VĚSTNÍK
ÚŘADU PRO OCHRANU OSOBNÍCH ÚDAJŮ
2007

Částka 44 | **28. března 2007** | **Cena 122,– Kč**

OBSAH

ÚVOD

Ve čtyřicáté čtvrté částce Věstníku Úřadu pro ochranu osobních údajů najdete přehled zrušených registrací za období od 26. 11. 2006 do 9. 3. 2007.

Rubrika Sdělení Úřadu obsahuje podstatné části rozhodnutí Úřadu, k nimž dospěl na základě řešení případů porušení zákona o ochraně osobních údajů, nebo podezření z porušení tohoto zákona. Rubrika Sdělení přináší, v návaznosti na stanovisko ředitele odboru legislativního a právního Ministerstva školství, mládeže a tělovýchovy ČR, dokument nazvaný „Vyjádření a doporučení ÚOOÚ k možnosti instalovat kamerový systém v prostorách školy". Materiál předkládá základní přístupová kritéria Úřadu pro ochranu osobních údajů k této problematice, která lze shrnout do zásad, jež je nutno v konkrétním případě vždy posoudit dříve, nežli se učiní rozhodnutí o instalaci kamerového systému. Ti, kteří se po důkladném zvážení rozhodnou ve svých zařízeních kamerové systémy instalovat zde najdou vysvětlení, jak postupovat z pohledu zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.

Součástí rubriky je dále „Informace o stanovisku Ministerstva vnitra ČR ke zveřejňování záznamů městských kamerových systémů". Se závěry MV ČR k této záležitosti se Úřad ztotožňuje a proto jej také publikuje ve svém Věstníku.

V zájmu vyšší informovanosti o dokumentech vytvořených v rámci WP29 - Pracovní skupiny pro ochranu dat podle článku 29 (tj. čl. 29 směrnice 95/46/ES), která se zabývá problematikou ochrany osobních údajů a soukromí, předkládá Úřad tři stanoviska této pracovní skupiny. Jsou jimi Stanovisko č. 1/2006 o ochraně údajů na vnitřní postupy oznamování podezření z protiprávního jednání (whistleblowing), Stanovisko č. 6/2006 k návrhu nařízení Rady o příslušnosti, použitelném právu, uznávání a výkonu rozhodnutí a spolupráci ve věcech vyživovací povinnosti a Stanovisko č. 10/2006 ke zpacovávání osobních údajů Společností pro celosvětovou mezibankovní finanční komunikaci /Society for Worldwide Interbank Financial Telecommunication (SWIFT)/. V souvislosti s posledním uvedeným stanoviskem č. 10/2006 vydal Úřad na své tiskové konferenci konané dne 25. ledna 2007 u příležitosti Dne ochrany osobních údajů „Prohlášení pro tisk" k otázce týkající se skutečnosti, že společnost SWIFT poskytuje bez vědomí klientů finančích institucí údaje o mezibankovních finančních transakcích na vyžádání úřadům USA v rámci boje poti terorismu. Posledním publikovaným materiálem je pracovní dokument pracovní skupiny WP 29 o ochraně údajů a důsledcích iniciativy eCall na ochranu soukromí. Úřad přetiskuje oficiální překlady právně nezávazných dokumentů WP29 v jejich původní podobě a nepřebírá odpovědnost za případné nepřesnosti překladu.

Přehled zrušených registrací

Číslo registrace	Subjekt	Datum zrušení
00013746/001	KARBON INVEST A.S.	1. 12. 2006
00013746/002	KARBON INVEST A.S.	1. 12. 2006
00013746/003	KARBON INVEST A.S.	1. 12. 2006
00009354/001	MORAVSKÉ TEPLÁRNY A.S.	28. 12. 2006
00008205/001	DŮM DĚTÍ A MLÁDEŽE STARÉ MĚSTO OKRES UHERSKÉ HRADIŠTĚ	12. 01. 2007
00008552/001	MUZEUM UMĚNÍ OLOMOUC	27. 01. 2007
00008552/002	MUZEUM UMĚNÍ OLOMOUC	27. 01. 2007
00014435/001	PENZIJNÍ FOND VIVA A.S. V LIKVIDACI	27. 01. 2007
00004753/001	MADSEN & TAYLOR, A. S.	14. 02. 2007
00016294/001	KENVELO CZ,SPOL. S R.O.	14. 02. 2007
00016294/002	KENVELO CZ,SPOL. S R.O.	14. 02. 2007
00030028/001	CME MEDIA SERVICES S.R.O.	14. 02. 2007

II. SDĚLENÍ ÚŘADU

Z rozhodovací činnosti Úřadu

Sdělení úvodem:
Úřad pro ochranu osobních údajů se prostřednictvím následující stručné charakteristiky vyjadřuje k některým problematickým okruhům případů porušování povinností při zpracování osobních údajů projednávaných Úřadem pro ochranu osobních údajů v rámci své rozhodovací činnosti.

1. Ke zveřejňování osobních údajů na Internetu

Zveřejňování nejrůznějších osobních údajů na webových stránkách je stále velmi aktuálním tématem. Typické jsou případy zveřejnění osobních údajů dlužníků anebo občanů, jejichž záležitosti byly projednávány orgány obcí.

Je tedy nutné zdůraznit, že zpřístupnění osobních údajů prostřednictvím webových stránek je jejich zpracováním podle § 4 písm. e) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (dále jen „zákon o ochraně osobních údajů“), a subjekt, který osobní data tímto způsobem zpřístupňuje (nemusí se jednat o tentýž subjekt, který předmětné stránky spravuje a provozuje) je z pohledu zákona o ochraně osobních údajů správcem osobních údajů ve smyslu § 4 písm. j) tohoto zákona. Správce osobních údajů je povinen při zpracování dat postupovat v souladu se zákonem o ochraně osobních údajů, tedy dodržet veškeré povinnosti zde stanovené. Jednou ze základních povinností správce, podle § 5 odst. 2 zákona o ochraně osobních údajů, je povinnost zpracovávat osobní údaje pouze se souhlasem subjektu údajů. Bez tohoto souhlasu je zpracování možné jen, je-li naplněno některé z liberačních ustanovení podle § 5 odst. 2 písm. a) až g) zákona o ochraně osobních údajů.

Avšak skutečnost, že správce různými způsoby zpracovává osobní údaje na základě určitého právního titulu (tedy souhlasu nebo zákonného zmocnění), neznamená, že může takové údaje automaticky, bez tohoto právního titulu, také publikovat na Internetu.

Jednou z dalších základních zásad zpracování osobních údajů, kterou se musí každý správce osobních údajů řídit, je zásada účelnosti zpracování vyjádřená v § 5 odst. 1 písm. f) zákona o ochraně osobních údajů, tj. využívání údajů pouze k tomu účelu, k němuž byly shromážděny. Např. zaměstnavatel, který zcela legálně zpracovává poměrně rozsáhlé soubory osobních údajů o svých zaměstnancích, tak není oprávněn tyto údaje bez dalšího (zejména bez souhlasu dotčených zaměstnanců) zpřístupnit na Internetu. V případě zaměstnanců, jejichž pracovní povinnosti souvisí např. se stykem s veřejností, lze zveřejnit kontaktní informace, ale pouze v nezbytném rozsahu. Jiným příkladem může být publikování informace, že určitá osoba je vzhledem k neplnění svých smluvních závazků dlužníkem, a to aniž by součástí tohoto (nebo jiného) smluvního ujednání byl souhlas dotčeného subjektu se zpracováním osobních údajů tímto způsobem (tj. zveřejněním v případě prodlení).

Každý, kdo zvažuje zveřejnění osobních údajů na webových stránkách, musí tedy před tímto krokem důkladně zvážit, zda bude zapotřebí získat k tomuto kroku souhlas subjektů údajů (tj. předem získaný, svobodný a informovaný souhlas podle § 5 odst. 4 zákona o ochraně osobních údajů), anebo zda naplňuje některou z uvedených výjimek, při jejichž aplikaci je však nutno vycházet spíše z restriktivního výkladu. *(čj. 1/06/SŘ-OSČ, 3/06/SŘ-OSČ, 4/06/SŘ-OSČ)*

2. K zabezpečení osobních údajů zpracovávaných v rámci zdravotnické dokumentace

V souvislosti se zpracováním osobních údajů ve zdravotnické dokumentaci (podle § 67a a § 67b zákona č. 20/1966 Sb., o péči o zdraví lidu) a při nakládání s ní je především nezbytné přijmout a důsledně dodržovat odpovídající opatření směřující k tomu, aby nedošlo k neoprávněnému nebo nahodilému přístupu k osobním údajům nebo k jejich ztrátě.

Povinnost přijmout taková opatření vyplývá z § 13 odst. 1 zákona o ochraně osobních údajů tomu, kdo zdravotnickou dokumentaci vede, tedy zdravotnickému zařízení (bez ohledu na to, jedná-li se o osobu právnickou nebo fyzickou osobu podnikající). Obsahem této povinnosti je vyhodnocení všech rizik předmětného zpracování osobních údajů, v návaznosti na konkrétní organizaci zpracování a okolnosti, za nichž ke zpracování dochází, a dále přijetí a provedení odpovídajících opatření. Vhodná opatření pro zabezpečení ochrany osobních údajů je nezbytné přijmout nejen ve vztahu k běžným činnostem zdravotnického zařízení jako správce či zpracovatele osobních údajů, ale také zvláště pro každou ojedinělou operaci s osobními údaji, případně s jejich nosiči, která vybočuje z běžné činnosti správce nebo zpracovatele, jako je např. přeprava písemností (zdravotnické dokumentace) na jiné místo, jejich předávání jiným subjektům anebo skartace písemností uchovávaných v archivu. Při vyhodnocování rizik a přijímání opatření ve smyslu § 13 odst. 1 zákona o ochraně osobních údajů je dále nezbytné vypořádat se i s rizikem odcizení dokumentace nebo jiných nosičů, tedy i osobních údajů, které obsahují.

Je třeba zdůraznit, že přijetí odpovídajících bezpečnostních opatření je zvláště důležité vzhledem k tomu, že v rámci zdravotnické dokumentace jsou zpracovávány kromě „obyčejných“ osobních údajů i údaje citlivé ve smyslu § 4 písm. b) zákona o ochraně osobních údajů. *(čj. 8/06/SŘ-OSČ, 9/06/SŘ-OSČ, 22/06/SŘ-OSČ)*

3. Ke zpracování osobních údajů v souvislosti se správou nemovitostí

V souvislosti s výkonem správy domu, ať již ve vlastnictví společenství vlastníků jednotek nebo družstva, dochází vždy ke zpracování osobních údajů obyvatel domu. Tyto údaje jsou nezbytné pro řádný výkon správy domu, jako je např. správa

fondu oprav nebo rozúčtování společných nákladů. Toto zpracování může provádět jak vlastník nemovitosti sám, v pozici správce osobních údajů, nebo lze výkonem této činnosti pověřit jiný subjekt, který potom jedná v roli zpracovatele osobních údajů. Odpovědnost za zpracování osobních údajů nese primárně správce ve smyslu § 4 písm. j) zákona o ochraně osobních údajů, v případě překročení či nedodržení stanovených podmínek zpracování však také (anebo pouze) zpracovatel [viz § 4 písm. k) tohoto zákona].

Při zpracování osobních údajů shromážděných při výkonu správy domu je vždy nutné dbát zejména na dodržení zásady účelnosti zpracování vyjádřené v § 5 odst. 1 písm. f) zákona o ochraně osobních údajů, tedy využívat tyto údaje skutečně jen k účelu, k němuž byly shromážděny. Vybočením z této zásady, a tedy porušením povinnosti při zpracovávání osobních údajů, může být i zveřejnění osobních údajů např. v souvislosti s existencí dluhu vůči majiteli či správci nemovitosti na místě přístupném i jiným osobám, než které jsou z titulu svého členství ve společenství vlastníků jednotek nebo družstvu oprávněny takové informace obdržet.

V domech, kde je část obyvatel vlastníky jednotek či družstevníky a část nájemníky těchto subjektů, je pro náležité plnění povinností stanovených zákonem o ochraně osobních údajů při správě domu velmi podstatné rozlišování postavení jednotlivých obyvatel domu. Informace (včetně osobních údajů), na něž mají nárok spoluvlastníci domu, tedy osoby podílející se finančně např. na správě společných prostor nebo na opravách, není možné automaticky zpřístupnit všem, kteří v daném domě bydlí, bez rozdílu. Např. sdělení, že určitý spoluvlastník nebo družstevník dluží na poplatcích do fondu oprav nebo kolik přispěl na realizovanou rekonstrukci domu, lze sdělit ostatním spoluvlastníkům a družstevníkům, nikoli ale nájemníkům, naopak informace týkající se nájemníků lze, v přiměřené míře, zpřístupnit ostatním spoluvlastníkům nemovitosti (neboť např. počet osob v domácnosti hraje roli při správě celého domu), ale již ne ostatním nájemníkům.

Současně lze konstatovat, že i v případě, kdyby všichni obyvatelé domu byli vlastníky jednotek nebo členy družstva, není vhodné informaci obsahující osobní údaje umístit ve veřejně přístupných částech domu (a to i zamčeného), neboť nelze zajistit, že nebude takto zpřístupněna jiným osobám, např. návštěvám. *(čj. 2/06/SŘ-OSČ, 5/06/SŘ-OSČ, 33/06/SŘ-OSČ)*

4. K problematice aktualizace zpracovávaných osobních údajů

Na základě ustanovení § 5 odst. 1 písm. c) zákona o ochraně osobních údajů je každý správce či zpracovatel osobních údajů povinen zpracovávat pouze přesné osobní údaje a, je-li to nezbytné, také zpracovávané údaje aktualizovat. S touto povinností úzce souvisí i povinnost vyjádřená v § 5 odst. 1 písm. e) zákona o ochraně osobních údajů, tedy povinnost uchovávat osobní údaje pouze po dobu, která je nezbytná k jejich zpracování.

Z uvedeného je zřejmé, že každý, kdo zpracovává osobní údaje, musí v závislosti na rozsahu a okolnostech předmětného zpracování přijmout systém opatření, jejichž prostřednictvím zajistí, že nebudou zpracovávány nepřesné či chybné osobní údaje (tj. případné nedostatky v kvalitě údajů budou zjištěny), a dále že nebudou uchovávány osobní údaje, jejichž zpracování již není z hlediska dosažení stanoveného cíle nezbytné.

V této souvislosti je nutno uvést, že zpracováním nepřesných osobních údajů podle § 5 odst. 1 písm. c) zákona o ochraně osobních údajů není pouze zpracování nesprávných údajů vzniklých např. gramatickou chybou, ale i zpracování formálně správných údajů v souvislosti s nesprávnou informací. Např. zpracování přesných identifikačních údajů spolu s informací o tom, že daná osoba je dlužníkem, ačkoli tomu tak ve skutečnosti není. Ve smyslu § 4 písm. a) zákona č. 101/2000 Sb. je totiž nutno pod pojmem osobní údaj rozumět jakoukoli informaci, kterou je možno vztáhnout ke konkrétní osobě.

Povinnost zpracovávat pouze přesné osobní údaje však neznamená, že je vždy nezbytné zpracovávat jen absolutně správné údaje, neboť nepřesnosti mohou vzniknout již při shromažďování dat od samotných subjektů údajů, z čehož nelze vyvozovat odpovědnost daného správce. Nicméně zákon o ochraně osobních údajů požaduje, aby správce osobních údajů (případně zpracovatel na základě jeho pověření) prováděl, je-li to vzhledem k účelu zpracování nezbytné, také aktualizaci zpracovávaných osobních údajů, tedy nápravu zjištěných nepřesností. Zákon o ochraně osobních údajů správci neukládá, aby prováděl tuto kontrolu správnosti zpracovávaných údajů nepřetržitě, ale ponechává vyhodnocení způsobu vyrovnání se s touto povinností na dotyčném správci (vyhodnocení splnění této povinnosti je pak úkolem Úřadu v kontrolním nebo v sankčním řízení). Opatření směřující ke zjištění zpracování nesprávných osobních údajů jsou tak nezbytná zejména v systémech, jejichž provoz je zcela či do značné míry automatizovaný, a které jsou intenzivně využívány.

Ke zjištění, že jsou zpracovávány nepřesné nebo již nadbytečné osobní údaje, často dochází na základě žádosti samotného subjektu údajů o opravu, doplnění či likvidaci zpracovávaných dat. Je nezbytné uvést, že takové žádosti subjektu údajů (je-li důvodná) je správce na základě § 21 zákona o ochraně osobních údajů povinen vyhovět. *(čj. 10/06/SŘ-OSČ, 13/06/SŘ-OSČ, 31/06/SŘ-OSČ)*

5. Ke zpracování rodných čísel pro účely vedení soudních sporů

Zvláštní úprava využívání rodných čísel je již od 1. dubna 2004 obsažena v zákoně č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel), který v ustanovení § 13c odst. 1 taxativně stanoví, kdy lze rodná čísla využívat. Vzhledem k tomu, že rodné číslo je i přes svůj zvláštní status osobním údajem ve smyslu § 4 písm. a) zákona o ochraně osobních údajů, představuje zákon o evidenci obyvatel lex specialis k tomuto zákonu. Ten, kdo zpracovává rodná čísla, je tedy správcem osobních údajů podle § 4 písm. j) zákona o ochraně osobních údajů a vztahují se na něj veškeré povinnosti tímto zákonem uložené, pokud zákon o evidenci obyvatel nestanoví jinak.

V soukromé sféře mohou být rodná čísla využívána zejména na základě souhlasu jejich nositelů, tj. podle § 13c odst. 1

písm. c) zákona o evidenci obyvatel. Ustanovení § 13c odst. 1 písm. a) tohoto zákona totiž opravňuje k využívání rodných čísel pouze zde uvedené orgány státní správy a pro aplikaci postupu podle § 13c odst. 1 písm. b) zákona o evidenci obyvatel, tedy využití rodného čísla, stanoví-li tak zvláštní zákon, je nezbytné, aby takový zvláštní právní předpis výslovně stanovil povinnost identifikovat účastníky určitého právního vztahu rodnými čísly.

V praxi se však stále vyskytují situace, kdy jsou rodná čísla soukromoprávními subjekty (typicky právními zástupci) běžně využívána pro označení stran soudního sporu či účastníků řízení, případně je tento údaj přímo vyžadován ze strany příslušných státních orgánů. Tuto praxi je však nutno zcela odmítnout, neboť to jsou právě státní instituce, které buď přímo zákon o evidenci obyvatel nebo jiná norma opravňuje k získávání a využívání rodných čísel. Naopak jednotlivé strany sporu či účastníci řízení a jejich zástupci jsou tímto postupem fakticky nuceni zpracovávat rodná čísla v rozporu se zákonem, neboť např. získání souhlasu se zpracováním rodného čísla žalovaného žalobcem bude zřejmě jen výjimečné a právní předpisy zpracování rodných čísel soukromoprávními subjekty obvykle neumožňují.

Např. § 79 odst. 1 zákona č. 99/1963 Sb., občanský soudní řád, povinnost identifikovat účastníky soudního řízení (fyzické osoby) rodným číslem nestanoví, pouze požaduje, aby návrh na zahájení řízení kromě obecných náležitostí obsahoval jméno, příjmení a bydliště účastníků. Z uvedeného je zřejmé, že zákon č. 99/1963 Sb. není zvláštním zákonem ve smyslu § 13c odst. 1 písm. b) zákona o evidenci obyvatel, který by umožňoval využívání rodných čísel.

Oprávnění k využívání rodných čísel pro identifikaci účastníků řízení nelze vyvozovat ani ze skutečnosti, že některé veřejné evidence dostupné i ve formě dálkového přístupu (typicky katastr nemovitostí a obchodní rejstřík) rodná čísla obsahují a tak jej zpřístupňují široké veřejnosti. Zpracování rodných čísel v souvislosti s vedením těchto evidencí je v souladu s § 13c odst.1 písm. a) zákona o evidenci obyvatel. Předmětné zvláštní právní předpisy, upravující podmínky fungování těchto evidencí, však již neobsahují oprávnění uživatelů volně disponovat se zde uvedenými rodnými čísly.

Závěrem je třeba uvést, že souhlasem s využitím rodného čísla podle § 13c odst. 1 písm. c) zákona o evidenci obyvatel je, s ohledem na absenci zvláštní úpravy, nutno rozumět souhlas se zpracováním osobních údajů podle zákona o ochraně osobních údajů, tedy svobodný a vědomý projev vůle, předcházející samotnému zpracování. *(čj. 15/06/SŘ-OSČ)*

Poznámka: Za jednotlivými texty, které jsou rozděleny do tématických okruhů, jsou vždy kurzívou uvedena interní čj., pod kterými jsou jednotlivé případy v Úřadu evidovány.

Vyjádření a doporučení ÚOOÚ k možnosti instalovat kamerový systém v prostorách školy

Zpracováno 12. března 2007

Vydává se v návaznosti na publikované vyjádření odboru legislativního a právního Ministerstva školství, mládeže a tělovýchovy ČR ze dne 6.12. 2006.[1)]

Základní přístupová kriteria Úřadu pro ochranu osobních údajů (dále jen „Úřad“) lze shrnout do těchto zásad, které je nutno v konkrétním případě vždy posoudit dříve, nežli se učiní rozhodnutí o instalaci kamerového systému:

– Ochrana práva jednotlivce by měla být vždy zohledněna ve vztahu k zájmům, provozovatele školy nebo školského zařízení (dále jen „škola“), který musí vykonávat svá práva a povinnosti způsobem co nejméně zasahujícím do soukromí, a to nejen zaměstnanců a žáků, ale i dalších osob.
– Škole musí být zřejmý velmi závažný důvod nebo vážná příčina, pro který je kamerový systém instalován a který neumožňuje použít jiný, méně invazivní prostředek zasahující do soukromí osob pohybujících se ve sledovaném prostoru. Přitom je třeba zdůraznit, že kamerový systém nelze nasazovat a ani následně využívat za účelem sledování fyzických osob – žáků, učitelů nebo zaměstnanců školy, ale pouze pro legitimní účely jako je například ochrana majetku.
– Musejí být dána jasná pravidla pro přístup jen vymezeného okruhu osob k systému a v něm uchovávaným záznamům nebo k jeho jednotlivým částem, včetně oprávnění manipulovat se sledovacími zařízeními nebo jejich režim upravovat.
– Rovněž je nezbytné řešit zvláštní režim přístupu oprávněných osob k uchovávaným záznamům, to znamená, jak osob pověřených správcem pro nahlížení do záznamů, tak osob, které využijí svého práva přístupu k zaznamenaným údajům o nich.
– Musí být stanovena doba uchovávání záznamů, která nepřesáhne dobu potřebnou k tomu, aby incident zaznamenaný kamerou bylo možno zjistit dodatečnými prostředky a předat k vyšetření příslušným orgánům. Přitom doba uchování by při běžném provozu systému neměla přesáhnout délku několika dnů s přihlédnutím k možným odchylkám jednotlivých záznamů pořizovaných například během prázdnin.
– Před spuštěním systému by měl být vypracován projekt rozmístění kamer a instalace jednotlivých sledovacích a záznamových zařízení včetně stanovení režimu (časového) pro provoz jednotlivých snímacích stanovišť, který by měl být kritériem pro posouzení funkčnosti systému

i z pohledu zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „zákon“).

Pokud se shrnou shora uvedené podmínky a předpoklady pro zákonný rámec provozování kamerových systémů, lze v zásadě s přihlédnutím k současným postojům Úřadu, jejichž snahou je omezit provozování kamerových systémů ve školách jen na nezbytně nutnou míru, souhlasit s větší částí stanoviska MŠMT v tom směru, že:

1. Skutečnost, že neexistuje zvláštní právní úprava podmínek pro provozování kamerových systémů neznamená, že škola při splnění svých zákonných povinností správce osobních údajů nemůže rozhodnutí o instalaci kamerového systému se záznamem učinit.
2. Pokud se škola k tomuto kroku rozhodne, ocitá se toto zpracování v režimu zákona a musí proto splnit zde uváděné zákonné podmínky:
   - Učinit oznámení o zpracování podle § 16 zákona.
   - Zpracovávat osobní údaje pouze se souhlasem subjektu údajů podle § 5 odst. 2, pokud škola neprokáže kvalifikovaný důvod, který by ji opravňoval ke zpracování osobních údajů bez souhlasu.
   - Provozovat systém tak, aby bylo soukromí osob s ohledem na jejich právo podle § 10 zákona narušováno minimálně (posuzováno je např. i umístění kamer, úhel záběru, zobrazovací schopnost apod.).
   - Informovat monitorované osoby o instalaci a provozu systému podle § 11 zákona.
   - Přijmout bezpečnostní opatření pro provozování systému a ochranu zpracovávaných informací podle § 13 zákona a stanovit přiměřenou dobu pro uchovávání záznamů podle § 5 odst. 1 písm. e).
   - Respektovat podmínky zvláštních právních předpisů upravujících možnosti sledování osob (zejména § 316 odst. 2 zákoníku práce).

Závěr:

Nad rámec výše uvedeného doporučení lze uvést:

Záměrem tohoto vyjádření je odstranit přetrvávající rozdíly v přístupu k otázce, v jakých prostorách žáci i zaměstnanci školy, uplatňují své právo na soukromí.

V tomto směru se odkazuje na judikaturu Evropského soudu pro lidská práva (ESLP)[2], podle které je nutno pod pojmem soukromí člověka rozumět právo každého člověka na vytváření a rozvíjení vztahu s dalšími lidskými bytostmi, a to i na pracovišti (a lze tedy dovodit, že i v prostorách, kde jsou žáci vzděláváni). Dle soudu není dost dobře možné přesně oddělit soukromý a profesionální život, neboť právě v rámci svých pracovních aktivit má většina lidí největší příležitost navazovat a rozvíjet vztahy s vnějším okolím, a proto právo na respektování soukromého života zahrnuje i právo na respektování soukromí v zaměstnání (viz např. rozhodnutí ve věci Niemietz v. Německo z roku 1992).

Poznámka:

[1] Plné znění dokumentu „Vyjádření odboru legislativního a právního MŠMT k otázce používání kamer ve školách“ ze dne 6. 12. 2006 je k dispozici na internetové adrese http://www.ucitelskenoviny.cz/nastenka_clanek.php?odkaz=kamery.html .

