kontakty na ně. Toto shromažďování, jakož i následné předávání Komisi by pak bylo zpracováváním osobních údajů a vztahovaly by se na ně vnitrostátní právní předpisy provádějící směrnici 95/46/ES nebo nařízení (ES) č. 45/2001 podle toho, kdo ve skutečnosti údaje zpracovává. Rovněž udělení pravomoci provádět kontroly nouzových zásob v členských státech Komisi, které zahrnuje pravomoc shromažďovat údaje obecně, by mohlo znamenat shromažďování, a tudíž zpracovávání osobních údajů.

⁽¹⁾ Úř. věst. L 281, 23.11.1995, s. 31.

⁽²⁾ Úř. věst. L 8, 12.1.2001, s. 1.

⁽³⁾ KOM(2008) 775 v konečném znění.

7. V rámci neformální konzultace, která byla omezena pouze na ustanovení o pravomoci Komise provádět šetření, evropský inspektor ochrany údajů doporučil Komisi, aby určila, zda zpracovávání osobních údajů v souvislosti se šetřením Komise bude pouze nahodilým jevem nebo zda bude probíhat pravidelně a sloužit účelům šetření. V závislosti na výsledku tohoto posouzení byly navrženy dva přístupy.
8. V případě, že se zpracování osobních údajů nepředpokládá a bylo by tedy čistě náhodné, evropský inspektor ochrany údajů doporučil za prvé výslovně vyloučit zpracovávání osobních údajů, které by sloužilo účelům šetření Komise a za druhé uvést, že žádné osobní údaje, s nimiž se Komise setká v průběhu šetření, nebudou shromažďovány nebo zohledňovány, a dojde-li náhodně k jejich shromáždění, budou okamžitě zničeny. Jako obecné podpůrné ustanovení evropský inspektor ochrany údajů dále navrhl vložit ustanovení, které uvádělo, že touto směrnicí nejsou dotčena pravidla pro ochranu údajů podle směrnice 95/46/ES a nařízení (ES) č. 45/2001.
9. V případě, že se naopak předpokládá, že ke zpracovávání údajů bude v souvislosti s šetřením Komise docházet pravidelně, evropský inspektor ochrany údajů doporučil Komisi, aby vložila znění zohledňující výsledek náležitého posouzení ochrany údajů. To by mělo zahrnovat tyto prvky: I) skutečný účel zpracování údajů, II) nutnost zpracovávat údaje pro splnění tohoto účelu a III) proporcionalitu zpracovávání údajů.
10. Ačkoliv se neformální doporučení evropského inspektora ochrany údajů týkalo pouze pravomoci Komise provádět šetření, jsou jeho připomínky rovněž použitelné na ostatní hlavní činnosti vysvětlené v návrhu směrnice, zejména shromažďování informací členskými státy a jejich předávání Komisi.
11. Konečný návrh směrnice jasně ukazuje, že Komise došla k závěru, že se pro účely dané směrnice nepředpokládá žádné zpracovávání osobních údajů. Evropský inspektor ochrany údajů bere s potěšením na vědomí, že jeho první navrhovaný přístup je v návrhu plně zohledněn.
12. Vyjadřuje proto podporu způsobu, jakým Komise zajistila v navrhované směrnici soulad s pravidly pro ochranu údajů. Ve zbývajících částech tohoto stanoviska jsou poskytnuta pouze některá podrobnější doporučení.
- Připomínky k jednotlivým detailům*
13. Článek 15 navrhované směrnice se zabývá povinnostmi členských států zasílat Komisi týdenní statistický výkaz úrovně komerčních zásob držených na jejich vlastním území. Tyto informace budou za běžných okolností obsahovat pouze minimum osobních údajů. Mohly by však obsahovat údaje o fyzických osobách, které vlastní zásoby ropy nebo které pracují pro právní subjekt, který tyto zásoby vlastní. S cílem předejít tomu, aby členské státy poskytovaly tyto údaje Komisi, stanoví čl. 15 odst. 1, že pokud tak členské státy učiní, „nebudou uvádět jména vlastníků zásob“. Přestože je třeba mít na paměti skutečnost, že ne vždy vede odstranění jména k tomu, že z údajů nelze zpětně vysledovat fyzickou osobu, zdá se, že v současné situaci (statistické výkazy úrovně zásob ropy) bude tato dodatečná věta stačit k zajištění toho, aby Komisi nebyly předávány žádné osobní údaje.
14. Pravomoc Komise provádět šetření je stanovena v článku 19 navrhované směrnice. Článek jasně ukazuje, že se Komise řídila prvním přístupem, který je vysvětlen v bodě 8 výše. Stanoví, že shromažďování údajů nesmí být součástí kontrol prováděných Komisí. A i když se Komise s takovými údaji setká, nesmí je zohlednit a, dojde-li náhodně k jejich shromáždění, musí být zničeny. S cílem sladit toto znění se zněním použitým v právních předpisech o ochraně údajů a s cílem zabránit jakýmkoliv nedorozuměním doporučuje evropský inspektor ochrany údajů nahradit slovo „shromažďování“ v první větě druhého odstavce slovem „zpracování“.
15. Evropský inspektor ochrany údajů rovněž vítá, že bylo do návrhu zařazeno obecné podpůrné ustanovení týkající se příslušných právních předpisů pro ochranu údajů. Článek 20 členským státům, jakož i Komisi a dalším subjektům Společenství, jasně připomíná jejich povinnosti podle směrnice 95/46/ES a nařízení (ES) č. 45/2001. Dané ustanovení navíc zdůrazňuje práva, která mají podle těchto pravidel subjekty údajů, jako je právo vznést námitku proti zpracování svých údajů, právo na přístup ke svým údajům a právo na opravu svých údajů v případě nepřesnosti. Snad jen jednu připomínku lze uvést k umístění tohoto ustanovení v návrhu. Jelikož je obecné povahy, nevztahuje se pouze na pravomoc Komise provádět šetření. Evropský inspektor ochrany údajů proto doporučuje přesunout článek do první části směrnice, například za článek 2.
16. Odkaz na směrnici 95/46/ES a nařízení (ES) č. 45/2001 je uveden rovněž ve 25. bodě odůvodnění. Cíl tohoto bodu odůvodnění však není úplně jasný, poněvadž pouze uvádí právní předpisy pro ochranu údajů jako takové a nic dalšího. V bodě odůvodnění by mělo být jasně stanoveno, že ustanoveními této směrnice nejsou uvedené právní předpisy dotčeny. Navíc se zdá, že z poslední věty tohoto bodu odůvodnění vyplývá, že právní předpisy pro ochranu údajů výslovně požadují, aby osoby provádějící kontroly okamžitě zničily náhodně shromážděné údaje. Ačkoliv to může být důsledkem stanovených pravidel, dané právní předpisy tuto povinnost neobsahují. Obecnou zásadou při ochraně údajů je, že osobní údaje nejsou uchovávány déle, než je nutné pro účely, pro něž byly shromážděny nebo jsou dále