[2] Více informací o ESLP je k dispozici na internetové adrese www.echr.coe.int .

Informace o stanovisku Ministerstva vnitra ČR ke zveřejňování záznamů městských kamerových systémů

V Informačním servisu prevence kriminality za leden 2007, který vydává Ministerstvo vnitra ČR – odbor prevence kriminality, bylo publikováno stanovisko tohoto odboru ke zveřejňování záznamů z městských kamerových systémů. Se závěry MV k této problematice a s jeho právním názorem na přípustnost zveřejňování záznamů městských kamerových systémů se Úřad pro ochranu osobních údajů ztotožňuje, a proto jej publikuje i ve svém Věstníku. Stanovisko je přetištěno se souhlasem Ministerstva vnitra ČR.

Zveřejňování záznamů z městských kamerových systémů

V posledních měsících se na odbor prevence kriminality Ministerstva vnitra obrací čím dál více zástupců měst a obcí či pracovníků obecních policií s dotazem, zda je možné zveřejňovat záznamy z městských kamerových dohlížecích systémů.

Uvádíme proto obecnou odpověď na tuto veskrze právní otázku. Úvodem je třeba poznamenat, že záznam z kamerového dohlížecího systému je podle českého právního řádu osobním údajem ve smyslu ustanovení § 4 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů (dále jen zákon o ochraně osobních údajů). Z této skutečnosti pak vyplývá řada povinností pro správce a zpracovatele osobních údajů – záznamů z kamerového dohlížecího systému, kterým je v tomto případě konkrétní město či obec.

Zejména se tedy jedná o povinnosti uložené správcům osobních údajů v ustanoveních § 5, § 11 až § 16 zákona o ochraně osobních údajů, které obsahují například povinnost správce stanovit účel, k němuž mají být osobní údaje zpracovány, zpracovat pouze přesné osobní údaje, uchovávat osobní údaje pouze pro dobu odpovídající stanovenému účelu, informovat subjekt údajů o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovány, a v neposlední řadě má správ-

ce také oznamovací povinnost k Úřadu pro ochranu osobních údajů.

V případě obcí respektive měst provozuje kamerový dohlížecí systém většinou obecní respektive městská policie. Ve smyslu ustanovení § 3 odst. 6 zákona o ochraně osobních údajů je v případě zajišťování veřejného pořádku a vnitřní bezpečnosti ve smyslu zvláštního zákona (v tomto případě zákona č. 553/1991 Sb., o obecní policii, ve znění pozdějších předpisů, dále jen zákon o obecní policii) město či obec jako správce osobních údajů vyňato z povinností stanovených v § 5 odst. 1, § 11 a § 12 zákona o ochraně osobních údajů.

Z výkladového ustanovení § 4 písm. e) zákona o ochraně osobních údajů vyplývá, že zpracováním osobních údajů je mimo jiné i jejich zveřejňování. Zároveň ustanovení § 5 odst. 2 zákona o ochraně osobních údajů stanovuje taxativní výčet situací, kdy lze zpracovávat (tedy včetně zveřejňování) osobní údaje bez souhlasu subjektu údajů. V tomto taxativním výčtu se však zveřejňování nevyskytuje, a proto je tuto činnost nutno vykonávat toliko se souhlasem subjektů údajů. U zveřejňování osobních údajů nelze ani použít vynětí z určitých výše uvedených povinností ve smyslu již uvedeného ustanovení § 3 odst. 6 zákona o ochraně osobních údajů, jelikož toto neuvádí vynětí z povinností stanovených v § 5 odst. 2 zákona o ochraně osobních údajů.

Celou situaci lze tedy shrnout tak, že, i kdyby byly osobní údaje zveřejňovány v souvislosti se zajištěním veřejného pořádku na základě zvláštního zákona o obecní policii, má obec či město povinnost zveřejňovat osobní údaje jen se souhlasem subjektů údajů tedy osob vyskytujících se na záznamech. V opačném případě by byl porušen zákon o ochraně osobních údajů, který je zákonnou limitou práva na soukromí, jehož ústavní základ je obsažen v čl. 7 odst. 1 Listiny základních práv a svobod.

Závěrem je nutné podotknout, že situace v případech, kdy městský kamerový dohlížecí systém provozuje Policie České republiky, je v podstatě identická s výše popsaným právním režimem záznamů zpracovávaných obecní policií.

Poznámka: Výše uvedený materiál je k dispozici na http://www.mvcr.cz/ministerstvo/opk/servis/leden07.pdf .

Prohlášení pro tisk ke zpracovávání osobních údajů Společností pro celosvětovou mezibankovní finančí komunikaci (SWIFT)

(Materiál je součástí tiskové zprávy z tiskové konference Úřadu konané 25. 1. 2007)

Sdělení úvodem:
V souvislosti se zveřejněním Stanoviska č.10/2006 Pracovní skupiny pro ochranu dat podle článku 29 směrnice 95/46/ES, které se týká zpracovávání osobních údajů Společností pro celosvětovou mezibankovní finanční komunikaci /Society for Worldwide Interbank Financial Telecommunication (SWIFT)/, publikuje Úřad současně svůj postoj k otázce týkající se skutečnosti, že společnost SWIFT poskytuje bez vědomí klientů finančních institucí údaje o mezibankovních finančních transakcích, na vyžádání úřadům USA v rámci boje proti terorismu. Materiál „Prohlášení pro tisk" je součástí tiskové zprávy Úřadu z jeho tiskové konference konané dne 25. ledna 2007 u příležitosti Dne ochrany osobních údajů. Úřad pro ochranu osobních údajů považuje za solidní, aby klienti bank a finančních institucí i široká veřejnost byli o problému informování, což je i cílem tohoto prohlášení pro tisk.

V červnu minulého roku se na Úřad pro ochranu osobních údajů, stejně jako na ostatní obdobné dozorové orgány nad ochranou osobních údajů ve členských státech EU i jinde ve světě, obrátila Privacy International s upozorněním, že společnost SWIFT poskytuje bez vědomí klientů finančních institucí údaje o mezibankovních finančních transakcích na vyžádání úřadům USA v rámci boje proti terorismu.

Privacy International je soukromá organizace se sídlem v Londýně, se členy z 30 zemí, založená v roce 1990; jejím cílem je střežit soukromí, lidská práva a občanské svobody.

SWIFT (Society for Worldwide Interbank Financial Telecommunication) je světovou finanční službou pro usnadňování mezinárodních peněžních transferů. Jde o společnost družstevního typu založenou a provozovanou v rámci belgického práva, s ústředím v Belgii, v sídle Národní banky Belgie. Má řadu úřadoven v různých zemích (žádnou v ČR). Významnou úlohu v dozorových orgánech společnosti mají centrální banky zemí tzv. G-10, které základní kontrolní pravomoc přenesly právě na Národní banku Belgie.

Z informace Privacy International a výsledků následného zjišťování zejména belgických úřadů dále vyplývá, že SWIFT má dvě operační centra, jedno v EU a druhé v USA. Provozovna v USA má funkci „záložní" a přesně zrcadlí všechny podchycené operace. Na základě smlouvy uzavřené mezi společností SWIFT a úřady USA se z operačního centra data ve velkých množstvích přenášejí do tzv. „black-boxů", které již jsou pod kontrolou USA, a to pravděpodobně na základě přibližných vymezení typu „od-do", „země-země", „banka-banka" apod.; z nich pak Ministerstvo financí USA (US Department of Treasury) vybírá již individualizovaná data. Vše se děje na základě úředních žádostí o informace (tzv.

„subpoenas“), které jsou pro subjekty působící v rámci jurisdikce USA závazné.

Záležitostí předávání osobních údajů společností SWIFT úřadům USA v rámci boje proti terorismu se na svých jednáních zabývala také Pracovní skupina pro ochranu dat podle článku 29 („WP 29“), což je nezávislý poradní orgán Evropské komise složený z předsedů národních dozorových orgánů pro oblast ochrany osobních údajů.

22. listopadu 2006 přijala pracovní skupina WP 29 v této záležitosti podrobné stanovisko (http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_cs.pdf). Upozorňuje v něm na porušení několika ustanovení příslušné směrnice o ochraně osobních údajů (95/46/EC) a tedy i odpovídajících ustanovení v národních legislativách. Jedná se zejména o skutečnost, že data byla ve velkém rozsahu předávána pro účel nekompatibilní s původním komerčním účelem jejich sběru (čl. 6/1/b směrnice). Ani SWIFT, ani finanční instituce dále neinformovaly subjekty údajů o způsobu zpracování jejich údajů ve spojení s transfery do USA, jak to vyžadují čl. 10 a 11 směrnice. Nerespektovány jsou i čl. 25 a 26 směrnice, stanovující podmínky předávání údajů do „třetích“ zemí s neadekvátní legislativní ochranou osobních údajů, mezi které patří i USA. V souvislosti s bojem proti terorismu nemá příslušné zpracování dat právní oporu ani v právních normách EU, ani v nějakém závazném mezinárodním ujednání mezi EU a USA.

WP 29 v závěrech vyzývá k okamžitému zahájení akcí, které by vedly k nápravě situace a k zastavení porušování zákona. Vyslovila názor o společné odpovědnosti společnosti SWIFT a finančních institucí, nicméně v nestejné míře této odpovědnosti. Hlavní opatření by se měla týkat v první řadě hlavní odpovědné osoby „správce“ dat, kterou je SWIFT. I když banky tuto společnost založily, již dlouhou dobu nově přistupující banky a finanční instituce nemají na její činnost přímý vliv, ve své naprosté většině nemají možnost její činnost kontrolovat a nerozhodují o povaze a způsobu poskytovaných služeb. Určitý vliv na její činnost a tedy i určitou míru odpovědnosti mají centrální banky zemí G-10 v čele s Národní bankou Belgie vzhledem ke své účasti v kontrolním aparátu a tedy i možnosti nepřímo činnost společnosti ovlivňovat. Zásadní odpovědnost společnosti SWIFT za předávání dat do USA je tedy nepochybná.

Úřad pro ochranu osobních údajů se nespokojil jen pouhým sledováním vývoje v zahraničí. Již v červenci 2006 se předseda Úřadu obrátil dopisem na generálního guvernéra ČNB, ve kterém ho o případu informoval a požádal o součinnost při získávání dalších informací. V listopadu 2006 bylo po pracovní linii informováno MF ČR a na vyžádání byly informace s hodnocením situace poskytnuty také dalším rezortům, jmenovitě MZV ČR a MV ČR. Ještě v roce 2006 také byla z rozhodnutí předsedy Úřadu zahájena v rámci kompetencí Úřadu jakožto nezávislého orgánu dozoru kontrola několika bank, jejímž řízením byl pověřen inspektor Ing. Jan Zapletal. Účelem kontroly bylo prověřit, zda nedošlo při zpracovávání osobních údajů klientů bank v souvislosti s jejich předáváním do systému „SwiftNet Fin“ k porušení zákona a v takovém případě pak, kromě možných finančních sankcí, přijmout opatření na zastavení a nápravu příslušné závadné činnosti.

I když kontrola Úřadu pro ochranu osobních údajů ve vybraných bankách dosud formálně uzavřena nebyla, již dnes je možné konstatovat, že zákon kontrolovanými subjekty z hlediska zpracování osobních údajů jejich klientů, které jsou součástí záznamů o mezibankovních transakcích předávaných do zahraničí a posléze také poskytované společností SWIFT úřadům v USA v rámci boje proti terorismu, porušen nebyl. Ve smlouvách kontrolovaných subjektů se společností SWIFT není žádná zmínka svědčící o tom, že by záznamy mohly být používány i pro jiné účely, nekompatibilní s komerčními účely, pro které jsou českými bankami zpracovávány a do zahraničí předávány. Transfery záznamů s osobními údaji do zahraničí kontrolované banky vesměs směřují v rámci EU, respektive Evropského hospodářského prostoru, s výjimkou informací o platbách ve měnách zemí mimo tento prostor, které nejprve směřují do banky v příslušné „třetí“ zemi. O tomto principu v souvislosti s použitím měny „třetí“ země jsou však klienti v rámci všeobecných obchodních podmínek informováni. Tokům osobních údajů v rámci EU/EHP nesmí být kladena žádná překážka z titulu ochrany osobních údajů. Jednoznačně tak stanoví již zmíněná směrnice 95/46/EC ve svém čl. 1 odst. 2 a stejně tak to vyplývá i z příslušného ustanovení § 27 odst. 1 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.

Závěrem nezbývá nežli znovu zdůraznit, že odpovědnost za stávající praxi je především na společnosti SWIFT, která osobní údaje do USA předává a úřadům USA poskytuje. Jistou odvozenou míru spoluzodpovědnosti je možné vyvodit i pro finanční instituce, které jsou součástí kontrolních mechanismů SWIFT, tedy centrální banky zemí G-10 v čele s Národní bankou Belgie. A právě tam je také třeba hledat nápravu a zvažovat případné sankce. Objevují se úvahy, že řešení do budoucna je možné očekávat od jednání orgánů EU s úřady USA s cílem právně podepřít transfery dat do USA mezinárodní smlouvou. To by ovšem současnou praxi příliš nezměnilo, nicméně by se docílilo určitých smluvních záruk pro zacházení s osobními údaji ze strany amerických úřadů.

Úřad pro ochranu osobních údajů ovšem považuje za solidní, aby klienti bank a finančních institucí i široká veřejnost byli o problému alespoň informováni, což je i cílem tohoto prohlášení pro tisk.

Poznámka: Výše uvedený materiál je také k dispozici na internetové adrese Úřadu http://www.uoou.cz/index.php?l=cz&m=top&mid=03&u1=&u2=&t= .

Pracovní skupina na ochranu údajů vytvořená podle ČLÁNKU 29

00195/06/CZ
WP 117

Stanovisko 1/2006 k problematice užívání právních předpisů EU o ochraně údajů na vnitřní postupy oznamování podezření z protiprávního jednání (whistleblowing) v oblasti účetnictví, vnitřních účetních kontrol, záležitostí auditu, boje proti úplatkářství a trestné činnosti v bankovním a finančním sektoru

Přijaté dne 1. února 2006

Tato pracovní skupina, která byla vytvořena podle článku 29 směrnice 95/46/ES, představuje nezávislý evropský poradní orgán v oblasti ochrany údajů a soukromí. Její úkoly jsou vymezené v článku 30 směrnice 95/46/ES a článku 15 směrnice 2002/58/ES.

Služby sekretariátu zabezpečuje ředitelství C (Občanské právo, základní práva a občanství) Generálního ředitelství Evropské komise pro spravedlnost, svobodu a bezpečnost, B-1049 Brussel, Belgie, kancelář č. LX-46 01/43.

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

OBSAH

PRACOVNÍ SKUPINA PRO OCHRANU FYZICKÝCH OSOB PŘI ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

vytvořená směrnicí Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995[1]
s ohledem na článek 29 a čl. 30 odst. 1 písm. c) a čl. 30 odst. 3 této směrnice,

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

PŘIJALA TOTO STANOVISKO:

I. ÚVOD

Toto stanovisko obsahuje pokyny k provádění vnitřních postupů oznamování podezření z protiprávního jednání (dále jen „oznamování“) v souladu s právními předpisy EU o ochraně údajů stanovenými směrnicí 95/46/ES[2].

Skutečnost, že zavádění postupů oznamování v Evropě v průběhu roku 2005 vyvolalo množství otázek, včetně otázek týkajících se ochrany údajů, ukazuje, že rozvoj těchto činností ve všech členských zemích EU může být spojen se značnými obtížemi. Tyto obtíže jsou do značné míry zapříčiněny kulturními rozdíly, které vyplývají ze společenských, a/nebo historických důvodů, jejichž existenci nelze popřít ani přehlížet.

Pracovní skupina si je vědoma, že tyto obtíže zčásti souvisí se širokou škálou záležitostí, na něž lze upozorňovat pomocí vnitřních postupů oznamování protiprávních jednání. Je jí rovněž známo, že postupy oznamování vyvolávají v některých členských státech EU specifické problémy v oblasti pracovního práva a že na těchto otázkách, které si i nadále budou vyžadovat pozornost, se stále pracuje. Pracovní skupina musí rovněž brát v úvahu skutečnost, že v některých zemích EU je používání postupů oznamování upraveno právními předpisy, ale ve většině zemí EU chybí specifická právní či jiná úprava této problematiky.

Z toho důvodu považuje pracovní skupina za předčasné přijmout v této fázi obecně platné konečné stanovisko k oznamování. V rámci tohoto stanoviska se rozhodla zabývat se těmi otázkami, u nichž je potřeba vydání pokynů EU nejnaléhavější. Vzhledem k této skutečnosti a z důvodů uvedených v tomto dokumentu se toto stanovisko formálně omezuje na uplatňování právních předpisů EU o ochraně údajů na vnitřní postupy oznamování v oblasti účetnictví, vnitřních účetních kontrol, otázek auditu, boje proti úplatkářství a trestné činnosti v bankovním a finančním sektoru.

Pracovní skupina přijala toto stanovisko s jasnou představou o tom, že musí dále rozvíjet otázku případné slučitelnosti právních předpisů EU o ochraně údajů s vnitřními postupy oznamování v jiných oblastech než těch, které zde byly zmíněny, a to například v oblasti lidských zdrojů, zdraví a bezpečnosti práce, ohrožování a poškozování životního prostředí a páchání trestných činů. V nejbližších měsících provede analýzu této otázky,

---

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

[2] V souladu s konkrétním vymezením okruhu činnosti pracovní skupiny se tento pracovní dokument nezabývá jinými právními problémy, jež mohou vyvstat v souvislosti s mechanismy oznamování, zejména v oblasti pracovního a trestního práva.

aby zjistila, zda je i v souvislosti s těmito záležitostmi zapotřebí pokynů EU a v kladném případě vypracuje další dokument, v němž doplní nebo upraví principy rozvinuté v současném dokumentu.

II. ODŮVODNĚNÍ OMEZENÉHO PŘEDMĚTU ÚPRAVY TOHOTO STANOVISKA

V roce 2002 přijal Kongres Spojených států amerických v reakci na různé finanční skandály společností zákon známý pod názvem Sarbanes-Oxley Act („zákon SOX").

Podle tohoto zákona se musí americké veřejné společnosti a jejich dceřiné společnosti (organizační složky) v EU, jakož i neamerické společnosti kotované na amerických trzích s cennými papíry zavést v rámci svého auditorského výboru *„postupy k přijímání, uchovávání a vyřizování stížností předložených emitentovi v souvislosti s účetnictvím, vnitřními účetními kontrolami nebo otázkami auditu , jakož i možnost důvěrného anonymního předkládání oznámení zaměstnanci emitenta o sporných otázkách účetnictví nebo auditu."*[3] Článek 806 zákona SOX obsahuje navíc ustanovení, jehož cílem je zajistit ochranu zaměstnanců společností s veřejně obchodovatelnými účastnickými cennými papíry, kteří předloží důkazy o podvodu, před odvetnými opatřeními, které by je mohly postihnout proto, že podali oznámení cestou postupu oznamování[4]. Ve Spojených státech je pro sledování uplatňování zákona SOX příslušná Komise pro cenné papíry (Securities and Exchange Commission, dále jen „SEC").

Uvedená ustanovení byla zapracována do pravidel systému Nasdaq[5] a Newyorské burzy cenných papírů (New York Stock Exchange, dále jen „NYSE")[6]. Společnosti, které jsou kotovány na burzách cenných papírů Nasdaq nebo NYSE, musí těmto burzovním institucím každoročně předkládat potvrzení o správnosti, úplnosti a oprávněnosti svého účetnictví. Prostřednictvím tohoto certifikačního řízení společnosti prokazují, že dodržují určité předpisy, včetně předpisů upravujících oznamování podezření z protiprávního jednání.

Společnostem, které nedodrží podmínky týkající se oznamování, může Nasdaq, NYSE nebo SEC ukládat přísné sankce a pokuty. Z důvodu nejistoty ohledně slučitelnosti postupů oznamování s právními předpisy EU o ochraně údajů jsou dotyčné společnosti jednak ohroženy sankcí ze strany orgánů EU pro ochranu údajů v případě porušení právních předpisů EU o ochraně údajů, a jednak sankcí ze strany amerických orgánů v případě, že poruší zákonné předpisy USA.

---

3 Sarbanes-Oxley Act, čl. 301 odst. 4.

4 Sarbanes-Oxley Act, článek 406, zejména pak pokyny vydané nejvýznamnějšími institucemi amerických trhů s cennými papíry (NASDAQ, NYSE), rovněž stanoví, že společnosti kotované na těchto trzích musí přijmout „etický kodex" vyšších finančních úředníků a ředitelů v oblasti účetnictví, účetního výkaznictví a záležitostí auditu, který by měl zajistit mechanismy vynucování těchto právních předpisů.

5 Předpis č. 4350 (D) (3): „Povinnosti a pravomoci auditorského výboru".

6 Newyorská burza cenných papírů (NYSE), článek 303A.06: „Auditorský výbor".

Uplatňování některých ustanovení zákona SOX na evropské dceřiné společnosti (organizační složky) amerických společností a na evropské společnosti kotované na amerických burzách cenných papírů je v současné době předmětem soudního přezkumu ve Spojených státech amerických[7]. Navzdory této relativní nejistotě v otázce, zda se na společnosti se sídlem v Evropě vztahují všechna ustanovení zákona SOX, se i společnosti, na něž se vztahují ustanovení zákona SOX s jasnými extrateritoriálními účinky, chtějí řídit zvláštními ustanoveními uvedeného zákona upravujícími oznamování.

Vzhledem k sankcím, které hrozí společnostem v EU, považuje pracovní skupina 29 za nejdůležitější zaměřit svou analýzu především na ty postupy oznamování, které upravují oznamování podezření z porušení právních předpisů v oblasti účetnictví, vnitřních účetních kontrol a otázek auditu ve smyslu zákona Sarbanes-Oxley Act, jakož i na dále uvedené související otázky. Touto analýzou hodlá pracovní skupina přispět k nastolení právní jistoty pro společnosti, na něž se vztahují jak právní předpisy EU o ochraně údajů, tak i zákon SOX.

III. ZVLÁŠTNÍ DŮRAZ NA PRÁVNÍ PŘEDPISY O OCHRANĚ ÚDAJŮ TÝKAJÍCÍ SE OCHRANY OSOB OZNAČENÝCH ZA PODEZŘELÉ PROSTŘEDNICTVÍM POSTUPŮ OZNAMOVÁNÍ

Vnitřní postupy oznamování jsou zpravidla zaváděny v zájmu uplatnění zásad řádné správy a řízení společností při jejich běžném fungování. Institut oznamování představuje doplňkový mechanismus umožňující zaměstnancům oznamovat protiprávní jednání vnitřní cestou s využitím zvláštního informačního kanálu. Doplňuje obvyklé informační a sdělovací kanály organizace, jimiž jsou například zástupci zaměstnanců, liniové řízení, personál zodpovědný za kontrolu kvality nebo interní auditoři, jejichž specifickým úkolem je oznamování takových protiprávních jednání. Na oznamování je třeba nahlížet jako na doplněk vnitřního řízení, nikoliv jeho alternativu.

Pracovní skupina zdůrazňuje, že postupy oznamování musí být uplatňovány v souladu s právními předpisy EU o ochraně údajů. V praxi se bude uplatňování postupů oznamování ve většině případů opírat o zpracovávání osobních údajů (t.j. shromažďování, zaznamenávání, uchovávání, zpřístupňování a výmaz údajů týkajících se identifikované nebo identifikovatelné osoby), což si vyžádá uplatnění právních předpisů o ochraně údajů.

Uplatňování těchto právních předpisů bude mít různé důsledky pro vytváření a správu postupů oznamování. V tomto dokumentu je podrobně popsána rozsáhlá škála těchto důsledků (viz oddíl IV).

Pracovní skupina konstatuje, že stávající nařízení a pokyny týkající se oznamování mají sice za cíl zajistit zvláštní ochranu osobě, která podává oznámení prostřednictvím takovéhoto postupu (dále jen „oznamovatel“), nikdy však zvláště neupravují ochranu osob označených za podezřelé, a to především ochranu v souvislosti se zpracováváním jejich osobních údajů, třebaže má každá fyzická osoba i v případě, že byla označena za podezřelou, nárok na právní ochranu, jež jí přiznávají směrnice 95/46/ES a odpovídající ustanovení vnitrostátních právních předpisů.

---

[7] Odvolací soud USA (1. obvod) dne 5. ledna 2006 rozhodl, že ustanovení zákona SOX o ochraně osob, které podávají oznámení o podezření z protiprávního jednání, se nevztahují na cizí státní příslušníky pracující mimo území USA v zahraničních organizačních složkách společností, jež se jinak řídí ustanoveními zákona SOX.

Uplatňování právních předpisů EU o ochraně údajů na postupy oznamování si vyžaduje věnovat zvláštní pozornost problematice ochrany osoby, která mohla být označena za podezřelou na základě upozornění. V této souvislosti pracovní skupina zdůrazňuje, že postupy oznamování obsahují značné riziko stigmatizace a viktimizace této osoby uvnitř organizace, k níž přináleží. Tato osoba bude vystavena takovýmto rizikům dokonce dříve, než bude informována o tom, že je označena za podezřelou, a než dojde k vyšetřování oznámených skutečností za účelem jejich prokázání nebo vyvrácení.

Pracovní skupina zastává názor, že řádné uplatňování právních předpisů o ochraně údajů na postupy oznamování přispěje ke snížení takovýchto rizik. Domnívá se rovněž, že uplatňování těchto právních předpisů nebude v žádném případě mařit zamýšlený účel postupů oznamování, ale naopak obecně přispěje k řádnému fungování těchto postupů.

IV. POSOUZENÍ SLUČITELNOSTI POSTUPŮ OZNAMOVÁNÍ S PRÁVNÍMI PŘEDPISY O OCHRANĚ ÚDAJŮ

Problematika uplatňování právních předpisů o ochraně údajů na postupy oznamování zahrnuje řešení otázek zákonnosti postupů oznamování (1); uplatňovaní zásad kvality údajů a proporcionality (2); získávání jasných a úplných informací o postupu (3); ochranu práv obviněné osoby (4); bezpečnosti operací zpracování údajů (5); správy interních postupů oznamování (6); záležitostí spojených s mezinárodním předáváním údajů (7); požadavků oznamování a předběžné kontroly (8).