zpracovány. Bude-li první část bodu odůvodnění upravena právě navrženým způsobem, bude poslední věta zbytečná. Evropský inspektor ochrany údajů proto navrhuje vypustit poslední větu 25. bodu odůvodnění.

III. ZÁVĚRY

17. Evropský inspektor ochrany údajů by rád vyjádřil podporu způsobu, jakým Komise zajistila v navrhované směrnici soulad s pravidly pro ochranu údajů.

18. Jako podrobné připomínky evropský inspektor ochrany údajů doporučuje:

— nahradit v první větě čl. 19 odst. 2 slovo „shromažďování“ slovem „zpracování“;

— přesunout článek 20, který je obecným ustanovením k ochraně údajů, do první části směrnice, konkrétně přímo za článek 2;

— doplnit do 25. bodu odůvodnění, že ustanoveními směrnice nejsou dotčena ustanovení směrnice 95/46/ES a nařízení (ES) č. 45/2001;

— vypustit poslední větu 25. bodu odůvodnění.

V Bruselu dne 3. února 2009.

Peter HUSTINX
evropský inspektor ochrany údajů

IV

(Informace)

INFORMACE ORGÁNŮ A INSTITUCÍ EVROPSKÉ UNIE

KOMISE

Směnné kurzy vůči euro ⁽¹⁾

5. června 2009

(2009/C 128/06)

1 euro =

měna	směnný kurz	měna	směnný kurz
USD americký dolar	1,4177	AUD australský dolar	1,7606
JPY japonský jen	137,48	CAD kanadský dolar	1,5657
DKK dánská koruna	7,4472	HKD hongkongský dolar	10,9887
GBP britská libra	0,87920	NZD novozélandský dolar	2,2263
SEK švédská koruna	10,9250	SGD singapurský dolar	2,0530
CHF švýcarský frank	1,5191	KRW jihokorejský won	1 768,65
ISK islandská koruna		ZAR jihoafrický rand	11,4189
NOK norská koruna	8,9700	CNY čínský juan	9,6871
BGN bulharský lev	1,9558	HRK chorvatská kuna	7,3550
CZK česká koruna	27,003	IDR indonéská rupie	14 078,75
EEK estonská koruna	15,6466	MYR malajsijský ringgit	4,9556
HUF maďarský forint	289,10	PHP filipínské peso	67,016
LTL litevský litas	3,4528	RUB ruský rubl	43,5789
LVL lotyšský latas	0,7094	THB thajský baht	48,464
PLN polský zlotý	4,5420	BRL brazilský real	2,7345
RON rumunský lei	4,2185	MXN mexické peso	18,7066
TRY turecká lira	2,1834	INR indická rupie	66,7910