1. Zákonnost postupů oznamování (článek 7 směrnice 95/46/ES)

K tomu, aby byl postup oznamování zákonný, musí být dán jeden z legitimních důvodů ke zpracování údajů podle článku 7 směrnice o ochraně údajů.

Za současného stavu jsou v tomto kontextu zřejmě relevantní dva důvody: buďto je zavedení postupu oznamování potřebné ke splnění právní povinnosti (čl. 7 písm. c)) nebo ochraně právního zájmu správce údajů nebo třetí osoby, které byly tyto údaje zpřístupněny (čl. 7 písm. f))[8].

i) Zavedení postupu oznamování je potřebné ke splnění právní povinnosti správce údajů (čl. 7 písm. c))

Zavedení postupu oznamování by mělo mít za cíl plnění právní povinnosti ukládané právními předpisy Společenství nebo členského státu. Přesněji řečeno by mělo jít o právní povinnost zavést postupy vnitřní kontroly ve vymezených oblastech.

V současné době tato povinnost existuje ve většině členských států, například v bankovním sektoru, kde se vlády rozhodly posílit vnitřní kontroly, především v souvislosti s činnostmi úvěrových a investičních společností.

---

[8] Společnosti by měly brát v úvahu, že v některých členských státech podléhá zpracování údajů o podezřeních ze spáchání trestných činů dalším zvláštním podmínkám zajišťujícím zákonnost jejich zpracovávání (viz níže, oddíl IV, 8).

Tato právní povinnost zavést posílené kontrolní mechanismy existuje rovněž v rámci boje proti úplatkářství, především v důsledku provádění Dohody OECD o boji proti úplatkářství zahraničních veřejných činitelů v mezinárodních obchodních transakcích (Dohody OECD ze dne 17. prosince 1997).

Na druhé straně nelze povinnost uloženou na základě cizího právního nebo jiného předpisu, který by vyžadoval zavedení postupů oznamování, nutně chápat jako právní povinnost zakládající legitimitu zpracování údajů v EU. V případě jakékoliv jiné interpretace by byla usnadněna možnost obcházet normy EU stanovené ve směrnici 95/46 cestou cizích právních předpisů. V důsledku toho nelze považovat ustanovení zákona SOX o oznamování za legitimní základ pro zpracovávání údajů podle článku 7 písm. c).

V některých zemích EU však může na základě vnitrostátních právních předpisů existovat právní povinnost zavést postupy oznamování v oblastech, které jsou upraveny zákonem SOX[9]. V dalších zemích EU, kde neexistují takovéto právní povinnosti, je však možné dosáhnout téhož výsledku na základě čl. 7 písm. f).

ii) Zavedení postupu oznamování je nutné k prosazení oprávněného zájmu správce údajů (článek 7 písm. f))

Zavedení postupů oznamování může být potřebné k prosazení oprávněného zájmu správce údajů nebo třetí osoby, která byla s údaji seznámena (čl. 7 písm. f)). Tento důvod je přijatelný pouze za podmínky, že „neexistuje zájem na ochraně základních práv a svobod subjektu, o němž jsou údaje vedeny, který by převažoval nad těmito oprávněnými zájmy“.

Významné mezinárodní organizace včetně EU[10] a OECD[11] uznávají, že v zájmu zabezpečení adekvátního fungování společností je důležité opírat se o zásady řádné správy a řízení společností. Zásady či pokyny vypracované na těchto fórech mají zajistit zvyšování transparentnosti a podnítit rozvoj řádných finančních a účetních činností, čímž přispívají k ochraně zúčastněných stran a finanční stabilitě trhů. Zejména uznávají oprávněnost zájmu organizace na zavádění vhodných postupů, jejichž prostřednictvím se zaměstnancům umožní oznamovat nesrovnalosti a sporné účetní nebo auditorské praktiky řídícímu orgánu nebo auditorskému výboru. V rámci takovýchto postupů oznamování je třeba zajistit režim přiměřeného a nezávislého přešetřování oznámených skutečností, což vyžaduje vhodné postupy výběru osob zapojených do řízení postupu oznamování. Rovněž je třeba zajistit režim vhodných navazujících opatření.

---

[9] Nizozemský zákoník správy a řízení společností (Corporate Governance Code), 9.12.2003, oddíl II, 1.6.

Návrh španělského Jednotného kodexu správy a řízení registrovaných společností, kapitola IV, čl. 67 odst. 1 písm. d). Tento kodex musí ještě přezkoumat španělský Úřad na ochranu údajů, který posoudí jeho důsledky na ochranu údajů.

[10] Evropské společenství: Doporučení Komise ze dne 15. února 2005 o úloze řídících pracovníků registrovaných společností s nevýkonnými nebo dozorčími právy a o výborech nejvyššího (dozorčího) orgánu (Úř. věst. L 52, 25.2.2005, s. 51).

[11] OECD: Principy řádné správy a řízení společností OECD 2004. Část 1, oddíl IV.

Kromě toho se v těchto pokynech a předpisech zdůrazňuje, že by bylo vhodné zajistit ochranu oznamovatelů a zavést přiměřené záruky jejich ochrany před odvetnými opatřeními (diskriminační přístup a disciplinární opatření)[12].

Cíl zajištění finanční bezpečnosti na mezinárodních finančních trzích a především předcházení podvodům a protiprávnímu jednání v oblasti účetnictví, vnitřních účetních kontrol, otázek auditu i oznamování úplatkářství, trestné činnosti v bankovním a finančním odvětví nebo zneužívání informací v obchodním styku a boj proti těmto jevům lze vskutku považovat za oprávněné zájmy zaměstnavatele, jimiž lze odůvodnit zpracovávání osobních údajů v rámci postupů oznamování v těchto oblastech. Životně důležitým zájmům obchodních společností, především těch, které jsou registrovány na finančních trzích, je zajistit, aby byly zprávy o podezřeních z účetních manipulací nebo o chybném účetním auditu, které mohou mít vliv na finanční výkazy společností a dotýkat se oprávněných zájmů zúčastněných stran na finanční stabilitě společnosti, předkládány správní radě za účelem přijetí přiměřených opatření.

V této souvislosti je možné považovat americký Sarbanes-Oxley Act za jednu z těchto iniciativ přijatých k zajištění stability finančních trhů a ochranu oprávněných zájmů zúčastněných stran přijetím právních předpisů, které zaručují přiměřenou správu a řízení společností.

Z uvedených důvodů zastává pracovní skupina názor, že zavádění takovýchto vnitřních mechanismů odpovídá oprávněným zájmům správců údajů i v těch zemích EU, kde neexistuje zvláštní právní požadavek na zavedení postupů oznamování v oblasti účetnictví, vnitřních účetních kontrol, záležitostí audit a boje proti úplatkářství a trestné činnosti v bankovním a finančním odvětví.

Ustanovení čl. 7 písm. f) však vyžaduje zajištění rovnováhy mezi oprávněnými zájmy odůvodňujícími zpracovávání osobních údajů a základními právy osob, o nichž jsou tyto údaje vedeny. Pro účely posouzení této rovnováhy zájmů by se měly zohlednit otázky proporcionality, subsidiarity i závažnosti údajných protiprávních jednání, které lze oznamovat, jakož i důsledky pro subjekt, o němž jsou údaje vedeny. V rámci posouzení rovnováhy zájmů bude rovněž potřebné zavést přiměřená ochranná opatření. V článku 14 směrnice 95/46/ES se mimo jiné stanoví, že v případě zpracování údajů na základě čl. 7 písm. f) mají fyzické osoby právo kdykoliv vznést z vážných oprávněných důvodů námitky proti zpracovávání údajů, které se jejich týkají. Tyto otázky jsou podrobněji rozvedeny v dalším textu .

2. Uplatňování zásad kvality údajů a proporcionality (článek 6 směrnice o ochraně údajů)

Podle směrnice 95/46/ES musí být osobní údaje zpracovávané nestranným a zákonným způsobem[13] shromažďovány pouze pro účely účel specifikovaného, výslovně stanoveného a zákonného použití[14] a nelze je používat pro účely neslučitelné s těmito účely. Kromě toho musí být zpracovávané údaje adekvátní, relevantní a nesmí být

---

[12] Viz například Public Interest Disclosure Act 1998 (Spojené království).

[13] Čl. 6 odst. 1 písm. a) směrnice 95/46/ES.

[14] Čl. 6 odst. 1 písm. b) směrnice 95/46/ES.

nepřiměřené vzhledem k účelům, pro něž které jsou shromažďovány, popř. dále zpracovávány[15]. Soubor těchto pravidel se někdy označuje jako „zásada proporcionality". Dále je nutno přijmout přiměřená opatření k zajištění výmazu nebo opravy nepřesných nebo neúplných údajů[16]. Uplatňování těchto zásadních pravidel ochrany údajů má řadu důsledků pro způsob podávání oznámení zaměstnanci organizace a jejich zpracování touto organizací. Analýza těchto důsledků je obsažena v dalším textu.

i) Možnost omezení počtu osob oprávněných oznamovat nesrovnalosti nebo protiprávní jednání prostřednictvím postupů oznamování

V souvislosti s uplatňováním zásady proporcionality pracovní skupina doporučuje, aby společnost odpovědná za postup oznamování pečlivě zvážila, zda by bylo vhodné omezit počet osob způsobilých oznamovat údajné protiprávní jednání prostřednictvím postupu oznamování, a to především vzhledem k závažnosti údajných protiprávních jednání, která jsou předmětem oznámení. Pracovní skupina však bere na vědomí, že kategorie vymezených zaměstnanců mohou v některých případech zahrnovat všechny zaměstnance v některé z oblastí, na něž se vztahuje toto stanovisko.

Pracovní skupina si je vědoma toho, že rozhodujícím činitelem budou okolnosti každého jednotlivého případu. Nemá proto zájem normativně upravit toto otázku a ponechává na správcích údajů, aby posoudili, zda jsou taková omezení vhodná vzhledem ke zvláštním okolnostem, za nichž působí, přičemž jejich rozhodnutí může podléhat ověření ze strany příslušných orgánů.

ii) Možnost omezení počtu osob, které mohou být označeny za podezřelé prostřednictvím postupů oznamování

V souvislosti s uplatňováním zásady proporcionality pracovní skupina doporučuje, aby společnost zavádějící postup oznamování pečlivě posoudila, zda by bylo vhodné omezit počet osob, o nichž lze podávat prostřednictvím tohoto postupu oznámení, a to především s ohledem na závažnost oznamovaných údajných protiprávních jednání. Pracovní skupina však bere na vědomí, že vymezené kategorie zaměstnanců mohou v některých případech zahrnovat všechny zaměstnance v některé z oblastí, na něž se vztahuje toto stanovisko.

Pracovní skupina si je vědoma, že rozhodujícím činitelem budou okolnosti každého jednotlivého případu. Nehodlá tudíž normativně upravovat toto otázku a ponechává na správcích údajů, aby posoudili, zda jsou tato omezení vhodná vzhledem ke zvláštním okolnostem, za nichž působí, přičemž jejich rozhodnutí může podléhat ověření ze strany příslušných orgánů.

iii) Přednost vytipovaných a důvěrných oznámení před anonymními oznámeními

Otázka, zda by se v rámci postupů oznamování mělo umožnit podávat oznámení anonymně, nikoli otevřeným způsobem (t.j. s uvedením totožnosti oznamovatele zásadně pod podmínkou zachovávaní důvěrnosti) si zasluhuje zvláštní pozornost.

---

[15] Čl. 6 odst. 1 písm. c) směrnice 95/46/ES.

[16] Čl. 6 odst. 1 písm. d) směrnice 95/46/ES.

Anonymnost nemusí být vhodným řešením, ať již pro oznamovatele nebo pro organizaci, a to z mnoha důvodů:

- anonymita nezabrání ostatním úspěšně odhadnout, kdo záležitost předložil;
- vyšetřování záležitosti je obtížnější, jestliže lidé nemohou klást doplňující otázky;
- ochranu oznamovatele před odvetnými opatřením i v případě, že je stanovená zákonem[17], lze snáze zajistit, jestliže se záležitost nastolí otevřeným způsobem;
- anonymní oznámení mohou soustředit pozornost lidí na oznamovatele, například v domnění, že předkládá záležitost ve zlém úmyslu;
- organizace se vystavuje riziku, že vytvoří prostředí, v němž dochází k podávání oznámení ve zlém úmyslu;
- vědomí zaměstnanců, že prostřednictvím postupu oznamování může kdykoliv dojít k podání anonymního oznámení týkajícího se jejich osoby, by mohlo způsobit zhoršení sociálního klimatu v rámci organizace.

Pokud jde o právní předpisy o ochraně údajů, představují anonymní oznámení specifický problém v souvislosti se zásadním požadavkem nestranného shromažďování údajů. Pracovní skupina zastává názor, že v zájmu splnění tohoto požadavku by mělo být pravidlem, aby se prostřednictvím postupů oznamování podávala pouze oznámení s uvedením totožnosti oznamovatele.

Pracovní skupina si však uvědomuje, že oznamovatelé nemusí být vždy v takové pozici nebo duševním stavu, aby v oznámení uvedli svou totožnost. Rovněž si je vědoma skutečnosti, že v rámci společností se běžně podávají anonymní stížnosti, a to zejména v situacích, kde neexistují organizované mechanismy anonymního oznamování, a že tuto realitu nelze ignorovat. Pracovní skupina proto zastává názor, že lze výjimečně a za dále uvedených podmínek se mohou prostřednictvím postupů oznamování podávat a řešit anonymní oznámení.

Pracovní skupina se domnívá, že by postupy oznamování měly být nastaveny tak, aby nebyla dávána přednost anonymním zprávám jako obvyklému způsobu podávání stížností. Společnosti by především neměly veřejně oznamovat možnost podávání anonymních zpráv prostřednictvím tohoto mechanismu. Na druhé straně, jelikož by postupy oznamování měly zajišťovat zachovávání mlčenlivosti při nakládání s totožností oznamovatele, mělo by být osobě, která zamýšlí podat oznámení na základě postupu oznamování, dáno na srozuměnou, že nebude v důsledku svého jednání vystavena postihu. Z tohoto důvodu by měl oznamovatel být při prvním kontaktu s postupem oznamování informován, že jeho totožnost bude uchována v tajnosti ve všech fázích řízení a zejména nebude odhalena třetím stranám, ať již se jedná o osobu, proti níž bylo vzneseno podezření nebo o liniový management zaměstnavatele. Bude-li osoba podávající oznámení prostřednictvím uvedeného mechanismu vzdor těmto informacím trvat na své anonymitě, oznámení bude v rámci postupu přijato. Rovněž je nutné informovat oznamovatele o tom, že může být nutné sdělit jejich totožnost příslušným osobám činným v dalším vyšetřování nebo v následném soudním řízení zahájeném na základě výsledku vyšetřování provedeného v rámci postupu oznamování.

---

[17] Například podle zákona Spojeného království „Public Interest Disclosure Act“.

Při zpracovávaní anonymních oznámení je nutno postupovat velmi obezřetně. V rámci této obezřetnosti by se například mohlo vyžadovat, aby první příjemce přezkoumal, zda je možno připustit oznámení a zda je vhodné uvést jej v rámci postupu do oběhu. Rovněž by bylo vhodné zvážit, zda by se anonymní oznámení z důvodu rizika zneužití měla vyšetřovat a zpracovávat rychleji než stížnosti podané pod podmínkou mlčenlivosti. Takováto zvláštní obezřetnost však neznamená, že by se anonymní oznámení neměla vyšetřovat, aniž by došlo k náležitému posouzení všech skutečností případu jako tehdy, bylo-li oznámení podáno otevřeně.

iv) Proporcionalita a přesnost shromažďovaných a zpracovávaných údajů

V souladu s čl. 6 odst. 1 písm. b) a c) směrnice o ochraně údajů lze osobní údaje shromažďovat pouze pro účely specifikovaného, výslovně stanoveného a zákonného použití a tyto údaje musí být adekvátní, relevantní a nikoli nepřiměřené účelům, k nimž se shromažďují nebo dále zpracovávají.

Vzhledem k tomu, že účelem postupu oznamování je zajištění řádné správy a řízení společností, měly by se údaje shromažďované a zpracovávané v rámci postupů oznamování omezit jen na skutečnosti, které souvisí s tímto účelem. Společnosti, které zavádějí tyto postupy, by měly přesně vymezit druh informací, jež se mají prostřednictvím postupu zpřístupňovat, tím, že podávané informace omezí na informace týkající se účetnictví, vnitřních účetních kontrol, auditu nebo bankovní a finanční trestné činnosti a boje proti úplatkářství. Je všeobecně známo, že v některých zemích mohou právní předpisy výslovně stanovit uplatňování postupů oznamování na jiné kategorie závažných protiprávních jednání, jež je zapotřebí zveřejnit z důvodu veřejného zájmu[18]. Ty však nepatří do předmětu úpravy tohoto stanoviska, neboť se nemohou uplatňovat v jiných zemích. V rámci postupu by se měly zpracovávat jen ty osobní údaje, které jsou objektivně naprosto nutné k prověření předložených tvrzení. Oznámení o stížnostech by se kromě toho měly uchovávat odděleně od ostatních osobních údajů.

Pokud se skutečnosti oznámené v rámci postupu oznamování nevztahují na oblasti příslušného mechanismu, lze je předat příslušným odpovědným osobám společnosti, popř. organizace, jsou-li ohroženy významné zájmy subjektu, jehož se údaje týkají, nebo morální integrita zaměstnanců, nebo v případě, že vnitrostátní právní předpisy stanoví zákonnou povinnost oznamovat informace veřejným orgánům nebo orgánům činným v trestním řízení.

v) Přísné dodržování lhůt pro uchovávaní údajů

Ve směrnici 95/46/ES se stanoví, že se zpracovávané osobní údaje uchovávají po dobu potřebnou pro účel, pro nějž byly shromážděny nebo dále zpracovány. Tento požadavek je nutný k zajištění souladu se zásadou proporcionality zpracovávaní osobních údajů.

Osobní údaje zpracovávané v rámci postupů oznamování by poté měly být neprodleně vymazány, obvykle do dvou měsíců od ukončení vyšetřování skutečností uvedených v oznámení.

---

[18] Například podle zákona Spojeného království „Public Interest Disclosure Act 1998“.

Uvedené lhůty se nevztahují na případy, kdy bylo zahájeno soudní nebo disciplinární řízení proti obviněnému nebo oznamovateli, jenž se dopustil oznámení nepravdivých skutečností nebo pomluvy. V uvedených případech se osobní údaje uchovávají až do ukončení takovýchto řízení i během lhůty pro podání opravného prostředku. Tyto lhůty pro uchovávaní údajů se řídí právními předpisy jednotlivých členských států.

Jestliže subjekt, který vyřizuje upozornění, zjistí, že toto upozornění je neopodstatněné, je neprodleně proveden výmaz souvisejících osobních údajů.

Kromě toho se i nadále uplatní vnitrostátní právní předpisy upravující archivaci údajů obchodních společností. Tyto předpisy mohou především upravovat přístup k archivovaným údajům a přesně vymezit účely, pro něž je přístup umožněn, okruh osob, kterým lze umožnit přístup k této dokumentaci, a jiná vhodná bezpečnostní opatření.

3. Poskytování jasných a úplných informací o postupu oznamování (článek 10 směrnice o ochraně údajů)

V zájmu splnění požadavku jasnosti a úplnosti informací o postupu je správce údajů povinen informovat subjekt, jehož se údaje týkají, o existenci, účelu a fungování postupu oznamování, o adresátech oznámení, právu na přístup k údajům, a na opravu a výmaz údajů o osobách, kterých se oznámení týká.

Správci údajů by rovněž měli informovat o skutečnosti, že je totožnost oznamovatele uchovávána v tajnosti po celou dobu řízení a že zneužití postupu může mít za následek zahájení řízení proti osobě, která se takového zneužití dopustila. Na druhé straně lze uživatele postupu informovat i o tom, že při užití postupu v dobré víře nebudou ohroženi sankcí.

4. Práva osoby, proti níž bylo vzneseno podezření

Právní rámec vytvořený směrnicí 95/46/ES klade důraz na ochranu osobních údajů příslušného subjektu. Vzhledem k tomu by z hlediska ochrany údajů měly být postupy oznamování zaměřeny na práva subjektu, kterého se údaje týkají, aniž by došlo k porušení práv oznamovatele. Mezi právy dotčených stran, včetně legitimní potřeby společnosti provést vyšetřování, by mělo být dosaženo rovnováhy.

i) Právo na informace

V článku 11 směrnice 95/46/ES se stanoví povinnost informovat fyzické osoby v případě, že osobní údaje nebyly získány přímo od nich, ale od třetí strany.

Osoba odpovědná za řízení postupu oznamování informuje osobu označenou v oznámení za podezřelou co možná nejdříve poté, co byly zaznamenány údaje, které se jí týkají. Podle článku 14 má tato osoba rovněž právo vznést námitky proti zpracovávání jejích údajů v případě, že je legitimita zpracovávaní založena čl. 7 písm. f). Právo vznést námitky však lze uplatňovat jen ze závažných oprávněných důvodů, jež se týkají konkrétní situace této osoby.

Zaměstnanec, o němž bylo podáno oznámení, musí být informován především o: [1] subjektu odpovídajícím za řízení postupu oznamování, [2] skutcích, z jejichž spáchání je obviněn, [3] odděleních nebo útvarech jeho obchodní společnosti nebo jiných subjektů či společností ve skupině, k níž přináleží jeho společnost, jimž lze doručit oznámení a [4] o tom, jak může uplatnit své právo na přístup k informacím a na jejich opravu.

Pokud však existuje vážné riziko, že by byla poskytnutím těchto informací ohrožena schopnost společnosti účinně prověřit daná tvrzení nebo získat potřebné důkazy, může být podezřelá osoba informovaná až poté, co takové riziko zanikne. Účelem této výjimky z pravidla stanoveného článkem 11 je zajistit důkazní prostředky a ochránit je před zničením nebo pozměněním osobou označenou za podezřelou. Výjimku je nutno uplatňovat restriktivně na základě posouzení každého jednotlivého případu, přičemž by dotčené zájmy měly být uváženy v širších souvislostech.

V rámci postupu oznamování je třeba přijmout nutná opatření zabraňující zničení zpřístupněných informací.

ii) Právo na přístup k údajům, jejich opravu a výmaz

Podle článku 12 směrnice 95/46/ES mají subjekty, o kterých se vedou údaje, možnost přístupu k údajům zaznamenaným o jejich osobách pro účely kontroly přesnosti údajů a jejich opravy v případě, že jsou nepřesné, neúplné nebo neaktuální (dále jen „právo na přístup k údajům a jejich opravu“). V důsledku toho se při zavádění postupů oznamování musí zajistit respektování práva fyzických osob na přístup k údajům a na opravu nesprávných, neúplných nebo neaktuálních údajů.

Výkon těchto práv však lze omezit v zájmu zajišťování ochrany práv a svobod jiných subjektů zapojených do mechanismu oznamování. Takovéto omezení by se mělo uplatňovat na základě posouzení každého jednotlivého případu.

Osoba označená v oznámení za podezřelou nesmí být v rámci postupu za žádných okolností informována o totožnosti oznamovatele s uvedením důvodu, že jako osoba podezřelá má právo na přístup k informacím. To však neplatí, jestliže oznamovatel úmyslně podá nepravdivé oznámení. S výjimkou uvedeného případu by však vždy mdlo být zaručeno utajení totožnosti oznamovatele.

Kromě výše uvedených skutečností mají subjekty, o nichž se vedou údaje, právo na opravu nebo výmaz svých údajů, jestliže jejich zpracovávání není v souladu s ustanoveními této směrnice, a to především z důvodu neúplnosti nebo nepřesnosti údajů (plánek 12 písm. b)).

5. Bezpečnost úkonů zpracovávání údajů (článek 17 směrnice 95/46/ES)

i) Hmotněprávní opatření k zajištění bezpečnosti údajů

V souladu s článkem 17 směrnice 95/46/ES přijme společnost anebo organizace, která odpovídá za řízení postupu oznamování, veškerá odůvodněná technická a organizační opatření na zajištění bezpečnosti údajů při jejich shromažďování, předávání anebo uchovávání. Účelem tohoto článku je zajistit ochranu údajů před náhodným anebo nezákonným zničením nebo náhodnou ztrátou a neoprávněným zveřejněním nebo neoprávněným přístupem.

Oznámení lze přijmout jakýmikoliv elektronickými či jinými prostředky zpracování údajů. Uvedené prostředky by měly být používány výlučně pro postup oznamování s cílem zabránit jeho využití v rozporu s jeho původním účelem a přispět ke zvýšení ochrany důvěrnosti údajů.

V souladu s bezpečnostními předpisy platnými v různých členských státech musí být tato bezpečnostní opatření přiměřená účelu vyšetřování oznámených problémů.

Jestliže provádění postupu oznamování zajišťuje externí poskytovatel služeb, je potřebné zaručit přiměřenou ochranu informací prostřednictvím smlouvy mezi ním a správcem údajů. Kromě toho musí správce údajů především přijmout veškerá potřebná opatření k zajištění bezpečnosti informací zpracovávaných v průběhu celého řízení.

ii) Zachovávání mlčenlivosti o oznámeních podaných prostřednictvím postupu oznamování

Zachovávání mlčenlivosti o oznámeních je základním předpokladem ke splnění povinnosti zaručit bezpečnost operací zpracovávání údajů vyžadovanou směrnicí 95/46/ES.

V zájmu dosažení cíle, jemuž má postup oznamování sloužit, a s cílem motivovat fyzické osoby, aby postup využívaly a oznamovaly skutečnosti, které mohou nasvědčovat pochybení anebo protiprávnímu jednání ze strany společnosti, je velmi důležité zajistit dostatečnou ochranu oznamovatelů prostřednictvím povinnosti zachovávat mlčenlivost o oznámeních a utajení jejich totožnosti před třetími stranami.

Společnosti, které zavádějí postupy oznamování, by měly přijmout vhodná opatření k zajištění utajení totožnosti oznamovatele a zabránění jejich zpřístupnění osobě označené za podezřelou, a to v průběhu jakéhokoliv vyšetřování. Pokud se však prokáže, že oznámení je neodůvodněné, a oznamovatel podal nepravdivé oznámení úmyslně, může mít osoba označená za podezřelou zájem na zahájení řízení ve věci urážky na cti anebo pomluvy. V tomto případě může být nutné oznámit osobě označené za podezřelou totožnost oznamovatele, pokud to umožňuje vnitrostátní právní úprava. Vnitrostátní právní předpisy a zásady, jimiž se řídí oznamování v oblasti správy a řízení společností, rovněž zajišťují ochranu oznamovatele před odvetnými opatřeními za využití postupu oznamování, jimiž jsou např. disciplinární opatření anebo diskriminační přístup uplatňovaný ze strany společnosti anebo organizace.

Zachovávání mlčenlivosti o osobních údajích musí být zaručeno v průběhu jejich shromažďování, zpřístupňování anebo uchovávání.

6. Správa postupů oznamování

V souvislosti s postupy oznamování je potřeba pečlivě zvážit, jakým způsobem se mají oznámení přijímat a jak se s nimi má nakládat. Třebaže pracovní skupina dává přednost zajištění postupu v rámci společnosti, je si vědoma, že společnosti se mohou rozhodnout využít externích poskytovatelů služeb, kterým svěří část správy postupu, především v oblasti přijímání oznámení. Tito externí poskytovatelé služeb musí být vázáni přesně vymezenou povinností zachovávat mlčenlivost a zavázat se k dodržování zásady ochrany údajů. Bez ohledu na to, zda společnost zřídila vnitřní postup oznamování, anebo využila externích poskytovatelů služeb, musí především dodržovat ustanovení článků 16 a 17 směrnice.

i) Zvláštní interní organizační jednotka pověřená správou postupů oznamování

V rámci společnosti anebo skupiny je nutno zřídit zvláštní organizační jednotku pověřenou zpracováváním oznámení a vedením vyšetřování.

Tuto organizační jednotku má tvořit pouze omezený počet speciálně vyškolených a motivovaných osob smluvně zavázaných zachovávat zvláštní povinnosti v souvislosti s ochranou důvěrných informací.

Postup oznamování by měl být důsledně oddělen od jiných organizačních jednotek společnosti, např. oddělení lidských zdrojů.

Dále je nutno v potřebném rozsahu zajistit, aby byly shromažďované a zpracovávané informace zprostředkovávány pouze osobám, které mají v rámci společnosti anebo skupiny, do které společnost patří, zvláštní pověření provádět vyšetřovaní oznámených skutečností nebo přijímat potřebná opatření navazující na oznámené skutečnosti. Osoby, jimž jsou tyto informace poskytovány, musí o nich zachovávat mlčenlivost a zajistit dodržování bezpečnostních opatření.

ii) Možnost využití externích poskytovatelů služeb

Jestliže se společnosti nebo skupiny společností obrátí na externí poskytovatele služeb a svěří jim část správy postupu oznamování, nesou i nadále zodpovědnost za výsledné operace zpracovávání údajů, jelikož externí poskytovatelé služeb působí jen jako zpracovatelé údajů ve smyslu směrnice 95/46/ES.

Externími poskytovateli služeb mohou být společnosti provozující telefonická střediska, specializované společnosti nebo advokátní kanceláře, které se specializují na přijímání oznámení a v některých případech i na provádění některých nutných vyšetřovacích úkonů.

Tito externí poskytovatelé služeb budou rovněž povinni dodržovat zásady zakotvené v směrnici 95/46/ES. Na základě smlouvy se společností, jejímž jménem se postup oznamování provozuje, se musí zavázat, že budou informace shromažďovány a zpracovávány v souladu se zásadami zakotvenými ve směrnici 95/46/ES, a to výlučně jen pro účely, pro než byly shromážděny. Především musí dodržovat přesně vymezené povinnosti zachovávat mlčenlivost a oznamovat zpracovávané informace pouze vymezeným osobám ve společnosti nebo organizaci, které jsou pověřeny vyšetřováním oznámených skutečností anebo přijímáním potřebných opatření v návaznosti na oznámené skutečnosti. Rovněž budou povinni dodržovat lhůty pro uchovávání údajů, jimiž je vázán správce údajů. Společnost, která používá tyto postupy, musí z důvodu své funkce jakožto správce údajů pravidelně prověřovat dodržování zásad stanovených pokyny externích poskytovatelů služeb .

iii) Zásada vyšetřování podniků EU v EU a výjimky z této zásady

S přihlédnutím k charakteru a struktuře nadnárodních skupin může být zapotřebí zprostředkovávat skutečnosti a výsledky oznámení v rámci širší skupiny i mimo EU.

O tom, na jaké úrovni, a tedy v kterém státě by se mělo oznámení posuzovat, by se v zájmu dodržení zásady proporcionality mělo zpravidla rozhodnout s přihlédnutím k povaze a závažnosti údajného protiprávního jednání. Pracovní skupina je toho názoru, že by skupiny měly v zásadě oznámení řešit na místní úrovni, t.j. v jednom z členských států EU, aniž by automaticky zprostředkovávaly veškeré informace ostatním společnostem skupiny.

Pracovní skupina však uznává určité výjimky z tohoto pravidla.

Údaje přijaté prostřednictvím postupu oznamování lze zprostředkovat v rámci skupiny v případě, že je jejich zprostředkování potřebné z důvodu vyšetřování, a to vzhledem

k povaze nebo závažnosti oznámeného protiprávního jednání nebo pokud to vyžaduje struktura skupiny. Zprostředkování informací se považuje za potřebné pro účely vyšetřování, například v případě, kdy je v oznámení označen za podezřelého partner jiné právnické osoby v rámci skupiny, popř. významný člen nebo řídící pracovník dotčené společnosti. V takovém případě musí být údaje zprostředkovávány za podmínky zachování mlčenlivosti a bezpečnosti příslušné organizační jednotky právního subjektu, jemuž se informace poskytují a který poskytuje v souvislosti se správou oznámení stejné záruky jako organizace pověřená vyřizováním těchto oznámení ve společnosti působící v EU.

7. Předávání údajů do třetích zemí

Předávání údajů do třetích zemí se řídí články 25 a 26 směrnice 95/46/ES. Užití článků 25 a 26 nabývá na významu především tehdy, jestliže společnost svěří část správy postupu oznamování externímu poskytovatelovi služeb působícímu mimo EU, anebo pokud byly údaje získané oznámením uvedeny do oběhu v rámci skupiny, a v důsledku toho byly poskytnuty některým společnostem mimo území EU.

K těmto přenosům údajů může dojít především v případě společností působících v EU jako dceřiné společnosti (organizační složky) společností ze třetích zemí.

Jestliže třetí země, do níž mají být údaje odeslány, nezajišťuje přiměřenou úroveň ochrany osobních údajů podle článku 25 směrnice 95/46/ES, lze údaje předávat z těchto důvodů:

[1] příjemcem osobních údajů je subjekt působící ve Spojených státech amerických, který se zavázal dodržovat zásady „bezpečného přístavu“ (Safe Harbour);

[2] příjemce uzavřel se společností v EU, která údaje předává, smlouvu o předávání údajů, v níž se zavázal k přiměřeným ochranným opatřením například na základě vzorové smluvní doložky vydané Evropskou komisí na základě rozhodnutí Komise ze dne 15. června 2001 nebo 21. prosince 2004;

[3] příjemce přijal soubor závazných vnitropodnikových pravidel, které byly náležitě schváleny příslušnými orgány ochrany údajů.

8. Dodržování oznamovací povinnosti

Na základě uplatňování článků 18 až 20 směrnice o ochraně údajů musí společnosti, které zřídily postup oznamování, dodržovat povinnost podávat oznámení vnitrostátním orgánům pro ochranu údajů nebo se podrobit předběžným kontrolám prováděným těmito orgány.

V členských státech, kde je prováděn tento postup oznamování, mohou operace zpracovávání údajů, jež by mohly vyvolat zvláštní rizika ohledně práv a svobod subjektu, o němž jsou údaje vedeny, podléhat předběžným kontrolám vnitrostátních orgánů pro ochranu údajů. O takovýto případ by se mohlo jednat, pokud vnitrostátní právní předpisy umožňují, aby údaje o podezřeních z trestných činů zpracovávaly soukromé právní subjekty za určitých zvláštních podmínek, například pod podmínkou předchozí kontroly příslušnými vnitrostátními orgány dozoru. O tento případ by se mohlo jednat rovněž tehdy, jestliže se vnitrostátní orgán domnívá, že operace zpracovávání údajů mohou subjektu, jehož se oznámení týká, bránit ve výkonu určitého práva, využívaní jistých výhod anebo v uzavírání smluv. Otázka, zda operace zpracovávání údajů podléhají

předchozí kontrole, se posuzuje na základě vnitrostátních právních předpisů a zvyklostí vnitrostátního orgánu pro ochranu údajů.

V – ZÁVĚRY

Pracovní skupina je toho názoru, že postupy oznamování mohou představovat užitečný prostředek, s jehož pomocí může společnost nebo organizace monitorovat dodržování obecných právních předpisů i předpisů týkajících se správy a řízení společností, zejména pak účetnictví, vnitřních účetních kontrol a auditu, jakož i boje proti úplatkářství a trestné činnosti v bankovním a finančním odvětví i jiných porušení trestného práva. Mohou dané společnosti napomoci při řádném provádění zásad správy a řízení společností a odhalovaní skutečností, které by mohly mít vliv na postavení společnosti.

Pracovní skupina zdůrazňuje, že postupy oznamování v oblastech účetnictví, vnitřních účetních kontrol a auditu, jakož i potírání úplatkářství a trestné činnosti v bankovním a finančním odvětví, jichž se týká předkládané stanovisko, je třeba zavádět v souladu se zásadami ochrany osobních údajů zakotvenými ve směrnici 95/46/ES. Zastává názor, že dodržování těchto zásad přispívá k řádnému fungování uvedených postupů. Zajištění základního práva na ochranu osobních údajů, ať již se jedná o oznamovatele nebo osobu označenou za podezřelou, má v průběhu celého řízení o oznámení s využitím postupu oznamování zásadní význam.

Pracovní skupina zdůrazňuje, že zásady ochrany údajů stanovené ve směrnici 95/46/ES je třeba v plné míře uplatňovat na postupy oznamování, především co se týče práva osoby označené za podezřelou na přístup k údajům i jejich opravu a výmaz. Pracovní skupina však s přihlédnutím k různým dotčeným zájmům uznává, že výkon těchto práv může ve velmi specifických případech podléhat omezením v zájmu dosažení rovnováhy mezi právem na ochranu soukromí a zájmy sledovanými postupem oznamování. Jakákoliv omezení této povahy by však měla být uplatňována restriktivně v rozsahu, v němž jsou nutná k dosažení cílů postupu oznamování.

V Bruselu dne 1. února 2006

Za pracovní skupinu

předseda
Peter Schaar

Pracovní skupina pro ochranu údajů zřízená podle článku 29

01313/06/CS
WP 123

Stanovisko č. 6/2006 k návrhu nařízení Rady o příslušnosti, použitelném právu, uznávání a výkonu rozhodnutí a spolupráci ve věcech vyživovací povinnosti

přijaté dne

9. srpna 2006

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

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

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

PRACOVNÍ SKUPINA PRO OCHRANU FYZICKÝCH OSOB
PŘI ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

zřízená směrnicí Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995,

s ohledem na ustanovení článku 29 a čl. 30 odst. 1 písm. a) a odst. 3 uvedené směrnice a ustanovení čl. 15 odst. 3 směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002,

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

přijala toto stanovisko:

I. Souvislosti

Pracovní skupina byla informována o návrhu Komise na vydání nařízení Rady o příslušnosti, použitelném právu, uznávání a výkonu rozhodnutí a spolupráci ve věcech vyživovací povinnosti Cílem návrhu je odstranit překážky, které zabraňují úspěšnému vymáhání výživného v rámci celé Evropské unie.

Zejména kapitola VIII tohoto návrhu („Spolupráce“) obsahuje postup, jehož součástí je úprava shromažďování informací o situaci oprávněného i povinného, jakož i výměny těchto informací prostřednictvím sítě ústředních orgánů členských států. V souvislosti s touto úpravou vyvstává řada otázek týkajících se ochrany údajů, jež chce pracovní skupina v tomto stanovisku blíže osvětlit.

II. Právní rámec zpracování osobních údajů

Podle postupu, jehož užití se předpokládá v tomto návrhu, lze v procesu shromažďování a zpracování osobních údajů rozlišit tři základní etapy:

- osobní údaje zpracovávané určitým počtem správců údajů k nejrůznějším účelům (například zaměstnavateli, finančními úřady, úřady sociálního zabezpečení nebo orgány, které vedou veřejné rejstříky a registry) jsou využívány ústředními orgány za účelem usnadnění vymáhání vyživovacích povinností;
- osobní údaje shromážděné ústředními orgány jsou sumarizovány a předány soudu, který rozhoduje o pohledávce výživného;
- soud, který rozhoduje o pohledávce výživného, tyto údaje zpracuje pro účely zajištění výkonu rozhodnutí o vyživovacích povinnostech.

Při užití tohoto postupu je třeba uplatnit řadu zásad a pravidel obsažených ve směrnici 95/46/ES (dále jen „Směrnice“).

V první etapě shromažďování údajů ústředním orgánem zpracovávaných k jinému, neslučitelnému účelu představuje výjimku ve smyslu zásady omezení účelu stanovené v článku 6 Směrnice. Takové výjimky lze uplatnit pouze tehdy, jsou-li splněny podmínky článku 13 Směrnice. Podle ustanovení tohoto článku „*členské státy mohou přijmout legislativní opatření s cílem omezit rozsah povinností a práv stanovených v různých článcích Směrnice, včetně čl. 6 odst. 1, jestliže toto omezení představuje opatření nezbytné pro zajištění […]*

ochrany subjektu údajů nebo práv a svobod druhých". Evropský soudní dvůr objasnil, že naopak předávání údajů třetím stranám k „hospodářským" účelům *„zakládá zásah ve smyslu článku 8 EÚLP*". Kromě toho by odchylky od zásady omezení účelu stanovené ve Směrnici musely zohlednit článek 13 Směrnice, a proto by musely *„být zdůvodněny z hlediska článku 8 Úmluvy"*, (věc Rechnungshof, C-465/00, §68 an.). Podle Úmluvy je ke zdůvodnění zásahu do práva na soukromý život nutné postupovat *„v souladu se zákonem*" a tento zásah musí být *„v demokratické společnosti nezbytný"* k dosažení cíle, který je ve veřejném zájmu. Štrasburská judikatura opakovaně připomněla, že právní předpisy upravující zásah do soukromého života *„musí s dostatečnou přesností vymezit rozsah diskreční pravomoci svěřené příslušným orgánům a způsob, jakým má být tato pravomoc vykonávána s ohledem na legitimní cíl daného opatření tak, aby byla občanům zajištěna dostatečná ochrana proti zvůli*[1] ".

Co se týče druhé a třetí etapy, spadá shromažďování a zpracování osobních údajů vnitrostátními ústředními orgány a soudy (nebo jinými vnitrostátními orgány, jimž je svěřeno rozhodování o vyživovací povinnosti) podle ustanovení článku 3 Směrnice do působnosti uvedené směrnice. Osobní údaje jsou v rámci soudní spolupráce v občanskoprávních věcech s přeshraničními prvky skutečně zpracovávány do té míry, v níž je to nezbytné pro řádné fungování vnitřního trhu, což bylo doloženo v důvodové zprávě návrhu samotného. Jedná se o oblast práva Společenství, a proto se zde neuplatní výjimky z působnosti Směrnice obsažené v čl. 3 odst. 2.

Vzhledem k tomu se toto zpracování údajů řídí zásadami a právními předpisy stanovenými Směrnicí, zejména pak následujícími ustanoveními:

- Článek 6 stanoví, že osobní údaje musejí být shromažďovány pro stanovené účely, výslovně vyjádřené a legitimní, a nesmějí být dále zpracovávány způsobem neslučitelným s těmito účely. Osobní údaje musejí být zároveň přiměřené, podstatné a nepřesahující míru s ohledem na účely, pro které jsou shromažďovány a/nebo dále zpracovávány; musejí být přesné a je-li to nezbytné, i aktualizované; musejí být uchovávány ve formě umožňující identifikaci subjektu údajů po dobu ne delší než je nezbytné pro uskutečnění cílů, pro které jsou shromažďovány nebo dále zpracovávány.
- Článek 7 vyžaduje přiměřený důvod, aby zpracování osobních údajů bylo oprávněné. Údaje lze zpracovávat zejména pokud je to nezbytné pro splnění právní povinnosti, které podléhá správce, nebo je-li to nezbytné pro vykonání úkolu ve veřejném zájmu nebo při výkonu veřejné moci, a to podle ustanovení písmene c) a e) citovaného článku.
- Článek 8, jedná-li se o citlivé údaje, například při výměně údajů o sociálních dávkách pobíraných z důvodu určitého zdravotního stavu. V takovýchto případech může být zpracování údajů oprávněné jen pokud je nezbytné pro zjištění, uplatnění nebo obranu právních nároků (čl. 8 odst. 2 písm. e) nebo jsou-li poskytnuta vhodná ochranná opatření, stanovená prostřednictvím vnitrostátních právních předpisů, mohou členské státy stanovit z důvodu významného veřejného zájmu i jiné výjimky (čl. 8 odst. 4).
- Ustanovení článků 10 a 11 ukládají povinnost informovat subjekty údajů o zpracování jejich osobních údajů.
- Článek 12 poskytuje subjektům údajů právo na přístup k jejich údajům a na opravu, výmaz nebo zablokování údajů, jejichž zpracování není v souladu s ustanoveními Směrnice.

[1] Rotaru v. Rumunsko, §55 an.; Amann v. Švýcarsko, §76 a §80; Khan v. Spojené království, §26; Valenzuela Contreras v. Španělsko, §60 a §61; Kopp v. Švýcarsko, §72 a §75; Funke v. Francie, § 57; Niemietz v. Německo, § 37; Kruslin v. Francie, §34 a §35; Malone v. Spojené království, §79 a §80.

- Článek 15 poskytuje občanům právo nestat se subjektem automatizovaných individuálních rozhodnutí.
- Články 16 a 17 ukládají všem subjektům pověřeným zpracováním údajů povinnost zachovávat důvěrnost a přijímat vhodná ochranná opatření.
- V článcích 22, 23 a 24 jsou upraveny opravné prostředky, náhrada škody a sankce za neoprávněné zpracování údajů.
- Články 25 a 26 upravují předávání osobních údajů do zemí, které nepatří do Evropského hospodářského prostoru.

III. Existující zajištění ochrany údajů.

Pracovní skupina s uspokojením konstatuje, že tento návrh již obsahuje řadu prvků, které mají za cíl dosáhnout souladu postupů zpracování údajů s výše vyjmenovanými zásadami a právními předpisy upravujícími ochranu údajů. Zmiňuje se zejména o dále uvedených opatřeních.

- ***Různé druhy informací musí být přístupné v různých stádiích postupu zjišťování existence vyživovací povinnosti.***

V souladu s článkem 6 Směrnice mohou být vyžádány a zpřístupněny osobní údaje nezbytné ke zjištění, kde se zdržuje povinný (například zjištění jeho adresy) a při zahájení řízení; na návrh osoby, která tvrdí, že má nárok na výživné, mohou být tyto údaje zpřístupněny. Naopak další údaje, které jsou nezbytné k vyhodnocení schopnosti povinného platit výživné a účinně plnit svou povinnost (například bankovní účty, mzda nebo obdobné příjmy) mohou být vyžádány a zpřístupněny jen tehdy, bylo-li v řádném kontradiktorním řízení prokázáno, že tato osoba skutečně dluží výživné.

- ***Existuje občanskoprávní filtrační mechanismus k zahájení výměny informací***

Podle návrhu může oprávněný prostřednictvím soudu podat ústřednímu orgánu žádost o informace. Podání žádosti prostřednictvím soudu představuje přiměřený kontrolní mechanismus ke zjištění věrohodného skutkového stavu, a k ověření, zda je návrh na vyměření výživného řádně odůvodněný a zda jsou dané údaje k tomuto účelu skutečně nezbytné.

- ***Vytváření kombinovaných rejstříků je zakázáno***

Současný návrh ukládá členským státům povinnost upravit přístup k údajům o povinném a oprávněném tak, že budou obsaženy v několika oddělených rejstřících. Vytváření konsolidovaných rejstříků obsahujících různé kategorie informací původně obsažených v oddělených rejstřících, s cílem usnadnit vyhledávání informací, by bylo spojeno se značnými riziky pro osoby, jichž se tyto údaje týkají. Návrh proto výslovně zakazuje vytváření konsolidovaných rejstříků, které by sdružovaly tyto informace.

- ***Existují záruky týkající se zpřístupněných údajů***

Návrh stanoví, že předávané informace smí být užívány pouze v souladu se zásadou omezení účelu zakotvenou ve Směrnici, a to pouze k usnadnění vymáhání nároků na výživné. Podle rozsahu předávaných informací a s tím spojených rizik je nutno vytvořit další ochranná opatření. Návrh obsahuje zejména tyto prvky:

– informace by měly být předávány dožádaným orgánem pouze dožadujícímu orgánu. Dožadující orgán poté smí předat informace pouze soudu nebo orgánu, který rozhoduje o nároku na výživné. Informace nesmí být sdělovány oprávněnému nebo třetí straně;

– jakmile dožádaný nebo dožadující orgán informace předá, musí provést jejich výmaz. Informace smějí být uchovávány pouze soudem, který rozhoduje o pohledávce výživného a to pouze po dobu, která je nezbytná k usnadnění vymáhání pohledávky výživného, nejdéle však po dobu jednoho roku. K tomuto poslednímu bodu vypracovala pracovní skupina konkrétně zaměřený komentář, který je obsažen v následujícím textu;

– dožádaný ústřední orgán musí poskytnout povinnému informace o zpracování jeho údajů v souladu s články 10 a 11 Směrnice.

IV. Komentář

Pracovní skupina vymezila další body, v nichž by měla být vytvořena doplňující opatření na ochranu údajů v systému výměny osobních údajů k zajištění plného souladu se zásadami a ustanoveními Směrnice. Vzhledem k tomu předkládá pracovní skupina následující připomínky k některým ustanovením návrhu.

- Návrh by měl obsahovat ustanovení upravující vhodná technická a organizační opatření k zajištění zabezpečení údajů v souladu s požadavky článku 17 Směrnice i přiměřenou povinnost mlčenlivosti. To se týká zejména předávaní osobních údajů, například podle článku 46.
- Článek 41 podává obecný popis úkolů ústředních orgánů při spolupráci v konkrétních případech. V oblasti výměny osobních údajů, a to zejména údajů o povinném, se jeví jako nezbytné předejít nedorozuměním a jasně stanovit, že takovéto shromažďování a výměnu lze provádět pouze za opatření na ochranu údajů, která jsou konkretizována v dalším textu. Za tímto účelem je nutno nahradit v čl. 41 odst.1 písm. a) bodu i) slova „zejména na základě článků 44 až 47“ přesnějším výrazem „za podmínek stanovených v článcích 44 až 47“. Co se týče výměny údajů o oprávněném, návrh by měl konkretizovat účel, který odůvodňuje takovouto výměnu a stanovit příslušné podmínky, jako je tomu v současné době v případě informací o povinném.
- Ustanovení čl. 44 odst. 1 odkazuje v hrubých rysech na povinnosti ústředních orgánů při obstarávání informací s obecným cílem usnadnit vymáhání pohledávek výživného a v písmenech a) až d) podává výčet konkrétních cílů. Toto ustanovení je ve své dosavadní formě příliš široké. Zásada omezení účelu a zásada proporcionality vyžaduje provedení řady změn; zejména:
  - by měl být podán restriktivní seznam datových prvků;
  - účely by měly být omezeny na 1) zjištění, kde se zdržuje povinný, a 2) zjištění a ohodnocení jeho majetku. Zjištění zaměstnavatele povinného nebo jeho bankovních účtů je relevantní jen když mzda nebo obdobný příjem a bankovní účet představují samy o sobě významné prvky majetkových hodnot povinného. Jsou-li tyto prvky zvláště zmíněny, měly by být uváděny v rubrice „ohodnocení majetku povinného“;
  - z ustanovení by mělo jasně vyplývat, že různé druhy údajů zpřístupňovaných pro uvedené účely by měly být shromažďovány a zpřístupňovány jen pokud je taková informace nezbytná a relevantní pro vymáhání těchto pohledávek; nemusí tomu tak být ve všech členských státech a za všech okolností;
  - text by měl odkazovat na zásadu, že by se neměly zpracovávat citlivé údaje.
- Ustanovení čl. 44 odst. 2 ukládá, aby shromažďování údajů obsáhlo minimálně informace z několika rejstříků. V zájmu omezení účelu a zajištění proporcionality by opět
  - mělo být vypuštěno vymezení minima zdrojů informací;

- měl by být uváděn jednoznačný vztah mezi vyžádanými informacemi a účelem; toto ustanovení by mělo zejména zajistit, že budou shromažďovány pouze informace, které jsou nezbytné a relevantní pro zamýšlený účel.
- Informace o odvodech sociálního pojištění zaměstnavateli podle písmene b) se nezdá být relevantní pro účely uvedené v čl. 44 odst. 1. Pokud se toto ustanovení skutečně vztahuje na povinného jakožto zaměstnavatele, mělo by být uvedeno, že jeho právní povinnosti vůči jeho zaměstnancům by neměly být dotčeny pohledávkami výživného vůči němu. Pokud se vztahuje na příspěvky, které zaměstnavatel povinného platí za povinného jakožto svého zaměstnance, takovéto příspěvky budou s největší pravděpodobností podléhat obdobné právní povinnosti, a tudíž by rovněž neměly být dotčeny žalobami na výživné. Proto se navrhuje, aby bylo z textu vypuštěno sousloví „*včetně odvodů sociálního pojištění zaměstnavateli"*.