⁽¹⁾ Zdroj: referenční směnné kurzy jsou publikovány ECB.

TISKOVÉ OPRAVY**Oprava úrokové míry použité Evropskou centrální bankou pro hlavní refinanční operace***(Úřední věstník Evropské unie C 124 ze dne 4. června 2009)**(2009/C 128/07)*

Strana 1 a obálka:

místo: „1,00 % 4. června 2009“,

má být: „1,00 % 1. června 2009“.

CENY PŘEDPLATNÉHO NA ROK 2009 (bez DPH, včetně poštovního za obvyklou zásilku)

Úřední věstník EU, řady L + C, pouze tištěné vydání	22 úředních jazyků EU	1 000 EUR ročně (*)
Úřední věstník EU, řady L + C, pouze tištěné vydání	22 úředních jazyků EU	100 EUR měsíčně (*)
Úřední věstník EU, řady L + C, tištěné vydání + roční CD-ROM	22 úředních jazyků EU	1 200 EUR ročně
Úřední věstník EU, řada L, pouze tištěné vydání	22 úředních jazyků EU	700 EUR ročně
Úřední věstník EU, řada L, pouze tištěné vydání	22 úředních jazyků EU	70 EUR měsíčně
Úřední věstník EU, řada C, pouze tištěné vydání	22 úředních jazyků EU	400 EUR ročně
Úřední věstník EU, řada C, pouze tištěné vydání	22 úředních jazyků EU	40 EUR měsíčně
Úřední věstník EU, řady L + C, měsíční CD-ROM (souhrnný)	22 úředních jazyků EU	500 EUR ročně
Dodatek k Úřednímu věstníku (řada S), CD-ROM, 2 vydání týdně	mnohojazyčné: 23 úředních jazyků EU	360 EUR ročně (= 30 EUR měsíčně)
Úřední věstník EU, řada C – Výběrová řízení	jazyky, kterých se týká výběrové řízení	50 EUR ročně

(*) Prodej podle jednotlivých čísel: do 32 stran: 6 EUR
od 33 do 64 stran: 12 EUR
více než 64 stran: cena stanovena jednotlivě

Předplatné *Úředního věstníku Evropské unie*, který vychází v úředních jazycích Evropské unie, je k dispozici ve 22 jazykových verzích. Zahrnuje řady L (Právní předpisy) a C (Informace a oznámení).

Každá jazyková verze má samostatné předplatné.

V souladu s nařízením Rady (ES) č. 920/2005, zveřejněným v Úředním věstníku L 156 ze dne 18. června 2005, které stanoví, že orgány Evropské unie nejsou dočasně vázány povinností sepsovat všechny akty v irštině a zveřejňovat je v tomto jazyce, je Úřední věstník vydáván v irském jazyce prodáván zvlášť.

Předplatné dodatku k Úřednímu věstníku (řada S – Dodatek k *Úřednímu věstníku Evropské unie*) zahrnuje znění ve všech 23 úředních jazycích na jednom mnohojazyčném CD-ROM.

Předplatné *Úředního věstníku Evropské unie* opravňuje na požádání k obdržení různých příloh Úředního věstníku. Předplatitelé jsou na vydávání příloh upozorňováni prostřednictvím „oznámení čtenářům“ zveřejňovaného v *Úředním věstníku Evropské unie*.

Prodej a předplatné

Placené publikace vydávané Úřadem pro úřední tisky jsou k dispozici u našich distributorů. Seznam distributorů se nachází na této internetové adrese:

http://publications.europa.eu/others/agents/index_cs.htm

EUR-Lex (<http://eur-lex.europa.eu>) nabízí přímý a bezplatný přístup k právu Evropské unie. Tyto internetové stránky umožňují nahlížet do *Úředního věstníku Evropské unie* a obsahují rovněž smlouvy, právní předpisy, judikaturu a návrhy právních předpisů.

Více informací o Evropské unii naleznete na adrese: <http://europa.eu>