- Ustanovení čl. 44 odst. 3 zakazuje vytváření nových rejstříků v členských státech. Za tímž účelem a pro úplnost by toto ustanovení místo obecné formulace mělo pojednávat o *nových typech zpracování osobních údajů, včetně vytváření nových rejstříků."* Je nutno výslovně zabránit zejména těm druhům zpracování údajů, které obsahují zvláštní rizika, jako je zpracování biometrických údajů.
- Ustanovení čl. 45 odst. 1 obsahující občanskoprávní filtr zpracování návrhu na přiznání výživného se v zásadě týká „soudu". Určení orgánu v rámci soudního systému, který smí rozhodnout o zasahování do práva na soukromí, se řídí článkem 8 EÚLP. Druhá věta tohoto ustanovení by tudíž měla znít „*příslušný orgán nebo soudní orgán této jurisdikce podle ustanovení vnitrostátního práva žádost postoupí...*"
- V čl. 45 odst. 4 je zřejmě typografická chyba. Je nutno uvést „*formuláře, na nějž odkazuje ustanovení odstavce 2"* nikoli odstavce 1.
- Ustanovení čl. 45 odst. 5 druhý pododstavec stanoví povinnost Komise zpřístupnit „tyto informace" veřejnosti. To se vztahuje k dotazu členských států, zda je zapotřebí předkládat doplňující doklady podle ustanovení prvního pododstavce. Výraz „tyto informace" však může být matoucí, neboť může být chápán tak, že odkazuje na osobní informace o povinném a oprávněném. Bylo by tudíž vhodné nahradit současné znění formulací *„Komise zpřístupní veřejnosti informace, zda členské státy požadují předkládání překladů"* nebo obdobnou větou.
- Článek 46 stanoví, aby dožadující ústřední orgán po předání informace soudu provedl její výmaz. V textu by mělo být uvedeno, že je tento výmaz nutno provést *„bezprostředně"* po předání.
- Ustanovení čl. 46 odst. 3 stanoví, že informace nesmí být uchovávána po dobu delší jednoho roku. Záměrem tohoto ustanovení je ochrana údajů a pracovní skupina tento úmysl Komise oceňuje. Pracovní skupina si však je rovněž vědoma, že tato doba může být v praxi příliš krátká nebo naopak příliš dlouhá pro zamýšlený účel zpracování. Aby bylo možno vzít v úvahu praktické potřeby, bylo by vhodnější stanovit, že soudní orgány mohou zpracovávat dané údaje pouze po dobu nezbytnou k tomu, aby se usnadnilo vymožení konkrétní pohledávky výživného.

- Článek 47 stanoví povinnost ústředního orgánu uvědomit povinného, že byly zpřístupněny jeho údaje. Toto ustanovení by mělo jasně vyjádřit, že oznámení musí být provedeno bezprostředně po zpřístupnění. Dále by v něm měla být obsažena informace o účelu zpracování. Ustanovení písmene c) by tudíž mělo znít *„o účelu zpřístupnění a o podmínkách...*[zbytek nezměněn]". Naopak název a adresa kontrolního orgánu uváděné v písmenu e) se nejeví jako nezbytné.
- Konkrétní odkaz na použitelnost směrnice 95/46/ES by měl být obsažen v textu nařízení v souladu s bodem odůvodnění 21. Článek 48 o vztazích k jiným nástrojům Společenství se jeví jako vhodný pro umístění tohoto odkazu. Navrhuje se tudíž, aby byl do článku 48 doplněn čtvrtý odstavec tohoto znění: "*4. Shromažďování a zpracování osobních údajů prováděné podle tohoto nařízení, zejména v rámci výměny informací podle článků 44 až 47, by mělo být prováděno v plném souladu s vnitrostátními právními předpisy přijatými na základě směrnice 95/46/ES“* nebo obdobná věta.
- Články 22, 24 a 35 se týkají zásahu jiného orgánu než vnitrostátního ústředního orgánu. V těchto případech by měla být stanovena povinnost informovat subjekt údajů podobně jako v článku 47.
- Příloha III obsahuje vzor informačního dopisu povinnému, proti němuž bylo vydáno rozhodnutí o přímých měsíčních platbách výživného. Tento návrh by měl zajistit, že informace obsažená v tomto dopisu bude v souladu s požadavky článku 11 Směrnice ohledně informací, které budou poskytnuty subjektu údajů, včetně konkrétního poučení o jeho právu na přístup k těmto údajům a na jejich opravu.
- Příloha V obsahuje vzor žádosti o předání informací. Bod 4.1.3 se týká „dalších užitečných informací“ a podává se v něm výčet řady prvků. V návrhu by mělo být jasně řečeno, že se to týká informací poskytnutých dožadující stranou s cílem usnadnit vyhledávání vyžádaných informací, ale netýká se to samotných vyžádaných informací. Nařízení by kromě toho mělo obsahovat ustanovení, která by konkretizovala podmínky užití těchto pomocných údajů v souladu se zásadami uvedenými v tomto dokumentu, a to včetně účelu, množství údajů a období, po něž je možné tyto údaje uchovávat. V souladu s předcházejícími komentáři k článku 47 by měl být upraven i návrh předchozích dvou případů informování povinného. Informování povinného je pravidlem a standardní volbou a nevychází ze zvláštního případu. Restriktivní opatření proti informování povinného představuje výjimku, kterou lze použít pouze ve zvláštním případě, při kterém musí být v žádosti výslovně uvedeno náležité odůvodnění.

Pracovní skupina pevně doufá, že úvahy obsažené v tomto stanovisku budou přiměřeným způsobem zohledněny.

V Bruselu dne 9. srpna 2006

Za pracovní skupinu

Předseda
Peter Schaar

Pracovní skupina zřízená podle článku 29

01935/06/CS
WP128

Stanovisko 10/2006 ke zpracovávání osobních údajů Společností pro celosvětovou mezibankovní finanční komunikaci (Society for Worldwide Interbank Financial Telecommunication (SWIFT))

Přijaté dne 22. listopadu 2006

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

Sekretariát zajišťuje ředitelství C (civilní soudnictví, práva a občanství) Evropské komise, generální ředitelství pro spravedlnost, svobodu a bezpečnost, B-1049 Brussels, Belgium, kancelář č. LX-46 01/43.

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

Shrnutí

Toto stanovisko pracovní skupiny zřízené podle článku 29 zahrnuje zjištění o zpracovávání osobních údajů Společností pro celosvětovou mezibankovní finanční komunikaci (Society for Worldwide Interbank Financial Telecommunication, dále jen „SWIFT“).

Pracovní skupina zřízená podle článku 29 v této souvislosti zdůrazňuje, že i v rámci boje proti terorismu a trestné činnosti musí zůstat základní práva zaručena. Proto trvá na respektování zásad globální ochrany údajů.

SWIFT je celosvětová služba přenosu finančních zpráv, která usnadňuje mezinárodní peněžní převody. SWIFT uchovává všechny zprávy po dobu 124 dní ve dvou operačních střediscích, z nichž jedno je v Evropské unii a druhé ve Spojených státech amerických – způsobem zpracování údajů uváděným v tomto dokumentu jako „zrcadlení“. Zprávy obsahují osobní údaje jako jména plátce a příjemce. Po teroristických útocích v září 2001 vydalo Ministerstvo financí USA podmínky pro úřední obsílky, které vyžadují, aby SWIFT poskytla přístup k informacím o zprávách uchovávaných ve Spojených státech amerických. SWIFT vyhověla úředním obsílkám, i když byla ujednána jistá omezení přístupu Ministerstva financí USA. Záležitost vešla ve známost díky pozornosti, kterou jí věnoval tisk, koncem června a začátkem července 2006.

Jako družstvo se sídlem v Belgii podléhá SWIFT belgickým právním předpisům na ochranu údajů, kterými se provádí směrnice Evropské unie o ochraně údajů 95/46/ES (dále jen „směrnice“). Finanční instituce se sídlem v Evropské unii, které užívají službu SWIFT, podléhají vnitrostátním právním předpisům pro ochranu údajů, kterými se provádí směrnice v členském státě, v němž jsou usazeny.

Pracovní skupina dochází k závěru, že:

- Jak SWIFT, tak i finanční instituce příkazce sdílejí společnou odpovědnost, třebaže na různé úrovni, za zpracování osobních údajů jako „správci údajů“ ve smyslu čl. 2 písm. d) směrnice.
- Další zpracovávání osobních údajů, při známém značném rozsahu úředních obsílek Ministerstva financí USA, je dalším účelem, který není slučitelný s původním obchodním účelem, ke kterému byly osobní údaje shromažďovány, ve smyslu čl. 6 odst. 1 písm. b) směrnice.
- Ani SWIFT, ani finanční instituce v Evropské unii neposkytly informace subjektům údajů o zpracování jejich osobních údajů, zejména pokud jde o jejich předávání do USA, jak je stanoveno v článcích 10 a 11 směrnice.
- Kontrolní opatření zavedená společností SWIFT, zejména v souvislosti s přístupem Ministerstva financí USA k údajům, nijak nenahrazují nezávislé přezkoumání, které mohlo být provedeno orgány dozoru zřízenými podle článku 28 směrnice.
- Pokud jde o předávání do operačního střediska Spojených států amerických, SWIFT se nemůže dovolávat článku 25 směrnice, aby prohlásila zpracování za oprávněné.
- Žádná z výjimek uvedených v čl. 26 odst. 1 směrnice se nevztahuje na zpracování údajů v USA.
- SWIFT nevyužila mechanismů uvedených v čl. 26 odst. 2 směrnice k tomu, aby obdržela oprávnění ke zpracování od belgického orgánu dozoru pro ochranu údajů.
- Pracovní skupina zřízená podle článku 29 vyzývá SWIFT a finanční instituce, aby neprodleně přijaly opatření za účelem napravení současného protiprávního stavu.
- Pracovní skupina zřízená podle článku 29 dále vyzývá k vyjasnění dohledu nad společností SWIFT.

Pracovní skupina zřízená podle článku 29 bude sledovat a monitorovat vše, co je uvedeno výše.

OBSAH

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

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

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

s ohledem na její jednací řád, a zejména na články 12 a 14 uvedené směrnice,

přijala toto stanovisko:

1. SOUVISLOSTI

Nezávislé orgány dozoru pro ochranu údajů v Evropské unii[2] posuzují závažnou otázku týkající se rozsáhlého předávání finančních údajů společností se sídlem v Evropské unii (SWIFT) orgánům Spojených států amerických. Podrobnosti a podmínky tohoto předávání, zejména zpracování osobních údajů týkajících se fyzických osob v Evropě, vyvolaly znepokojení orgánů pro ochranu údajů, které spojily své úsilí při šetření toku údajů a analýze jeho shody s evropskými zásadami soukromí, zejména se směrnicí o ochraně údajů (dále jen „směrnice“).

1.1 Sled událostí

Pozornost tisku ve sdělovacích prostředcích v Evropě a ve Spojených státech koncem června a začátkem července 2006 zpochybnila úlohu a odpovědnosti Společnosti pro celosvětovou mezibankovní finanční komunikaci (Society for Worldwide Interbank Financial Telecommunication, dále jen „SWIFT“) v souvislosti s předáním osobních údajů Úřadu pro řízení zahraničních aktiv (Office of Foreign Assets Control (OFAC)) Ministerstva financí Spojených států amerických. SWIFT je družstvo se sídlem v Belgii, které působí v oblasti zpracování finančních zpráv. Ukázalo se, že osobní údaje shromažďované a zpracovávané prostřednictvím sítě SWIFT pro mezinárodní peněžní převody pomocí identifikačního kódu banky (dále jen „BIC kód“) nebo „SWIFT“ kódu byly poskytovány Ministerstvu financí USA od konce roku 2001 na základě úředních obsílek podle amerického práva pro účely vyšetřování terorismu.

---

[1] Úřední věstník č. L 281 ze dne 23.11.1995, s. 31, k dispozici na webové stránce http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm

[2] Vedle orgánů Evropské unie zahájily šetření této otázky další orgány dozoru pro ochranu údajů: Austrálie, Kanada, Nový Zéland, Švýcarsko, Island.

Na základě pozornosti tisku vydala společnost SWIFT první prohlášení[3] dne 23. června 2006. SWIFT je podle jejího tiskového prohlášení „družstvo vlastněné průmyslem“, které poskytuje bezpečené, standardizované služby přenosu zpráv a komunikační software více než 7 800 finančním institucím na celém světě.“

Evropská komise se rozhodla, že bude tento případ pozorně sledovat a v červenci 2006 požádala belgické orgány o informace o podmínkách, za kterých SWIFT zpracovává osobní údaje, a zda dodržuje belgické právní předpisy pro ochranu údajů, kterými se provádí směrnice. Komise s členskými státy také ověřuje, zda banky využívající SWIFT k provádění platebních příkazů dodržují vnitrostátní právní předpisy pro ochranu údajů, pokud jde o zpracování osobních údajů týkajících se těchto plateb.

Rozhodnutím ze dne 6. července 2006[4] Evropský parlament vyzval členské státy k tomu, aby zajistily, že na vnitrostátní úrovni nebude právní vakuum a že se právní předpisy Společenství pro ochranu údajů budou vztahovat také na centrální banky, a aby tento stav ověřily. Evropský parlament vyjádřil v tomto rozhodnutí také vážné obavy ohledně účelů předávání údajů Ministerstvu financí USA. Také důrazně odmítl „jakékoli tajné operace na území Evropské unie“, které ovlivňují soukromí občanů Evropské unie. Dále prohlásil, že je hluboce znepokojen tím, že by se takové operace měly uskutečňovat bez vyrozumění občanů Evropy a jejich parlamentních zastoupení. Konečně vybídl Spojené státy americké a jejich tajné a bezpečnostní služby, aby jednaly v duchu dobré spolupráce a informovaly své spojence o veškerých bezpečnostních operacích, které hodlají uskutečnit na území Evropské unie. Byla nastolena otázka možnosti předávání spojeného s „nezákonnými činnostmi“, ale i předávání „informací o hospodářských činnostech dotčených osob a zemí“, které „by mohlo vést k celé řadě forem ekonomické a průmyslové špionáže“. Rozhodnutí požadovalo, aby členské státy předávaly výsledky jejich ověření Evropské komisi, Radě a Evropskému parlamentu.

Předseda pracovní skupiny zřízené podle článku 29 oznámil dne 27. července 2006, že se evropské orgány pro ochranu údajů rozhodly své činnosti koordinovat. Na příštím zasedání dne 26. a 27. září 2006 uspořádala pracovní skupina zřízená podle článku 29 první plenární rozpravu.[5]

Na veřejném slyšení uspořádaném dne 4. října 2006 Výborem pro občanské svobody Evropského parlamentu a Výborem pro hospodářské a měnové záležitosti Evropského parlamentu byla tato otázka, mimo další účastníky, projednána s vrchním finančním úředníkem společnosti SWIFT a s Evropskou centrální bankou[6].

---

[3] „Prohlášení společnosti SWIFT o politice souladu“ uveřejněné na webové stránce http://www.swift.com/index.cfm?item_id=59897

[4] Rozhodnutí Evropského parlamentu o zachycování údajů o bankovních převodech ze systému SWIFT tajnými službami USA (P6_TA-PROV(2006)0317)

[5] Tisková sdělení pracovní skupiny zřízené podle článku 29: Tiskové sdělení pracovní skupiny zřízené podle článku 29 ve věci Swift ze dne 28. července 2006: http://ec.europa.eu/justice_home/fsj/privacy/news/docs/PR_SWIFT_Affair_28_07_06_en.pdf; Tiskové prohlášení ve věci SWIFT ze dne 27. září 2006;

http://ec.europa.eu/justice_home/fsj/privacy/news/docs/PR_Swift_Affair_26_09_06_en.pdf .

[6] Plné znění veřejného slyšení lze najít na webové stránce http://www.europarl.europa.eu/news/expert/infopress_page/017-11292-275-10-40-902-20061002IPR11291-02-10-2006-2006-false/default_en.htm

Evropský inspektor ochrany údajů předložil několik úvodních připomínek ke svému šetření úlohy Evropské centrální banky (ECB) podle nařízení (ES) 45/2001.[7]

Na vnitrostátní úrovni kontaktovaly orgány dozoru pro ochranu údajů své příslušné bankovní organizace.

Belgický orgán pro ochranu údajů provedl šetření zákonnosti zpracovávání údajů společností SWIFT. Belgický orgán pro ochranu údajů navázal v průběhu tohoto šetření přímý kontakt se společností SWIFT za účelem stanovení jak působnosti, tak i rozsahu sledování a předávání údajů. Belgický orgán pro ochranu údajů stanovil ve svém rozhodnutí ze dne 27. září 2006, že předávání osobních údajů společností SWIFT do její americké pobočky je v rozporu s belgickým zákonem ze dne 8. prosince 1992 o ochraně soukromí v souvislosti se zpracováním údajů osobní povahy[8]. Belgický orgán pro ochranu údajů především zjistil, že SWIFT porušila základní ustanovení o povinnostech poskytování informací, omezení účelu zpracování údajů a předávání osobních údajů do třetích zemí. Belgický orgán pro ochranu údajů zjistil, že se SWIFT dopouštěla *„skrytého, soustavného, rozsáhlého a dlouhodobého porušování základních evropských zásad týkajících se ochrany údajů“*.

Na základě informací shromážděných během těchto šetření chce pracovní skupina analyzovat, jak SWIFT dodržuje zásady ochrany údajů, které jsou obsaženy ve směrnici a uskutečňovány ve všech členských státech podle vnitrostátních právních předpisů pro ochranu údajů se širokým rozsahem působnosti.

SWIFT zaslala předsedovi pracovní skupiny zřízené podle článku 29 kopii svých odpovědí orgánům pro ochranu údajů Belgie, Španělska a Francie[9].

1.2 Fakta

1.2.1 Zpracování údajů společností SWIFT v číslech

SWIFT zpracuje průměrně 12 milionů zpráv za den[10]. Celkový objem zpracovaných zpráv činil např. v roce 2005 až 2,5 miliardy zpráv, z nichž 1,6 miliardy byly pro Evropu a 467 milionů pro Ameriku. Informace zpracované společností SWIFT se týkají zpráv o finančních transakcích stovek tisíc občanů Evropské unie. Evropské finanční instituce (bez omezení na banky) využívají službu SWIFTNet FIN k celosvětovému přenosu zpráv v souvislosti s finančními převody mezi finančními institucemi. Tento přenos se uskutečňuje bez ohledu na to, zda jsou zprávy zpracovány v Evropské unii (EU) a v Evropském hospodářském prostoru (EHP) nebo ve třetí zemi.

---

[7] http://www.edps.europa.eu/Press/EDPS-2006-10-EN%20swift.pdf

[8] http://www.privacycommission.be/communiqu%E9s/AV37-2006.pdf

[9] Dopis společnosti SWIFT předsedovi pracovní skupiny zřízené podle článku 29 ze dne 31. července 2006.

[10] Výroční zpráva společnosti SWIFT 2005; k dispozici na webové stránce http://www.swift.com/index.cfm?item_id=59684 .

1.2.2 Kategorie zpracovávaných údajů

Zprávy přenášené prostřednictvím služby SWIFTNet FIN obsahují osobní údaje, jako jsou jména příjemce a příkazce. Zprávy týkající se plateb však mohou obsahovat více informací, například referenční číslo umožňující plátci a příjemci urovnat platbu pomocí jejich náležitých účetních dokladů. Některé druhy zpráv kromě toho umožňují zahrnout nestrukturované textové informace.

Nehledě na obchodní místa v různých zemích má SWIFT dvě operační střediska umístěná v pobočkách SWIFT, jedno v jednom členském státě Evropské unie a jedno ve Spojených státech amerických. V těchto operačních střediscích jsou jako součást služby SWIFTNet FIN všechny zprávy zpracované společností SWIFT uchovávány a zrcadleny po dobu 124 dní jako „záložní nástroj pro obnovu" pro klienty pro případ sporů mezi finančními institucemi nebo ztráty údajů. Po tomto období jsou údaje vymazány.

1.2.3 Úřední obsílky od Ministerstva financí USA

Od teroristických útoků v září 2001 adresovalo Ministerstvo financí USA řadu správních úředních obsílek operačnímu středisku SWIFT ve Spojených státech amerických. SWIFT na dotaz uvedla, že od Ministerstva financí USA dosud obdržela 64 úředních obsílek a že jim vyhověla.

Podle práva USA se správní úřední obsílkou rozumí příkaz od vládního úředníka třetí osobě, který příjemci nařizuje poskytnout některé informace.[11] Oblast úředních obsílek Ministerstva financí USA je v tomto případě věcně, územně i časově velmi široká a je blíže určena v úředních obsílkách a v korespondenci o jednáních mezi Ministerstvem financí USA a společností SWIFT. Tyto úřední obsílky jsou vydávány pro veškeré transakce, které souvisejí nebo mohou souviset s terorismem, vztahují se na počet zemí a jurisdikcí *x*, na den *y* nebo na lhůty „*od ... do ...*" v rozsahu od jednoho týdne do několika týdnů, na území USA i mimo něj. Týkají se zpráv o mezibankovních operacích v rámci USA, směřujících do/z USA a také zpráv z území mimo USA, například zpráv v rámci Evropské unie.[12]

SWIFT uzavřela soukromě dohodu s Ministerstvem financí USA o tom, jak vyhovět úředním obsílkám. SWIFT tvrdí, že tak obdržela *„významnou ochranu a záruky ohledně účelu, důvěrnosti, dohledu a kontroly nad omezenými soubory údajů poskytnutými na základě úředních obsílek"*[13].

Podle zjištění belgického orgánu pro ochranu údajů zajišťuje skutečné sdělování osobních údajů Ministerstvu financí USA operační středisko SWIFT v USA v několika

---

[11] Jednání před soudním výborem, podvýborem pro terorismus, technologii a vnitřní bezpečnost Spojených států amerických: „Nástroje pro boj proti terorismu: Orgán pro úřední obsílky a předběžné zadržení teroristů", svědectví Rachel Brandové, Principal Deputy Assistant Attorney General, Úřad pro soudní politiku, Ministerstvo spravedlnosti USA, dne 22. června 2004; http://kyl.senate.gov/legis_center/subdocs/062204_brand.pdf

[12] Srovnej stanovisko belgického orgánu pro ochranu údajů, B.2 (neoficiální překlad do angličtiny), poznámka pod čarou 8.

[13] „Prohlášení společnosti SWIFT o politice souladu" uveřejněné na webové stránce http://www.swift.com/index.cfm?item_id=59897.

krocích. Neprovádí se přímá extrakce individualizovaných údajů zrcadlených v databance společnosti SWIFT, nýbrž SWIFT místo toho dohodla koncept „černé skříňky“ s Ministerstvem financí USA, které povolilo předávání údajů ze zrcadlené databáze SWIFT do „černé skříňky“. Jakmile jsou údaje v „černé skříňce“, která je vlastnictvím Spojených států amerických, provede Ministerstvo financí USA expertní vyhledávání.

Další podrobnosti o sdělování osobních údajů Ministerstvu financí USA byly sděleny belgickému orgánu pro ochranu údajů a lze je najít v jeho stanovisku[14].

2. PLATNÝ RÁMEC PRO OCHRANU ÚDAJŮ

2.1 Použitelnost směrnice 95/46/ES

Protože jsou osobní údaje obsaženy ve zprávách přenášených prostřednictvím služby SWIFTNet FIN, má pracovní skupina za to, že se směrnice vztahuje na zpracovávání osobních údajů prostřednictvím služby SWIFTNet FIN.

Pracovní skupina zdůrazňuje, že skutečnost, že zpracovávání osobních údajů souvisí s poskytováním služby, není pro určení funkce subjektu jako správce údajů relevantní. Definice „zpracování osobních údajů“ a „osobních údajů“ jsou jasně vymezeny v článku 2 směrnice. Pokud činnosti vykonávané subjektem spadají pod tyto definice, vztahuje se na ně uvedená směrnice, a proto se zpracování údajů provede v plném souladu se směrnicí.

2.2 Právo použitelné pro SWIFT

Čl. 4 odst. 1 písm. a) směrnice uvádí, že každý členský stát použije na zpracování osobních údajů vnitrostátní ustanovení, která přijme na základě směrnice, pokud „(…) zpracování je prováděno v rámci činností provozovny správce na území členského státu“.

SWIFT má ústředí v La Hulpe v Belgii. SWIFT má také dvě operační střediska (jedno v Evropě a jedno ve Spojených státech amerických, která působí jako dokonalý „zrcadlový obraz“. Kromě toho má SWIFT několik obchodních míst ve Spojeném království, ve Francii, v Německu, v Itálii, ve Španělsku atd. Ústředí se sídlem v Belgii přijalo důležitá rozhodnutí o zpracovávání osobních údajů a předávání údajů Ministerstvu financí USA.

Zpracování osobních údajů společností SWIFT proto podléhá belgickým právním předpisům, kterými se provádí směrnice, bez ohledu na to, kde se údaje zpracovávají.

2.3 Právo použitelné pro finanční instituce

V souvislosti se zpracováním je pro finanční instituce využívající služby SWIFT k jejich mezinárodním platebním příkazům, které lze pokládat za správce, stanoveno použitelné vnitrostátní právo v čl. 4 odst. 1 písm. a) směrnice a pokud jde o instituce a orgány

---

[14] Viz. poznámka pod čarou 8.

Společenství, pak v článku 3 nařízení (ES) 45/2001[15]. To znamená, že v případě finančních institucí jsou použitelné různé – i když harmonizované – právní předpisy.

Pracovní skupina zdůrazňuje, že protože jsou osobní údaje zpracovávány při finančních transakcích týkajících se stovek tisíc občanů prostřednictvím institucí se sídlem v Evropské unii (družstvo SWIFT, jakož i finanční instituce využívající službu SWIFTNet FIN), jsou použitelné vnitrostátní právní předpisy pro ochranu údajů – přijaté na základě předpisů provádějících směrnici – různých dotčených členských států.

3. ÚLOHA SPOLEČNOSTI SWIFT A FINANČNÍCH INSTITUCÍ

Podle směrnice musí správce zajistit, aby byly dodržovány povinnosti související se zpracováním osobních údajů.

Otázkou je, zda SWIFT a/nebo finanční instituce mají být považovány za správce nebo zpracovatele údajů.

Podle definicí směrnice se „správcem“ rozumí „fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jakýkoli jiný subjekt, který sám nebo společně s jinými určuje účel a prostředky zpracování osobních údajů“ (čl. 2 písm. d)); „zpracovatelem“ se rozumí „fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jakýkoli jiný subjekt, který zpracovává osobní údaje pro správce“ (čl. 2 písm. e)).

3.1 Úloha společnosti SWIFT

SWIFT se vždy prezentovala jako „*pouze zprostředkovatel zpracování zpráv pro přenos zabezpečených a důvěrných finančních zpráv mezi finančními institucemi. SWIFT není banka, ani nevede účty pro klienty.*“ Tato prezentace byla také základem pro posuzování, která prováděly některé orgány pro ochranu údajů v členských státech při schvalování zpracování údajů jejich bankami.

Struktura mezinárodní služby SWIFT a smluvní ujednání mezi společností SWIFT a finančními institucemi jsou poměrně složité. Pracovní skupina však upozorňuje na to, že tento typ struktury včetně úlohy poskytovatele služeb spolupracujícího s dalšími subjekty není výjimečný. Zdá se, že struktura společnosti SWIFT je příkladem formální kooperativní sítě. Společnost SWIFT byla zřízena v roce 1973 skupinou evropských bank, která chtěla vyvinout nový způsob zasílání platebních příkazů korespondentským bankám standardizovaným způsobem. Pro tento účel byla podle belgického práva zřízena družstevní společnost s ručením omezeným.

Pracovní skupina poukazuje na podobné případy kooperativních sítí, jako je případ databází ukončených vztahů s obchodníky („Terminated Merchant Databases“), které provozují VISA a Mastercard ve spolupráci s finančními institucemi za účelem analýzy rizik spojených s přijetím každého jednotlivého obchodníka do systému VISA nebo

---

[15] 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; Úř. věst. L 8, 12.1.2001, s. 1.

Mastercard[16]. Pracovní skupina se také zmiňuje o případech zúčtování a vypořádání transakčních systémů a systémů rezervací pro cestující, kdy cestovní agentury a letecké společnosti na jedné straně a manažeři těchto systémů (například Galileo) na straně druhé mají různé odpovědnosti.

Nezávisle na smluvním vztahu mezi společností SWIFT a finančními institucemi podle občanského nebo obchodního práva, které může zahrnovat výraz „subdodavatel", z hlediska ochrany údajů, není SWIFT pouhým „subdodavatelem" nebo zpracovatelem ve smyslu článku 2 směrnice pro běžné zpracování osobních údajů k jejich obvyklému obchodnímu účelu. Fakta svědčí o tom, že se SWIFT v posledních několika desetiletích rozvíjela a že dělá více než jen jedná v zájmu svých klientů. I kdybychom se jen chvilku domnívali, že SWIFT jednala jako „zpracovatel", přece jen převzala určité odpovědnosti přesahující soubor požadavků a povinností kladených na zpracovatele, což nelze pokládat za slučitelné s jejím tvrzením, že je jen „zpracovatelem".[17] Vedení společnosti SWIFT působí v kontextu formální kooperativní sítě, která určuje jak účel, tak i prostředky zpracování údajů v rámci služby SWIFTNet a osobní údaje, které se prostřednictvím této služby zpracovávají. Vedení společnosti SWIFT rozhoduje nezávisle o úrovni informací poskytovaných finančním institucím v souvislosti se zpracováním. Vedení společnosti SWIFT může stanovit účel a prostředky zpracování prostřednictvím vývoje, marketingu a změn stávajících nebo nových služeb společnosti SWIFT a zpracování údajů, např. stanovením norem vztahujících se na její klienty, co se týče formy a obsahu platebních příkazů, aniž by si vyžádala souhlas finančních institucí. SWIFT také vytváří přidanou hodnotu za zpracování osobních údajů, např. uchovávání a ověřování správnosti osobních údajů a ochranu osobních údajů s vysokou úrovní zabezpečení. Vedení společnosti SWIFT má pravomoc přijímat důležitá rozhodnutí v souvislosti se zpracováním, např. o úrovni zabezpečení a umístění jejích operačních středisek. Vedení společnosti SWIFT konečně zcela nezávisle sjednává a vypovídá své dohody o službách a navrhuje a provádí změny svých různých smluvních dokumentů a politik[18]. Vše, co bylo uvedeno výše, naplňuje skutkový a právní význam pojmu zpracování.

Pokud jde o předávání osobních údajů Ministerstvu financí USA, rozhodla se SWIFT vyhovět úředním obsílkám USA. Prostřednictvím korespondence a uklidňujícího dopisu iniciovala neprůhledným způsobem jednání s Ministerstvem financí USA o podmínkách pro předávání osobních údajů Ministerstvu financí USA. Vědomě se rozhodla, že o tomto jednání nebude informovat příslušné finanční instituce. Kontrolní mechanismy získané a řízené společností SWIFT samozřejmě ovlivnily účel a rozsah předávání údajů Ministerstvu financí USA. Tyto činnosti značně přesahují obvyklé možnosti zpracovatele údajů se zřetelem na jeho předpokládanou nesamostatnost ve vztahu k příkazům správce údajů.

---

[16] Viz. např. pokyny „Guidelines for Terminated Merchant Databases" pracovní skupiny zřízené podle článku 29; k dispozici na webové stránce: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/others/2005-01-11-fraudprevention_en.pdf.

[17] Zpracovatelé údajů musí v každém případě dodržet směrnici, viz. např. čl. 17 odst. 3 týkající se bezpečnostních opatření.

[18] Srovnej ustanovení 4.5.3 obecných podmínek, které uvádí: „má se za to, že klient dal souhlas k takovému zpracování…".

Zatímco se SWIFT prezentuje jako zpracovatel údajů, a některé skutečnosti mohou naznačovat, že SWIFT v minulosti působila v některých případech jako zpracovatel pro finanční instituce, zastává pracovní skupina po uvážení účinného manévrovacího prostoru, který má v situacích popsaných výše, stanovisko, že SWIFT je správcem podle definice uvedené v čl. 2 písm. d) směrnice, jak co se týče běžného zpracování osobních údajů prostřednictvím její služby SWIFTNet, tak i dalšího zpracování prostřednictvím dalšího předávání osobních údajů Ministerstvu financí USA.

3.2 Úloha finančních institucí

Je nutno posoudit úlohu finančních institucí při používání služby SWIFTNet FIN. Některé finanční instituce nebyly společností SWIFT plně informovány o objemu a přesných charakteristikách zpracování a zrcadlení osobních údajů, včetně dalšího předávání zrcadlených osobních údajů Ministerstvu financí USA. Po zjištění těchto skutečností od 23. června 2006 si však všechny finanční instituce uvědomují tyto okolnosti, když zasílají osobní údaje prostřednictvím služby SWIFTNet FIN k účelu mezinárodních peněžních převodů.

Má se za to a očekává se, že si finanční instituce podrží určitý vliv na politiku družstva. Některé finanční instituce jsou zastoupeny v představenstvu společnosti SWIFT a současná struktura řízení společnosti SWIFT byla původně vytvořena tak, aby umožňovala bankám a finančním institucím ponechat si určitou kontrolu nad rozhodovacími procesy společnosti SWIFT. Proto by tyto instituce měly být považovány za spolupůsobící s družstvem, jehož členy jsou, při určování účelu a prostředků. Jsou také v přímém styku s dotčenými fyzickými osobami a hrají zásadní úlohu při provádění mezinárodních platebních příkazů svých klientů.

Je také důležité mít na paměti, že finanční instituce jsou samostatné a mohou sledovat vlastní cíle na mezibankovní úrovni. Pracovní skupina podotýká, že finanční instituce často přijímají v rámci mezibankovního styku velmi důležitá rozhodnutí o předávání osobních údajů společnosti SWIFT, mnohdy bez vědomí jejich klientů. Dokládají to tyto prvky:

- Finanční instituce často nezávisle rozhodují na mezibankovní úrovni o prostředcích používaných při provádění platebních příkazů. Mohou používat nebo vyvíjet alternativní nebo konkurenční služby pro přenos těchto finančních zpráv v rámci mezibankovního systému (např. elektronickou poštu, telefax, telefon). Výběr na této úrovni bude určovat globální parametry ochrany soukromí, pokud jde o platební příkazy prováděné finančními institucemi. Vzhledem k rozmanitosti služeb na mezibankovní úrovni se finanční instituce při výběru mezibankovní služby mohou řídit hledisky jinými než je bezpečnost informací – která je podmínkou samozřejmě vždy – například politikou profesionálního poskytovatele služeb v oblasti ochrany soukromí. Finanční instituce mohou využít buď politiku přísné ochrany soukromí konkrétního poskytovatele, nebo řešení, jako je virtuální privátní síť, jako záruku ochrany důvěry jejich klientů a jejich služeb v nejvyšší možné míře.

- Finanční instituce dodržují a akceptují smluvní rámec služby SWIFTNet FIN[19]. Ze smluvní dokumentace (Data Retrieval Policy[20]) a politiky souladu SWIFT jsou si zákazníci společnosti SWIFT vědomi obecné zásady předávání osobních údajů podléhajích úředním obsílkám, které jsou jim nebo společnosti SWIFT doručovány. Podle stanoviska belgického orgánu pro ochranu údajů argumentovala společnost SWIFT tím, že se mohlo jednat o tisíce nebo dokonce desítky tisíc úředních obsílek zaslaných finančním institucím za rok. Proto lze pochybovat o tom, že by si finanční instituce působící na trhu mezinárodních plateb nebyly vědomy obecné zásady úřední obsílky.
- Finanční instituce musí posoudit možné důsledky a rizika pro ochranu soukromí, včetně rizik porušení ochrany soukromí jejich klientů v souvislosti se službou SWIFTNet FIN, ke které se jako profesionální poskytovatel služeb smluvně zavazují. Proto je důležité prověřit, zda politika instituce příkazce týkající se ochrany soukromí obsahuje doložky o těchto rizicích.
- Vzhledem ke skutečnosti, že finanční instituce jednají jménem svých klientů dávajících platební příkazy, nesmějí předávat nutné údaje k jiným účelům než výhradně k převodu plateb. Je-li finanční instituci známo, že SWIFT užívá údaje jí svěřené i jinak než výhradně k převodu plateb, a přesto i nadále využívá služeb společnosti SWIFT, je nutno nastolit otázku právního základu takového převodu a použití: neexistuje-li zvláštní dohoda mezi finanční institucí a jejími klienty, nejeví se svěření bankovních údajů společnosti SWIFT k jiným účelům než pouze k uznané službě jako oprávněné.

Finanční instituce proto nejsou pouhými správci ve smyslu čl. 2 písm. d) směrnice, co se týče jejich vlastních zpracování údajů, nýbrž nesou určitou odpovědnost také v souvislosti se zpracováním údajů společností SWIFT. Skutečnost, že se struktura řízení družstva SWIFT v průběhu času patrně vyvinula do stádia, kdy by se řízení SWIFT stalo nezávislejším než bylo původně zamýšleno, nebrání jeho zakladatelům, tj. finančním institucím, ponechat si své oprávnění jako správci údajů ve smyslu směrnice.

Na základě výše uvedeného má pracovní skupina za to, že stanovisko, že existuje společná odpovědnost finančních institucí a družstva SWIFT, v němž jsou zastoupeny, za zpracování osobních údajů prostřednictvím služby SWIFTNet FIN, je podpořeno dostatečnými skutečnostmi. Společná odpovědnost však nutně neznamená stejnou odpovědnost. Zatímco SWIFT nese hlavní odpovědnost za zpracování osobních údajů prostřednictvím služby SWIFTNet FIN, nesou finanční instituce jistou odpovědnost také za zpracování osobních údajů svých klientů touto službou.

---

[19] Součástí smluvní dokumentace je „Uživatelská příručka společnosti SWIFT“, která obsahuje standardizované typy zpráv, které je třeba používat.

[20] Kde je stanoveno: *„Aby se vyloučily všechny pochybnosti, nic z této politiky, nebo obecněji ze závazku důvěrnosti společnosti SWIFT vůči svým klientům, nelze vyložit jako bránění společnosti SWIFT v získávání, užívání nebo uveřejňování údajů o platebním styku nebo údajů zpráv, jak je důvodně nezbytné pro vyhovění úřední obsílce v dobré víře nebo jinému zákonnému postupu soudu nebo jiného příslušného orgánu.“* Srovnej stanovisko belgického orgánu pro ochranu údajů, D.2, poznámka pod čarou 8.

3.3 Úloha centrálních bank

Spoluodpovědnost centrálních bank je nutno prověřit s přihlédnutím k různým úlohám, které hrají v souvislosti se společností SWIFT a v souvislosti s dohledem v oblasti finančních plateb. SWIFT především podléhá společnému dohledu centrálních bank skupiny deseti zemí (dále jen „skupina G-10“)[21]. Dohled se zaměřuje v první řadě na ověření, že SWIFT má účinné kontroly a postupy pro řízení rizik, pokud jde o finanční stabilitu a řádnost finančních infrastruktur. Kromě toho „přezkoumávají dohlížitelé postup společnosti SWIFT při odhalování a zmírňování provozních rizik a mohou také posuzovat právní rizika, průhlednost opatření a politik klientských přístupů. Strategický směr společnosti SWIFT může být projednán také s Radou a vrcholovým vedením“[22]. Hlavním nástrojem dohledu nad společností SWIFT je vliv a tlak, který může uplatnit dohlížecí orgán („přátelská domluva“). Dohlížitelé mohou sestavit doporučení pro SWIFT; je však také zřejmé, že dohled centrálních bank na SWIFT nezaručuje SWIFTu žádné osvědčení, schválení nebo oprávnění.

Ustanovení o zachování důvěrnosti neveřejných informací jsou obsažena v memorandech o porozumění mezi společností SWIFT a centrálními bankami.

Skupina G-10 byla v průběhu roku 2002 informována o předávání údajů orgánům Spojených států amerických. Tato skupina však měla za to, že tato otázka spadá mimo rámec působnosti její úlohy dozoru. Mnohé centrální banky kromě toho považovaly memoranda o porozumění týkající se důvěrnosti za překážku předložení této otázky příslušným orgánům na vnitrostátní a evropské úrovni. Proto se skupina G-10 ani nezabývala důsledky týkajícími se ochrany údajů z převodů orgánům USA, ani neinformovala příslušné orgány, ani nevybídla SWIFT, aby tak učinila.

Mimoto prezident Evropské centrální banky (ECB) na veřejném jednání v Evropském parlamentu uvedl, že centrální banky skupiny G-10 „*nedaly společnosti SWIFT souhlas ohledně jejího vyhovění úředním obsílkám. Ve skutečnosti jsme žádné takové oprávnění dát nemohli, i kdybychom chtěli, protože to není v naší kompetenci. Proto je za svá rozhodnutí zodpovědná výhradně společnost SWIFT*“. [23]

Za druhé je nutno upozornit na to, že omezená úloha, kterou centrální banky v současné době hrají při dohledu nad společností SWIFT, nevylučuje, že také centrální banka může být pokládána – jako kterákoli jiná finanční instituce užívající službu SWIFTNet – za (společného) správce, kdykoli vystupuje jako klient společnosti SWIFT (viz. odstavec 3.2 výše), v případě, že zpracovává osobní údaje pro účel mezibankovních transakcí. V tomto ohledu skutečnost, že některé centrální banky byly informovány o předávání

---

[21] Skupinu G-10 tvoří Belgická národní banka, Kanadská banka, Deutsche Bundesbank (Německá spolková banka), Evropská centrální banka, Banque de France, Banca d' Italia, Japonská banka, De Nederlandsche Bank, Sveriges Riksbank, Švýcarská národní banka, Bank of England a Federal Reserve System (USA) zastoupená Federal Reserve Bank of New York a Board of Governors of the Federal Reserve System.

[22] Financial Stability Review 2005, uveřejněno Belgickou národní bankou a k dispozici na její webové stránce www.nbb.be.

[23] Jean-Claude Trichet: Prohlášení prezidenta ECB na veřejném slyšení v Evropském parlamentu o zachycování údajů o bankovních převodech ze systému SWIFT tajnými službami USA.

údajů orgánům USA, by mohla být považována za relevantní pro určení jejich odpovědnosti jako uživatelů systému SWIFT.

4. POSOUZENÍ SLUČITELNOSTI S PRAVIDLY OCHRANY ÚDAJŮ

4.1 Uplatnění zásad kvality údajů a proporcionality (článek 6 směrnice)

V souladu s článkem 6 směrnice musejí být osobní údaje zpracovávány korektně a zákonným způsobem;[24] musejí být shromažďovány pro stanovené účely, výslovně vyjádřené a legitimní[25] a nesmějí být zpracovávány pro účely neslučitelné s původně stanovenými účely, pro které byly shromažďovány. Kromě toho musí být zpracované údaje přiměřené, podstatné a nepřesahující míru s ohledem na účely, pro které jsou shromažďovány a/nebo dále zpracovávány.[26] Tato posledně zmiňovaná pravidla se společně označují jako „zásada proporcionality“. Konečně musí být přijata vhodná opatření, aby nepřesné nebo neúplné údaje byly vymazány nebo opraveny.[27]

4.1.1 Obchodní účel

Osobní údaje byly shromažďovány finančními institucemi pouze pro účel zpracovávání platebních příkazů klientů a následně společností SWIFT pro účel provádění služby SWIFTNet FIN (obchodní účel). Tento obchodní účel týkající se zpracování osobních údajů může být proto považován za jediný stanovený, výslovně vyjádřený a legitimní.

Co se týče předávání osobních údajů do třetích zemí, viz. oddíl 4.6 níže.

4.1.2 Další zpracování pro neslučitelné účely

aa) Osobní údaje se nesmí zpracovávat pro účely, které jsou neslučitelné s původně stanoveným účelem. Svým rozhodnutím zrcadlit všechna zpracování údajů v operačním středisku v USA se společnost SWIFT dostala do předvídatelné situace, kdy podléhá úředním obsílkám podle práva USA.

V tomto případě SWIFT obdržela úřední obsílky vystavené Ministerstvem financí USA k účelu údajného vyšetřování pro podezření z terorismu. Tento další účel se zcela liší od původně stanoveného účelu jemu příslušného zpracování osobních údajů a může mít přímé důsledky pro fyzické osoby, jejichž osobní údaje se zpracovávají. Tento další účel není slučitelný s původně stanoveným, ryze obchodním účelem, pro který byly osobní údaje shromažďovány.

---

[24] Čl. 6 odst. 1 písm. a) směrnice.

[25] Čl. 6 odst. 1 písm. b) směrnice.

[26] Čl. 6 odst. 1 písm. c) směrnice.

[27] Čl. 6 odst. 1 písm. d) směrnice.

SWIFT si byla vědoma tohoto dalšího účelu. Vedení společnosti SWIFT jej přijalo a spolupracovalo. SWIFT neupozornila na tento účel ani uživatele jejích služeb, ani orgán dozoru pro ochranu údajů.

bb) Bylo také zjištěno, že dochází k rozsáhlému předávání údajů společností SWIFT Ministerstvu financí USA bez účinné možnosti kontroly individualizovaného charakteru požadovaných údajů. Podle společnosti SWIFT by všechny finanční zprávy mohly být potenciálně prozkoumány Ministerstvem financí USA pomocí systému „černé skříňky". Tento systém umožňuje Ministerstvu financí USA vyhledávat z „černé skříňky" všechny zprávy – a v nich obsažené osobní údaje – které považuje za nutné.

Pracovní skupina zdůrazňuje, že i pro účely údajného vyšetřování pro podezření z terorismu by měly být společností SWIFT předávány pouze specifické a individualizované údaje případ od případu, v plném souladu se zásadami ochrany údajů. Protože tomu tak není, není současná praxe přiměřená, a proto porušuje čl. 6 odst. 1 písm. c) směrnice.

cc) Článek 13 stanoví, že „členské státy mohou přijmout legislativní opatření s cílem omezit rozsah povinností a práv uvedených v čl. 6 odst. 1 [jako zásada omezení účelu], v článku 10, v čl. 11 odst. 1 [povinnost informovat subjekt údajů], a v článcích 12 [právo na přístup] a 21 [zveřejnění zpracování], pokud toto omezení představuje opatření nezbytné pro zajištění [následující seznam důležitých veřejných zájmů] c) veřejné bezpečnosti, d) předcházení trestným činům a jejich vyšetřování, odhalování a stíhání [...]; f) kontrolní, inspekční nebo regulační funkce vyplývající, i pouze příležitostně, z výkonu veřejné moci v případech uvedených v písmenech c), d) a e);".

Evropský soudní dvůr do jisté míry vysvětlil výklad těchto ustanovení. Ve spojených věcech C-465/00, C-138/01 a C-139/01 („Rechnungshof") ze dne 20. května 2003 soud objasnil, že sdělování údajů shromažďovaných původně pro „hospodářské" účely třetím stranám, včetně orgánů veřejné moci, „zakládá zásah ve smyslu článku 8 Evropské úmluvy o ochraně lidských práv a základních svobod". Výjimky ze zásady omezení účelu stanovené ve směrnici o ochraně údajů musí kromě toho splňovat článek 13 uvedené směrnice a musí být tedy „opodstatněné z hlediska článku 8 úmluvy" (Rechnungshof, C-465/00, § 68 a násl.).

Aby byl zásah do práva na soukromí opodstatněný podle Úmluvy, musí být učiněn „v souladu s právními předpisy" a být „nezbytný v demokratické společnosti" pro účel veřejného zájmu. Štrasburská judikatura znovu připomněla, že zákon, kterým se stanoví zásah, „musí uvádět rozsah každé takové diskreční pravomoci příslušných orgánů a způsob jejího uplatňování dostatečně jasně, s ohledem na legitimní cíl dotčeného opatření, aby jednotlivci měli náležitou ochranu před svévolí."

Těchto ustanovení se však nelze dovolávat, protože SWIFT se v těchto otázkách neřídila belgickým právem.[28]

---

[28] Stanovisko belgického orgánu pro ochranu údajů, srovnej poznámku pod čarou 8.

dd) Pracovní skupina navíc poukazuje na existenci právních struktur na vládní úrovni. Pracovní skupina zdůrazňuje, že systémy by se měly používat v souladu se zásadou zachování bankovního tajemství. V tomto ohledu odkazuje na 40+9 doporučení Finančního akčního výboru (FATF/GAFI), mezivládního orgánu založeného v roce 1989, jehož účelem je vyvíjení a prosazování vnitrostátních a mezinárodních politik boje proti praní peněz a financování terorismu. Pracovní skupina také upozorňuje na systém výměny finančních informací zavedený mezi příslušnými vnitrostátními finančními zpravodajskými buňkami 96 zemí (Egmont Secure Web, ESW), koordinovaný sítí FinCEN ve Spojených státech amerických. V tomto rámci lze poskytovat finanční informace žádající straně v souladu s vnitrostátními pravidly země poskytující tyto informace.

Pracovní skupina odkazuje také na stávající mechanismy spolupráce zřízené nebo vyvinuté podle třetího pilíře (soudní a policejní spolupráce), a zejména podle mezinárodních dohod o vzájemné právní pomoci podepsaných dne 25. června 2003 mezi Spojenými státy americkými a Evropskou unií[29] a, i když vzdáleněji, mezinárodní dohody o vydávání. I když tyto smlouvy nejsou dosud ratifikované, podle článku 18 Vídeňské úmluvy o smluvním právu[30], stát je povinen zdržet se jednání, které by mohlo mařit předmět a účel smlouvy, jestliže podepsal smlouvu nebo vyměnil listiny tvořící smlouvu s výhradou ratifikace, dokud neoznámil úmysl, že se nehodlá stát její smluvní stranou.

V důsledku rozhodnutí zrcadlit všechna zpracovávání údajů v operačním středisku USA se SWIFT dostala do předvídatelné situace, kdy podléhá úředním obsílkám podle práva USA a způsob zpracování osobních údajů se jeví jako obcházející již stávající struktury a mezinárodní dohody.

Pracovní skupina má celkově za to, že zásady omezení účelu a slučitelnosti, proporcionality a nezbytnosti zpracovávaných osobních údajů nejsou dodržovány.

4.2 Oprávněnost (článek 7 směrnice)

Aby bylo každé zpracování osobních údajů zákonné, musí být oprávněné a musí splňovat jeden z důvodů stanovených v článku 7 směrnice.

4.2.1 Nezbytné pro splnění smlouvy (čl. 7 písm. b) směrnice)

SWIFT zpracovává osobní údaje obsažené ve zprávách prostřednictvím služby SWIFTNet Fin pouze za účelem provádění platebních příkazů svěřených společnosti SWIFT.

---

[29] „Dohoda o vydávání mezi Evropskou unií a Spojenými státy americkými“ a „Dohoda o vzájemné právní pomoci mezi Evropskou unií a Spojenými státy americkými“. http://eur-lex.europa.eu/LexUriServ/site/en/oj/2003/l_181/l_18120030719en00270033.pdf a http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_181/l_18120030719en00340042.pdf#search=%22Agreement%20on%20mutual%20legal%20assistance%20between%20the%20european%20union%22

[30] Vídeňská úmluva o smluvním právu ze dne 23. května 1969. Spojené státy americké podepsaly tuto úmluvu.

I kdyby však v této souvislosti mohlo být takové zpracování pro tento obchodní účel pokládáno za nezbytné pro plnění smlouvy mezi společností SWIFT a dotčenými finančními institucemi, není způsob jeho provedení zrcadlením osobních údajů v operačním středisku v USA přijatelný z jiných důvodů uvedených v bodě 4.6 níže.

4.2.2 Nezbytné pro splnění právní povinnosti, které podléhá správce (čl. 7 písm. c) směrnice)

Zpracování a zrcadlení by mohlo být nezbytné pro splnění právní povinnosti, které podléhá správce.

Společnost SWIFT se sídlem v Belgii se ohledně tohoto konkrétního zpracování formálně nedovolávala právního základu v rámci belgického nebo evropského práva. Pracovní skupina dále podotýká, že belgické nebo evropské právo neukládá právní povinnost ohledně tohoto konkrétního zpracování údajů. Pracovní skupina kromě toho již ve svém „stanovisku SOX“[31] konstatovala, že *„povinnost stanovenou zahraničním zákonem nebo nařízením (…) nelze označit za právní povinnost, která by opravňovala ke zpracování údajů v Evropské unii. Jakýkoli jiný výklad by usnadnil obcházení pravidel Evropské unie stanovených ve směrnici zahraničními pravidly“*. Pracovní skupina má za to, že toto zdůvodnění plně platí také v tomto případě.

Proto nelze v tomto případě použít čl. 7 písm. c) směrnice pro odůvodnění zpracování a zrcadlení osobních údajů.

4.2.3 Nezbytné pro uskutečnění oprávněného zájmu správce (čl. 7 písm. f) směrnice)

Podle čl. 7 písm. f) směrnice by zpracování a zrcadlení mohlo být nezbytné pro uskutečnění oprávněných zájmů správce nebo třetí osoby či osob, kterým jsou údaje sdělovány, za podmínky, že nepřevyšují zájem nebo základní práva a svobody subjektu údajů, které vyžadují ochranu podle čl. 1 odst. 1.

Otázkou je, zda by mohl být čl. 7 písm. f) směrnice použit k odůvodnění zpracování a zrcadlení, jehož důsledkem je to, že zpracování v operačním středisku ve Spojených státech amerických podléhají úředním obsílkám USA.

Nelze popřít, že společnost SWIFT má oprávněný zájem na tom, aby vyhověla úředním obsílkám podle práva USA. Pokud by SWIFT těmto úředním obsílkám nevyhověla, podstupuje riziko uložení sankcí podle práva USA. Na druhé straně je také velmi důležité, aby byla nalezena a zachována „správná rovnováha“ mezi rizikem společnosti SWIFT sankcionované Spojenými státy americkými za případné neuposlechnutí úředních obsílek a ochranou práv fyzických osob.

---

[31] Stanovisko 1/2006 k uplatňování pravidel Evropské unie pro ochranu údajů týkajících se interních systémů oznamování v oblastech účetnictví, interních účetních kontrol, revizních záležitostí, boje proti bankovní a finanční trestné činnosti.

Čl. 7 písm. f) směrnice požaduje, aby byla nastolena rovnováha mezi oprávněným zájmem, který sleduje zpracování osobních údajů, a základními právy subjektů údajů. Tato kritéria rovnováhy zájmu by měla brát v úvahu otázky proporcionality, subsidiarity, závažnosti údajných trestných činů, které lze oznamovat, a důsledků pro subjekty údajů. V souvislosti s rovnováhou kritéria zájmu bude nutno zavést také dostatečná ochranná opatření. Především článek 14 směrnice stanoví, že je-li zpracování údajů založeno na čl. 7 písm. f), mají fyzické osoby právo vznést kdykoli z vážných a legitimních důvodů námitku proti zpracování osobních údajů, které se ho týkají.

Společnost SWIFT prováděla zpracovávání a zrcadlení jejích údajů „skrytě, soustavně, rozsáhle a dlouhodobě“[32], aniž by specifikovala další neslučitelný účel v době zpracování údajů a aniž by upozornila na tento účel uživatele jejích služeb. Toto další zpracovávání a zrcadlení pro neslučitelný účel by mohlo mít dalekosáhlé důsledky pro každého jednotlivce.

Pracovní skupina se proto domnívá, že zájmy týkající se základních práv a svobod četných subjektů údajů přesahují zájem společnosti SWIFT na tom, aby nebyla Spojenými státy americkými sankcionována za případné neuposlechnutí úředních obsílek.

4.3 Poskytování jasných a úplných informací o systému (články 10 a 11 směrnice)

Podle článků 10 a 11 směrnice je správce povinen informovat subjekty údajů o existenci, účelu a fungování jeho zpracování údajů, příjemcích osobních údajů a právu na přístup, opravu a výmaz subjektem údajů. Všichni klienti finančních institucí, bez ohledu na jejich státní příslušnost a zemi bydliště, mají právo vědět, co se s jejich „důvěrnými“ údaji stane.

Pracovní skupina podotýká, že tyto informace týkající se zpracování a zrcadlení v operačním středisku USA nebyly poskytnuty ani společností SWIFT, ani dotčenými finančními institucemi.

Podle článku 13 směrnice mohou členské státy Evropské unie přijmout legislativní opatření s cílem omezit rozsah některých povinností a práv uvedených ve směrnici. Takové omezení musí představovat opatření nezbytné pro zajištění např. předcházení trestným činům a jejich vyšetřování, odhalování a stíhání nebo nedodržování deontologických pravidel pro regulovaná povolání případ od případu a jen tehdy, jestliže je takový zásah opodstatněný z hlediska článku 8 Úmluvy o ochraně lidských práv. Taková celková, dlouhotrvající a rozsáhlá činnost by však bez poskytovaných informací nebyla v souladu s článkem 13.

---

[32] Stanovisko belgického orgánu pro ochranu údajů, srovnej poznámku pod čarou 8.

4.4 Splnění požadavků na oznamování (články 18 až 20 směrnice)

Správci údajů musí splnit požadavky článků 18 až 20 směrnice o ochraně údajů, pokud jde o oznamování jejich zpracovávání údajů vnitrostátním orgánům pro ochranu údajů nebo o předběžnou kontrolu těmito orgány.

V členských státech umožňujících takový postup by zpracování mohla podléhat předběžné kontrole vnitrostátním orgánem pro ochranu údajů v rozsahu, v jakém tato zpracování pravděpodobně představují zvláštní riziko z hlediska práv a svobod subjektů údajů. Posouzení, zda se na tato zpracování vztahují požadavky na předběžnou kontrolu, závisí na vnitrostátních právních předpisech a na zavedené praxi vnitrostátního orgánu pro ochranu údajů.

Pracovní skupina podotýká, že společnost SWIFT sice oznámila některé druhy zpracování belgickému orgánu pro ochranu údajů[33], ale neoznámila zpracování a zrcadlení v operačním středisku USA pro provádění mezinárodních platebních příkazů, ani další účel.

4.5 Dohlížecí mechanismy

Zřízení orgánů dozoru pro ochranu údajů v členských státech EU vykonávajících zcela nezávisle své úkoly je základním prvkem ochrany osob v souvislosti se zpracováním osobních údajů. Tato zásada úplné nezávislosti orgánu dozoru je stanovena v článku 28 směrnice.

Pro nedostatek informací poskytnutých vnitrostátnímu orgánu dozoru pro ochranu údajů společností SWIFT, finančními institucemi a dohlížiteli nemohly být účinně použity stávající kontrolní mechanismy pro ochranu údajů uvedené ve směrnici. Pracovní skupina lituje, že společnost SWIFT nebo finanční instituce neiniciovaly v souvislosti se zpracováním a zrcadlením osobních údajů v operačním středisku USA předběžnou konzultaci, formální či neformální, s orgány pro ochranu údajů.

Z ověření vnitrostátními orgány vyplývá, že v souvislosti s předáváním údajů společností SWIFT Ministerstvu financí USA k dalšímu účelu sestávala kontrolní opatření zavedená společností SWIFT hlavně ze soukromých prověrek prováděných konzultační společností a z revizí prováděných zaměstnanci společnosti SWIFT („revizory“), kteří z bezpečnostních důvodů nesměli oznamovat podrobnosti o interním zjištění. Společnost SWIFT také uvedla, že na ni dohlíží vrcholový výbor zřízený centrálními bankami skupiny G-10 a že o této věci informovala dohlížitele.

I když kontrolní opatření zavedená společností SWIFT mohou přispět ke zvýšení bezpečnosti zpracování údajů, trvá pracovní skupina důrazně na tom, že žádný jiný mechanismus zajištěný správci údajů nemůže nahradit kontrolu zpracování údajů nezávislým orgánem dozoru veřejné moci požadovaným podle článku 28 směrnice. V každém případě se dohlížecí skupina zřízená centrálními bankami skupiny G-10 vyjádřila, že není příslušná pro zkoumání otázek týkajících se ochrany osobních údajů.

---

[33] Stanovisko belgického orgánu pro ochranu údajů, srovnej poznámku pod čarou 8.

Pracovní skupina proto odsuzuje skutečnost, že v souvislosti s osobními údaji zpracovávanými prostřednictvím služby SWIFTNet FIN byly stávající mechanismy pro nezávislou kontrolu zpracování osobních údajů orgány dozoru veřejné moci obcházeny.

4.6 Přeshraniční toky údajů (články 25 a 26 směrnice)

Články 25 a 26 směrnice se použijí, jsou-li osobní údaje předávány do třetí země. Každé předání údajů vytvořených na území Evropské unie, které mají být použity mimo území Evropské unie, musí podléhat odpovídajícímu hodnocení podle směrnice. Ustanovení směrnice týkající se předávání osobních údajů do třetích zemí nelze kromě toho používat odděleně od ostatních ustanovení směrnice. Jak je výslovně uvedeno v čl. 25 odst. 1, použijí se tato ustanovení, „aniž by tím bylo dotčeno dodržování vnitrostátních předpisů přijatých na základě ostatních ustanovení této směrnice“. To znamená, že je nutno dodržovat další příslušná ustanovení směrnice bez ohledu na ustanovení týkající se účelu předání údajů do třetí země[34].

K běžné činnosti služby SWIFTNet FIN patří plynulý a rozsáhlý přeshraniční tok údajů v důsledku umístění operačních středisek společnosti SWIFT. Operační střediska společnosti SWIFT nejsou samostatné právní subjekty, nýbrž pobočky („*succursales*“) družstevní společnosti založené podle belgického práva. Režim ukládání a odesílání zpráv („store and forward“) těchto dvou operačních středisek společnosti SWIFT v Evropě a v USA je následující: zprávy jsou automaticky dekódovány v operačních střediscích pro uložení a přenos informací během několika milisekund. Tento režim „ukládání a odesílání“ je určen k ověření (kontrole správnosti nebo zda jsou uvedena písmena/čísla v polích povinných zpráv) informací (například ověření, že je uveden správný měnový kód převodu, např. „EUR“) na základě obsahu, který je standardizovaný. Během tohoto postupu jsou informace po dobu 124 dní rovněž uchovávány v obou operačních střediscích z bezpečnostních důvodů (záložní kopie), které pak působí jako dokonalý „zrcadlový obraz“. Tím je zajištěno, že ukládání údajů je paralelní a údaje jsou identické.

Pro oprávněné zpracování a zrcadlení osobních údajů ve Spojených státech amerických společností SWIFT musí být tyto údaje z Evropské unie nejprve předány podle belgických právních předpisů přijatých v souladu se směrnicí o předávání osobních údajů do třetích zemí, zejména s články 25 a 26. Předávání společností SWIFT do Spojených států amerických proto musí být posuzováno s přihlédnutím ke dvěma aspektům: jednak k obchodnímu zpracování a zrcadlení osobních údajů belgickou společností SWIFT do jejího operačního střediska ve Spojených státech amerických, jednak ke zpracování údajů Ministerstvem financí USA pro další účel schválený společností SWIFT.

4.6.1 Odpovídající ochrana údajů (čl. 25 odst. 1 směrnice)

Podle čl. 25 odst. 2 směrnice se odpovídající úroveň ochrany poskytovaná třetí zemí „posoudí s ohledem na všechny okolnosti související s předáním nebo předáváním údajů; zejména se přihlédne k povaze údajů, účelu a trvání předpokládaného či předpokládaných zpracování, zemi původu a zemi konečného určení, právním

[34] Pracovní skupina zřízená podle článku 29: Pracovní dokument o společném výkladu čl. 26 odst. 1 směrnice 95/46/ES ze dne 24. října 1995. WP 114.

předpisům, obecným nebo zvláštním, platným v dotčené třetí zemi, jakož i profesním pravidlům a bezpečnostním opatřením, která jsou ve třetí zemi dodržována.“

S ohledem na výše uvedená kritéria a uplatňování zásad stanovených v pracovním dokumentu WP12[35] pracovní skupina konstatuje, že ve Spojených státech amerických v současné době pouze systém „bezpečného přístavu“ zajišťuje odpovídající úroveň ochrany pro předávání údajů z Evropské unie do organizací Spojených států amerických, které se k tomuto systému připojily. Nevztahuje se to však na finanční služby[36].

Proto by se společnost SWIFT, jako belgická právnická osoba, nemohla odvolávat na článek 25 směrnice, pokud jde o zpracování a zrcadlení v operačním středisku v USA.

4.6.2 Dostatečná ochranná opatření zavedená příjemcem (čl. 26 odst. 2 směrnice)

Podle čl. 26 odst. 2 směrnice může členský stát povolit také předání nebo předávání osobních údajů do třetí země, která nezajišťuje odpovídající úroveň ochrany, pokud správce poskytne „*dostatečná ochranná opatření pro ochranu soukromí a základních práv a svobod osob, jakož i pro výkon odpovídajících práv“*. Na konci čl. 26 odst. 2 je také stanoveno, že tato ochranná opatření „*mohou zejména vyplývat z vhodných smluvních doložek“*. Pro usnadnění používání smluvních doložek přijala Evropská komise tři rozhodnutí o standardních smluvních doložkách, z nichž dvě upravují předávání od jednoho správce údajů druhému, zatímco třetí upravuje předávání od správce údajů zpracovateli údajů[37]. Kromě toho, nehledě na možnost používání smluvních doložek k zajištění těchto dostatečných ochranných opatření, pracuje pracovní skupina zřízená podle článku 29 od roku 2003 aktivně na možnosti nadnárodních skupin s použitím „závazných pravidel pro společnosti“ ke stejnému účelu[38].

V tomto případě však společnost SWIFT těchto možností pro své zpracování a zrcadlení v operačním středisku Spojených států amerických nevyužila[39].

---

[35] „Předávání osobních údajů do třetích zemí: Uplatnění článků 25 a 26 směrnice Evropské unie o ochraně údajů“ schválené pracovní skupinou dne 24. července 1998; http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_en.pdf.

[36] srovnej http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

[37] Co se týče předávání od jednoho správce údajů druhému, přijala Komise první soubor standardních smluvních doložek dne 15. června 2001; následně toto rozhodnutí změnila a připojila nový soubor alternativních doložek (rozhodnutí ze dne 27. prosince 2004). V souvislosti s předáváním od správce údajů zpracovateli údajů přijala Komise dne 27. prosince 2001 soubor standardních smluvních doložek. Všechny tyto doložky jsou k dispozici na této webové stránce: http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm.

[38] Srovnej pracovní dokument WP 74, „Předávání osobních údajů do třetích zemí: Uplatnění čl. 26 odst. 2 směrnice EU o ochraně údajů na závazná pravidla pro společnosti pro mezinárodní předávání údajů“ schválené pracovní skupinou dne 3. června 2003 a dalších doplňkových dokumentů WP107 a WP108.

[39] Kdyby společnost SWIFT těchto možností využila, připomíná pracovní skupina zřízená podle článku 29, že pokud jde o další předávání údajů, nesmí výjimky z platných právních předpisů pro ochranu údajů v žádném případě přesahovat omezení nutná v demokratické společnosti.

4.6.3 Výjimky (článek 26 směrnice)

Čl. 26 odst.1 směrnice uvádí, že předání nebo předávání osobních údajů do třetí země, která nezajišťuje odpovídající úroveň ochrany, může být provedeno tehdy, je-li splněna jedna z podmínek uvedených v písmenech a) až f). Jak pracovní skupina uvedla dříve ve svém pracovním dokumentu WP12[40] uvedeném výše, musí být výklad čl. 26 odst. 1 nezbytně striktní.

Pracovní skupina v tomto ohledu zdůrazňuje, že tato logika je stejná jako u dodatkového protokolu k úmluvě Rady Evropy č. 108. Zpráva o tomto protokolu uvádí, že „strany mají pravomoc stanovit výjimky ze zásady odpovídající úrovně ochrany. Příslušné vnitrostátní právní předpisy musí přesto respektovat zásadu obsaženou v evropském právu, aby doložky o výjimkách byly vykládány restriktivně, aby se výjimka nestala pravidlem.“.[41]

Možné výjimky v tomto případě jsou tyto:

4.6.3.1 Souhlas subjektu údajů (čl. 26 odst. 1 písm. a) směrnice)

Aby byla tato výjimka uplatněna oprávněně, musí subjekt údajů udělit svůj jednoznačný souhlas s předpokládaným předáním. Jak již bylo uvedeno v dřívějším pracovním dokumentu pracovní skupiny WP 12, musí být tento souhlas, ať jsou okolnosti, za nichž je dán, jakékoli, svobodným, výslovným a vědomým projevem vůle subjektu údajů, jak stanoví čl. 2 písm. h) směrnice.[42] Subjekt údajů musí být informován o předání do třetí země, která nezajišťuje odpovídající úroveň ochrany nebo nezavedla vhodná ochranná opatření, a potom se může rozhodnout, zda podstoupí související riziko nebo ne.

Společnost SWIFT neobdržela jasný souhlas subjektů údajů ke zpracování a zrcadlení v operačním středisku Spojených států amerických, a proto se nemůže odvolávat na čl. 26 odst. 1 písm. a) směrnice.

4.6.3.2 Předání je nezbytné pro splnění smlouvy mezi subjektem údajů a správcem nebo pro splnění předsmluvních opatření přijatých na žádost subjektu údajů (čl. 26 odst. 1 písm. b) směrnice)

Tato výjimka znamená, že předané údaje musí být opravdu nezbytné k účelu provádění této smlouvy nebo těchto předsmluvních opatření. Z tohoto důvodu dochází pracovní skupina k závěru, že tato podmínka nemohla být uplatněna na předání údajů společností SWIFT do operačního střediska Spojených států amerických, protože společnost SWIFT nemá přímý smluvní vztah s fyzickou osobou. Tato výjimka nemůže být uplatněna ani na předání dalších informací, které nejsou nezbytné pro účel předání, nebo předávání pro účel jiný než provádění smlouvy. Obecněji řečeno, umožňují výjimky z čl. 26 odst. 1

---

[40] Srovnej poznámku pod čarou 35 výše.

[41] Srovnej zprávu o dodatkovém protokolu k úmluvě č. 108 o kontrolních orgánech a přeshraničních tocích údajů, čl. 2 odst. 2 písm. a); tento dokument je přístupný na webové stránce:

http://conventions.coe.int/Treaty/EN/Reports/Html/181.htm

[42] Pracovní skupina zřízená podle článku 29: Pracovní dokument o společném výkladu čl. 26 odst. 1 směrnice 95/46/ES ze dne 24. října 1995. WP 114.

písmen b) až e) jen to, že se údaje nezbytné pro účel předání smí předávat jen na základě jednotlivých výjimek; co se týče dalších údajů, měla by být splněna další opatření dokládající odpovídající úroveň.

4.6.3.3 Předání je nezbytné pro uzavření nebo plnění smlouvy, která byla uzavřena nebo která má být uzavřena v zájmu subjektu údajů mezi správcem a třetí osobou (čl. 26 odst. 1 písm. c) směrnice)

Rovněž výjimka uvedená v čl. 26 odst. 1 písm. b), předání údajů do třetí země, která nezajišťuje odpovídající ochranu, nemůže být považována za spadající do výjimek obsažených v čl. 26 odst. 1 písm. c), pokud ji nelze pokládat za opravdu „nezbytnou pro uzavření nebo plnění smlouvy mezi správcem údajů a třetí osobou v zájmu subjektu údajů" a za splňující příslušné „kritérium nezbytnosti". Toto kritérium vyžaduje úzkou a skutečnou souvislost mezi zájmem subjektu a účely smlouvy.[43]

Pracovní skupina dochází k závěru, že se tato podmínka nesmí vztahovat na předávání údajů společností SWIFT do operačního střediska Spojených států amerických.

4.6.3.4 Předání je nezbytné nebo se stává právně závazným pro zachování důležitého veřejného zájmu nebo pro zjištění, výkon nebo obranu právních nároků před soudem (čl. 26 odst. 1 písm. d) směrnice)

Společnost SWIFT uvedla, že zrcadlení zpracování údajů do operačních středisek je považováno za rozhodující prvek v globálním finančním systému, že toto zrcadlení zpracování bylo navrženo dohlížiteli (centrálními bankami skupiny G-10) z bezpečnostních důvodů a že infrastruktura společnosti SWIFT bude považována za rozhodující pro globální finanční sektor. SWIFT se hájí tím, že tento důvod by opodstatňoval předávání na základě čl. 26 odst. 1 písm. d) směrnice.

Pracovní skupina nemůže s tímto výkladem souhlasit. I kdyby bylo zjištěno, že mezinárodní zrcadlení zpracování (v jiném světadílu než v Evropě) je „nezbytné nebo se stalo právně závazným pro zachování důležitého veřejného zájmu" ve smyslu čl. 26 odst. 1 písm. d) směrnice, je stále možné zrcadlit takové zpracování mimo rámec EU nebo EHP v zemi, která by poskytovala odpovídající úroveň ochrany. Pracovní skupina poukazuje na země jako Argentina[44] nebo Kanada[45], na které se podle rozhodnutí Evropské komise nahlíží tak, že splňují požadavky směrnice. „Zrcadlení" v zemi, která není členem Evropské unie a nemá odpovídající úroveň ochrany údajů, nebylo nezbytné a nemůže být opodstatněno čl. 26 odst. 1 písm. d).

Osobní údaje shromažďované a zpracovávané prostřednictvím sítě SWIFT pro mezinárodní peněžní převody pomocí BIC kódu nebo SWIFT kódu a zrcadlené v USA byly kromě toho poskytovány Ministerstvu financí USA od konce roku 2001 na základě úředních obsílek podle práva USA.

---

[43] Pracovní skupina zřízená podle článku 29: Pracovní dokument o společném výkladu čl. 26 odst. 1 směrnice 95/46/ES ze dne 24. října 1995. WP 114

[44] Rozhodnutí Komise C(2003) 173 ze dne 30. června 2003; Úř. věst. L 168, 5.7.2003.

[45] Rozhodnutí Komise 2002/2/ES ze dne 20.12.2001 o odpovídající ochraně osobních údajů, kterou poskytuje kanadský zákon o ochraně osobních informací a elektronických dokumentech; Úř. věst. L 2/13 ze dne 4.1.2002.

Plná sledovatelnost převodů finančních prostředků může být obzvláště důležitým a cenným nástrojem při předcházení, vyšetřování, odhalování a stíhání praní peněz a financování terorismu a podléhá ustanovením podle práva Evropské unie[46].

Pracovní skupina uznává, že boj proti terorismu představuje legitimní účel demokratických společností v zájmu bezpečnosti státu a že za tímto účelem lze přijmout opatření, která zasahují do základního práva na ochranu osobních údajů. Pracovní skupina si je v této souvislosti plně vědoma svého závazku. Má také za to, že mezinárodní nástroje skutečně poskytují vhodný právní rámec umožňující mezinárodní spolupráci. Za tímto účelem zastává pracovní skupina stanovisko, že by měly být využity možnosti, které současné formy mezinárodní spolupráce již k boji proti terorismu a vyšetřování pro podezření z terorismu nabízejí, při zajištění požadované úrovně ochrany základních práv.

Pracovní skupina však podotýká, že nelze použít ani čl. 26 odst. 1 písm. d) směrnice, protože předávání není nezbytné ani se nestává právně závazným pro zachování důležitého veřejného zájmu členského státu EU (Belgie). Autoři směrnice v této věci nepochybně opravdu předpokládali, že v této souvislosti platí pouze důležité veřejné zájmy stanovené vnitrostátními právními předpisy platnými pro správce údajů se sídlem v Evropské unii. Každý jiný výklad by zahraničnímu orgánu usnadnil obcházení požadavku odpovídající ochrany v zemi příjemce stanoveného ve směrnici.

4.6.3.5 Předání je nezbytné pro ochranu životně důležitých zájmů subjektu údajů (čl. 26 odst. 1 písm. e) směrnice)

Tato výjimka se vztahuje na předání, které se musí týkat osobního zájmu subjektu údajů, a souvisí-li se zdravotními údaji, musí být nezbytné pro základní diagnózu. Tato výjimka by se tedy neměla používat k tomu, aby opodstatnila předání osobních lékařských údajů pro účel jako je obecný lékařský výzkum.[47]

Společnost SWIFT netvrdila, že předání je nezbytné pro ochranu životně důležitých zájmů subjektů údajů k účelu zpracování a zrcadlení v operačním středisku USA. Pracovní skupina se domnívá, že tato výjimka zde není v žádném případě na místě. Nelze se odvolávat na čl. 26 odst. 1 písm. e) směrnice.

4.6.4 Zjištění

Společnost SWIFT se mohla odvolávat na čl. 26 odst. 2 směrnice ohledně zákonného předávání osobních údajů do svého operačního střediska v USA. Společnost SWIFT se však rozhodla předávat osobní údaje, aniž by splňovala zákonné požadavky belgických právních předpisů na tato mezinárodní předávání údajů.

Společnost SWIFT se nemůže odvolávat na žádnou z ostatních výjimek uvedených v článku 26 směrnice.

---

[46] Např. nařízení Evropského parlamentu a Rady o informacích o plátci podávaných v souvislosti s převodem finančních prostředků přijaté dne 8. listopadu 2006, dosud nezveřejněné; původní návrh Komise KOM (2005) 343.

[47] Pracovní dokument o společném výkladu čl. 26 odst. 1 směrnice 95/46/ES ze dne 24. října 1995; http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_en.pdf.

Co se týče zpracování a zrcadlení v USA, nebylo prováděno legálně ani zpracování a zrcadlení pro obchodní účely. Pokračující zpracovávání a zrcadlení, uvážíme-li jeho další neslučitelný účel a velký rozsah, přesahuje míru toho, co je nezbytné v demokratické společnosti a dále brání společnosti SWIFT předávat osobní údaje do Spojených států amerických.

5. ZÁVĚRY:

Z těchto důvodů zastává pracovní skupina toto stanovisko:

5.1 Směrnice Evropské unie o ochraně údajů 95/46/ES se vztahuje na výměnu osobních údajů prostřednictvím služby SWIFTNet FIN;

5.2 S ohledem na směrnici nesou společnost SWIFT a finanční instituce společnou odpovědnost za zpracování osobních údajů prostřednictvím služby SWIFTNet FIN, přičemž SWIFT nese hlavní odpovědnost a finanční instituce nesou určitou odpovědnost za zpracování osobních údajů jejich klientů.

5.3 Společnost SWIFT a finanční instituce v Evropské unii nedodržely ustanovení směrnice:

5.3.1 *SWIFT*: Pokud jde o zpracování a zrcadlení osobních údajů v rámci služby SWIFTNet FIN, musí společnost SWIFT jako správce údajů dodržovat své povinnosti podle směrnice, k nimž patří povinnost poskytovat informace, požadavek oznamovat zpracování, povinnost zajistit odpovídající úroveň ochrany za účelem splněné požadavků na mezinárodní předávání osobních údajů;

5.3.2 *Finanční instituce*: Finanční instituce v Evropské unii mají jako správci údajů právní povinnost ujistit se, že společnost SWIFT plně dodržuje právní předpisy, zejména právní předpisy pro ochranu údajů, aby byla zajištěna ochrana jejich klientů. Finanční instituce odpovídají za to, že mají dostatečné znalosti o různých platebních systémech a jejich technických a právních znacích a rizicích. Pokud by finanční instituce (dostatečně) neusilovaly o dosažení takových znalostí, podstoupily by značná právní rizika a rizika pro klienty v důsledku nedodržení základní povinné péče. Zejména zahrnují-li některé služby, jako služba SWIFTNet FIN, rozsáhlé předávání do zemí nezajišťujících odpovídající ochranu údajů s ohledem na směrnici nebo je-li pravděpodobné, že by tato předávání vyvolala určité obavy nebo rizika týkající se soukromí, má pracovní skupina za to, že je nezbytné, aby jednotliví klienti finančních institucí byli informováni finančními institucemi jako poskytovateli profesionálních služeb v souladu s požadavky směrnice týkajícími se průhlednosti.

5.4 Pracovní skupina zastává stanovisko, že nedostatek průhlednosti a odpovídajících a účinných kontrolních mechanismů souvisejících s celým procesem předání osobních údajů nejdříve do USA a potom na Ministerstvo financí USA představuje vážné porušení s ohledem na směrnici. Kromě toho

jsou porušeny záruky na předání údajů do třetí země stanovené směrnicí a zásady proporcionality a nezbytnosti.

Co se týče sdělování osobních údajů Ministerstvu financí USA má pracovní skupina za to, že skryté, soustavné, rozsáhlé a dlouhodobé předávání osobních údajů společností SWIFT Ministerstvu financí USA již léta důvěrným, neprůhledným a soustavným způsobem bez existujícího právního základu a bez možnosti nezávislé kontroly veřejnými orgány dozoru pro ochranu údajů zakládá porušení základních evropských zásad týkajících se ochrany údajů a není v souladu s belgickým a evropským právem. Stávající mezinárodní rámec je již k dispozici v souvislosti s bojem proti terorismu. Možnosti v něm nabízené by měly být využity při zajišťování požadované úrovně ochrany základních práv.

5.5 Pracovní skupina znovu připomíná[48] závazek demokratických společností zajistit dodržování základních práv a svobod osob. Právo osoby na ochranu osobních údajů je součástí těchto základních práv a svobod[49]. Směrnice Společenství o ochraně osobních údajů (směrnice 95/46/ES a 2002/58/ES) jsou součástí tohoto závazku[50]. Cílem těchto směrnic je zajistit dodržování základních práv a svobod, zejména práva na soukromí v souvislosti se zpracováváním osobních údajů, a přispívat k dodržování práv, která jsou chráněna článkem 8 Evropské úmluvy o ochraně lidských práv a článkem 8 Listiny základních práv Evropské unie. Ve všech těchto nástrojích jsou stanoveny výjimky pro boj proti trestné činnosti, které však musí respektovat zvláštní podmínky.

6. OPATŘENÍ, KTERÉ JE TŘEBA BEZODKLADNĚ PŘIJMOUT PRO ZLEPŠENÍ SOUČASNÉHO STAVU:

S ohledem na výše uvedené skutečnosti vyzývá tedy pracovní skupina k bezodkladnému přijetí těchto opatření za účelem zlepšení současného stavu:

6.1 **Ukončení protiprávního jednání:** Společnost SWIFT a finanční instituce splní své právní povinnosti podle vnitrostátních a evropských právních předpisů. To zahrnuje přijetí opatření pro zajištění, aby veškerá předání byla v souladu s právními předpisy. V případě nesouladu mohou správci údajů očekávat, že budou příslušnými orgány sankcionováni podle směrnice a vnitrostátních právních předpisů pro vynucení tohoto souladu.

6.2 **Obnova zákonnosti zpracování:** Pracovní skupina zřízená podle článku 29 vyzývá SWIFT a finanční instituce, aby neprodleně přijaly opatření za účelem napravení současného protiprávního stavu, a obnovily stav, kdy lze provádět mezinárodní peněžní převody v plném souladu s právními předpisy

---

[48] Článek 29: Stanovisko 10/2001 k nutnosti vyváženého přístupu v boji proti terorismu; http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2001_en.htm .

[49] Viz. zejména článek 8 Listiny základních práv Evropské unie, jakož i judikaturu Evropského soudu pro lidská práva ve věci „Aman“ ze dne 16. února 2000 a „Rotaru“ ze dne 4. května 2000.

[50] Viz. body 1, 2, 10 a 11 směrnice 95/46/ES.

pro ochranu údajů. Pracovní skupina vítá skutečnost, že některé orgány pro ochranu údajů již naléhají na finanční instituce, aby bezodkladně nalezly řešení.

6.3 **Opatření týkající se společnosti SWIFT:** Pro veškerá svá zpracování údajů musí společnost SWIFT jako správce přijmout opatření nezbytná pro splnění jejích povinností podle belgických právních předpisů pro ochranu údajů, kterými se provádí směrnice.

6.4 **Opatření týkající se centrálních bank:** Současný stav vyžaduje vyjasnění dohledu nad společností SWIFT. Pracovní skupina doporučuje nalézt vhodná řešení pro nastolení souladu zejména s pravidly ochrany údajů nepochybně spadajícími do oblasti působnosti dohledu, aniž by byly dotčeny pravomoci vnitrostátních orgánů dozoru pro ochranu údajů, jakož i pro zajištění, že příslušné orgány budou v případě potřeby řádně a včas informovány. Pracovní skupina se domnívá, že nedostatečný soulad s právními předpisy pro ochranu údajů může skutečně poškodit důvěru klientů v jejich banky a ovlivnit tak i finanční stabilitu platebního systému (ohrožení dobré pověsti). V případě možného porušení ústavních nebo lidských práv by nemělo být možné se odvolávat na právní překážky, jako je povinnost dohlížitelů zachovávat služební tajemství, které by mohly být použity jako argument pro omezení účinné kontroly nezávislými orgány pro ochranu údajů.

6.5 **Opatření týkající se finančních institucí:** Všechny finanční instituce v Evropské unii využívající službu SWIFTNet Fin, včetně centrálních bank, musí zajistit, aby podle článků 10 a 11 směrnice EU 95/46/ES byli jejich klienti řádně informováni o tom, jak jsou jejich osobní údaje zpracovávány a jaká práva subjekty údajů mají. Musí také poskytovat informace o skutečnosti, že k těmto údajům mohou mít přístup orgány Spojených států amerických. Orgány dozoru pro ochranu údajů budou tyto požadavky vynucovat za účelem jejich splnění všemi finančními institucemi na evropské úrovni a budou spolupracovat na harmonizovaných informačních oznámeních. V této souvislosti připomíná pracovní skupina zřízená podle článku 29 své stanovisko přijaté k harmonizovaným ustanovením o přístupu k informacím[51]. Zdá se také vhodné, aby finanční instituce a centrální banky zvážily alternativní technická řešení postupů užívaných v současné době v souladu se zásadami směrnice.

Pracovní skupina zdůrazňuje také toto:

6.6 **Zachování našich základních hodnot v boji proti trestné činností:** pracovní skupina připomíná, že žádná opatření přijatá v boji proti trestné činnosti a terorismu by neměla a nesmí snížit úroveň ochrany základních práv, kterou se vyznačují demokratické společnosti. Klíčovým prvkem boje proti terorismu je zajištění zachování základních práv, která jsou základem

---

[51] Pracovní skupina zřízená podle článku 29 „Stanovisko k harmonizovanějším ustanovením o přístupu k informacím“, ze dne 25. listopadu 2004. WP 100; http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_en.pdf.

demokratických společností a právě těmi hodnotami, o jejichž zničení usilují ti, kdo obhajují použití násilí.

6.7 **Zásady globální ochrany údajů:** Pracovní skupina považuje za nezbytné, aby zásady ochrany osobních údajů, včetně kontroly nezávislými orgány dozoru, byly plně respektovány v kterémkoli rámci globálních systémů výměny informací.

Pracovní skupina zřízená podle článku 29 bude sledovat a monitorovat výše uvedené.

V Bruselu dne 22. listopadu 2006

Za pracovní skupinu
předseda
Peter Schaar

Pracovní skupina zřízená podle článku 29

01609/06/CS
WP 125

Pracovní dokument o ochraně údajů a důsledcích iniciativy eCall na ochranu soukromí

Přijatý dne

26. září 2006

Tato pracovní skupina byla zřízena podle článku 29 směrnice 95/46/ES. Jde o nezávislý evropský poradenský orgán pro ochranu údajů a soukromí. Jeho úlohy jsou stanoveny v článku 30 směrnice 95/46/ES a článku 15 směrnice 2002/58/ES.

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

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

PRACOVNÍ SKUPINA PRO OCHRANU FYZICKÝCH OSOB V SOUVISLOSTI SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ
zřízená směrnicí Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995[1],

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

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

PŘIJALA TENTO PRACOVNÍ DOKUMENT:

1. ÚVOD

Cílem tohoto pracovního dokumentu je poukázat na otázky ohledně ochrany údajů a soukromí, které vyvstávají ve spojení s plánovaným zavedením harmonizované celoevropské služby tísňového volání z palubního systému vozidla („služba eCall"), která je založena na jednotném evropském čísle tísňového volání 112[2].
Jednou z iniciativ Evropské komise bylo zřízení fóra eSafety, společné veřejno-průmyslové iniciativy zaměřené na zvyšování silniční bezpečnosti využitím vyspělých informačních a komunikačních technologií. Služba eCall byla označena jako jedna z nejvyšších priorit a byla zřízena řídící skupina pro eCall složená ze zástupců všech zainteresovaných subjektů[3]. Řídící skupina pro eCall vypracovala doporučení zahrnující plán na zavedení služby eCall ve všech členských státech a na její zavedení jako standardní možnost do všech nových vozidel od 1 září 2010[4].

Řídící skupina pro eCall vydala memorandum o porozumění týkající se provádění služby eCall. Cílem tohoto memoranda je zajistit, aby služba eCall fungovala ve všech členských státech EU. Zavazuje zainteresované subjekty, aby systém eCall zaváděly společně na základě společně schváleného plánu a specifikace rozhraní, včetně minimálního souboru údajů (MSD). Memorandum podepsali v srpnu 2004 Evropská komise, za automobilový průmysl Asociace evropských výrobců automobilů (ACEA) a víceodvětvové partnerské uskupení ERTICO. V současnosti obsahuje přes 60 podpisů, včetně podpisu sedmi členských států EU[5], Švýcarska a Norska.

Nedávno schválil Evropský parlament velkou většinou rezoluci na podporu zavádění služby eCall[6], kterou vyzývá členské státy k podpisu memoranda.

Pracovní skupina zřízená podle článku 29 si je vědoma sociálně-hospodářského přínosu, který občanům může přinést všeobecné zavedení služby eCall, nicméně toto zavedení bude mít důsledky na ochranu soukromí a údajů, což je třeba zdůraznit a přiměřeně se tím zabývat.

---

1 Úř. věst. L 281, 23.11.1995, s. 31, dostupné na: http://ec.europa.eu/justice_home/fsj/privacy/

2 Sdělení Komise: druhé sdělení o e-bezpečnosti: Zpřístupnění systému eCall občanům (KOM(2005) 431, dostupné na této internetové stránce: http://europa.eu/information_society/activities/esafety/index_en.html

3 Sdělení Komise: Informační a komunikační technologie pro bezpečná a inteligentní vozidla, KOM(2003) 542 v konečném znění, 15.9.2003.

4 Doporučení řídící skupiny eCall včetně všech příloh lze nalézt na internetové adrese: http://www.esafetysupport.org/en/ecall_toolbox/driving_group_ecall.

5 Finsko, Švédsko, Řecko, Itálie, Litva, Slovinsko a Kypr.

6 Zpráva o bezpečnosti silničního provozu: Zpřístupnění systému eCall občanům. Zpravodaj: Gary Titley (A6-0072/2006)

Pracovní skupina zřízená podle článku 29 proto považuje za nutné, s ohledem na úkoly, které ji byly svěřeny čl. 30 odst. 1 písm. a) směrnice na ochranu údajů, a s cílem reagovat na otázky spojené s ochranou soukromí a údajů, které vyvstávají v souvislosti s předpokládaným zavedením služby eCall, analyzovat stávající situaci a této problematice věnuje tento pracovní dokument.

2. PRINCIP SLUZBY ECALL

Navrhovaná struktura služby eCall je založena na kvazi-souběžném hlasovém a datovém přenosu z generátoru eCall na nejbližší centrum tísňového volání („PSAP“). Úlohu centra tísňového volání bude plnit orgán veřejné správy anebo soukromý poskytovatel služby pod dohledem orgánu veřejné správy.

Tísňové volání vyšle v případě nehody generátor eCall automaticky pomocí senzorů umístěných ve vozidle (nebo jej spustí manuálně cestující ve vozidle) a přenese je do příslušného PSAP.

Tísňové volání sestává ze dvou prvků: z čistě hlasového (audio) telefonního hovoru na číslo 112 a z minimálního souboru údajů (MSD). Tísňové volání (údaje+hlas) se přenáší přes mobilní síť a operátor mobilní sítě (MNO) je zaregistruje jako tísňové volání na číslo 112. Na základě postupu při volání na číslo 112 přidá operátor mobilní sítě k volání identifikaci volající linky (CLI) a v souladu se směrnicí o univerzální službě[7] a doporučením E112[8] co nejpřesnější určení polohy.

Po tomto postupu předá telekomunikační operátor hlasový záznam spolu s CLI, co nejpřesnější informací o poloze a minimálním souborem údajů o tísňovém volání příslušnému centru pro tísňové volání. Centrum tísňového volání poté vyšle generátoru eCall zprávu, v které upřesní, že minimální soubor údajů byl správně přijat.

Je důležité zdůraznit, že u navrhované služby eCall nebude palubní systém sledován žádnou třetí stranou trvale, jelikož nebude trvale napojen na mobilní komunikační sítě, ale pouze tehdy, bude-li aktivován v případě nehody anebo spuštěn manuálně cestujícími ve vozidle.

Minimální soubor údajů (MSD)[9] sestává z údajů o i) čase nehody, ii) přesném určení polohy včetně směru jízdy, iii) identifikaci vozidla, iv) klasifikaci eCall vážnosti nehody (minimálně informace, zda bylo tísňové volání uskutečněno manuálně anebo automaticky), v) případném poskytovateli služby.

---

[7] Směrnice Evropského parlamentu a Rady 2002/22/ES ze dne 7. března 2002 o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací. Úř. věst. L 108, 24.4.2002, s. 51

[8] Doporučení Komise 2003/558/ES ze dne 25. července 2003 o zpracovávání informací o místě volajícího v elektronických komunikačních sítích pro účely rozšíření místních služeb tísňového volání. Úř. věst. L 189, s. 49

[9] Viz popis minimálního souboru údajů v závěrečných doporučeních řídící skupiny pro eCall, oddíl 4.2.2.4.

O zařazení nepovinných údajů týkajících se stavu nehody, které bylo původně plánováno v rámci minimálního souboru údajů, probíhá zatím diskuze. Tyto nepovinné údaje (např. typ paliva používaného ve vozidle) by měly být slučitelné s právními předpisy na ochranu údajů. Zejména by měly být slučitelné se zásadou proporcionality. Měly by obsahovat pouze údaje nezbytné pro přiměřené vyřízení nouzové situace.

Navrhovaná struktura služby eCall stanoví možnost rozšířit dále účinnost služby, pokud poskytovatel služby poskytne na základě doplňujících údajů obsažených v úplném souboru údajů (FSD) další osobní údaje a údaje o vozidle.

3. SLUŽBA ECALL Z HLEDISKA OCHRANY ÚDAJŮ A SOUKROMÍ A PRÁVNÍ ODŮVODNĚNÍ

3.1. Povinná anebo dobrovolná služba

Evropská komise spolu s členskými státy a zástupci automobilového odvětví se prozatím shodli na samoregulačním přístupu, ale pokud zavádění služby eCall nebude pokračovat podle dohodnutého plánu, může Komise přijmout další opatření, včetně regulačních opatření.

Přesto, že si pracovní skupina zřízená podle článku 29 uvědomuje, že obecné zavedení služby eCall by přineslo sociálně-hospodářský přínos a zvýšení veřejné bezpečnosti, existují jisté obavy ohledně ochrany údajů a soukromí, kterými je třeba se v tomto dokumentu zabývat.

Před bližším prozkoumáním účinků služby na ochranu údajů se pracovní skupina zřízená podle článku 29 zabývala dvěmi možnostmi pro provádění služby eCall, které je třeba zvážit na samém začátku a dále analyzovat:

- možnost 1) služba eCall by měla být poskytována na dobrovolném základě;
- možnost 2) služba eCall by měla být povinně využívanou službou.

Možnost 1:

Pokud bude služba eCall poskytována na dobrovolné bázi jako druh vyspělé služby na podporu bezpečnosti silničního provozu, je třeba zavést jednoduchý způsob její aktivace/deaktivace.

V tomto případě by se systém *de facto* instaloval do vozidla a jeho aktivace by byla dobrovolná[10]. Uživatel, který nemusí být nutně i vlastníkem vozidla, by měl kdykoli možnost zapnout anebo vypnout systém bez jakýchkoli technických anebo finančních překážek. Tuto možnost lze provést prostřednictvím např. zabudováním daného tlačítka/ovladače podobného ovladači airbagu, který by byl snadno použitelný.

[10] To neznamená, že službu by nešlo aktivovat automaticky, pokud jí bude motor vybaven, ale že si jí může uživatel kdykoli aktivovat/deaktivovat.

Tato možnost vychází ze skutečnosti, že jedním z ústředních kritérií pro zákonné zpracování údajů je čl. 7 písm. a) směrnice na ochranu údajů, který umožňuje zpracovávat údaje, jen pokud k tomu dala příslušná osoba jasný souhlas. Tento souhlas se poskytuje dobrovolně a příslušné osobě by se rovněž mělo umožnit svůj souhlas odvolat. Je třeba zdůraznit, že o dobrovolný souhlas se nejedná, pokud by musela příslušná osoba v tomto ohledu přijmout klauzuli v rámci smlouvy, o jejichž klauzulích není možno jednat (což je většinou případ smluv o prodeji vozidla).

Dále pracovní skupina zřízená podle článku 29 považuje za nezákonné situace např. pokud by pojišťovací společnosti nebo půjčovny automobilů vyvíjeli na zákazníka nátlak, aby ponechal službu eCall aktivovanou. Obdobnou povinnost by bylo možné požadovat po zaměstnancích používajícím firemní vozidla, pokud by byl na ně vyvíjen nátlak, ať již přímo či nepřímo, aby využívali službu eCall.

Pracovní skupina zřízená podle článku 29 by chtěla zdůraznit, že pokud nebude možné systém eCall aktivovat a zvláště deaktivovat kdykoli na místě bez dalšího úsilí a bezplatně, budou se uživatelé obávat případných důsledků na ochranu soukromí a mohou se rozhodnout, že systém nebudou používat. V tomto ohledu je také třeba navrhnout jednoduchou nezpoplatněnou aktivaci/deaktivaci, protože i to by mohlo být odrazovým můstkem pro všeobecné zavedení služby eCall.

I když v mnoha případech by mohlo být pro příslušnou osobu zpracování údajů v jejím životním zájmu a zavedení služby eCall by tak bylo slučitelné s ustanoveními čl. 7 písm. c), d) a e) směrnice na ochranu údajů, ve všech případech tomu tak nebude. Např. může dojít k tomu, že v případě nehody bude automaticky vysláno tísňové volání, ale záchranné služby nebudou zapotřebí.

Na základě informací o konfiguraci systému eCall, které jsou v současnosti dostupné, má pracovní skupina za to, že bude možné určit polohu příslušného vozidla, které přitom nebude trvale sledováno – protože systém bude zahrnut do komunikační sítě jen pokud dojde k nehodě anebo pokud bude spuštěn manuálně. Pracovní skupina tuto možnost vítá a chtěla by zdůraznit, že z hlediska ochrany údajů by nebylo přijatelné, aby byla příslušná zařízení trvale připojena na síť a vozidla tím trvale sledovatelná kvůli možné aktivaci přístroje eCall. To znamená, že by bylo např. přijatelné uchovávat v paměti přístroje eCall tři poslední polohy vozidla naposledy zaznamenané systémy GPS/Galileo (pokud je jimi vozidlo vybaveno a pokud jsou napojeny na přístroj eCall), aniž by docházelo k jakémukoli sdělování údajů, pokud by nedošlo ke spouštěcímu signálu (např. k nehodě nebo manuální aktivaci). V tomto případě by bylo nezbytné jasně vymezit rozsah shromažďovaných údajů a zabránit jakémukoli dalšímu využití informací – např. pro jiné účely než zajištění bezpečnosti silničního provozu.

Možnost 2:

Pokud by byla služba eCall povinná, byl by systém *de facto* instalován do vozidla a jeho aktivace by byla povinná. Tuto možnost bude však potřeba stvrdit příslušným právním předpisem platným v rámci celé EU. Takový právní předpis by musel být řádně odůvodněn, pokud jde o ochranu údajů.

Pokud by byla služba eCall povinným nástrojem, potom by musela být veškeré omezení soukromí při uplatňování zásad stanovených směrnicí na ochranu údajů, mezi jinými i zásada proporcionality, jasně stanovena v daném právním předpisu. Do systému eCall by měly být zapojeny technologie na ochranu soukromí s cílem poskytnout uživatelům služby eCall požadovanou úroveň ochrany soukromí. Je potřeba rovněž rozvíjet a integrovat do systému bezpečnostní prvky, které zabrání sledování a zneužívání údajů. To bude součást plánu pro možnost 1. S cílem získat poradenství ohledně nejlepších možných postupů je potřeba konzultovat vnitrostátní orgány na ochranu údajů.

Pro shrnutí: pokud bude služba eCall volitelná, je třeba představit řešení příznivé pro uživatele, které jim nabídne aby si sami zvolili, zda službu využijí, a to tím, že jim umožní z technického hlediska službu eCall vypnout/zapnout v závislosti na situaci, např. pomocí elektronických vypínačů, inteligentních karet anebo jiných zařízení umožňujících dobrovolnou aktivaci přístroje eCall, a v případě zájmu sdělovat kromě údajů obsažených v minimálním souboru údajů i další údaje. Pokud bude služba eCall volitelná, bude potřeba začlenit pravidla do příslušných právních předpisů s ohledem na zásady o ochraně údajů.

V obou zmíněných případech bude pracovní skupina zřízená podle článku 29 podporovat zvyšování povědomí o důsledcích služby na ochranu soukromí a údajů. Vnitrostátní orgány na ochranu údajů budou pod záštitou pracovní skupiny zřízené podle článku 29 napomáhat v rozšiřování povědomí o službě eCall s důrazem na otázky ohledně ochrany údajů jako např. transparentní a zákonné zpracování údajů shromažďovaných prostřednictvím služby eCall.

Pracovní skupina zřízená podle článku 29 upřednostňuje zavést službu eCall na dobrovolném principu. Pokud bude zvolena možnost, kdy bude služba zaváděna povinně, bude třeba zajistit řádné zabezpečení ochrany údajů.

3.2. Dvě úrovně poskytování služeb

Bez ohledu na to, zda bude zavedení služby eCall povinné či volitelné, předpokládá iniciativa eCall možnost rozšířeného systému poskytovatelů služeb s přidanou hodnotou. V daném případě budou existovat dvě úrovně služeb:

1) První plánovaná úroveň služeb bude iniciovat sdělování informací obsažených v MSD příslušnému centru tísňového volání, jako jsou poloha vozidla, čas nehody, identifikace vozidla a statut služby eCall (minimálně informace, zda bylo tísňové volání uskutečněno manuálně anebo automaticky), které stanoví stupeň závažnosti nehody.

Tato „základní“ služba je jediná, kterou podporuje Evropská komise.

2) Druhá úroveň služby spočívá v tom, že bude ke sdělovaným „základním“ informacím obsaženým v MSD přidávat doplňující informace, které bude mít k dispozici třetí strana poskytující služby s přidanou hodnotou, např. pojišťovací společnosti, automobilová call centra, lékařské společnosti, právníci, motoristické kluby atd. Pokud dojde k přenosu „úplného souboru údajů“ (FSD), bude vyžadováno uzavření smlouvy mezi vlastníkem vozidla a poskytovatelem služby.

V tomto případě by uživatel umožnil poskytovateli služby obdržet doplňující údaje o nehodě anebo o cestujících a poskytnout např. pomoc pojišťovací společnosti, automobilového klubu nebo jazykovou pomoc apod. Očekává se, že tato rozšířená služba bude rozvinuta tržními subjekty.

Proti tomuto schématu nelze v podstatě nic namítat. Tyto otázky jsou však komplexnější a vyžadují podrobnější posouzení. Vzhledem ke skutečnosti, že některé údaje, které budou zpracovávány, budou citlivé povahy, musí být přísně dodržována zejména pravidla pro ochranu údajů. U rozšířených základních funkcí tísňového volání, které spočívají v tom, že soukromému poskytovateli služby je kromě MSD zaslán i úplný soubor údajů, se vyžaduje podrobnější definice. Tyto služby by měly být plně v souladu s příslušnými právními předpisy o ochraně údajů a soukromí.

Pracovní skupina zřízená podle článku 29 připomíná základní zásady, kterými by se měli poskytovatelé služeb řídit:

i) Pracovní skupina chce zdůraznit, že FSD nebude *„a priori“* stanovený soubor informací, ale bude se spíše odvíjet od dohody učiněné mezi vlastníkem/uživatelem vozidla v rámci uzavřených smluv a bude záviset na FSD a jednotlivých poskytovatelích služeb (pojišťovacích společnostech, automobilových klubech, lékařských společnostech apod.). Proto účely, pro které lze FSD a jeho jednotlivé body použit, musí být jasně stanoveny v jednotlivých smlouvách. Ve smlouvách by rovněž mělo být jasně stanoveno, že poskytovatel služby je správcem příslušných údajů a je vázán veškerými povinnostmi souvisejícími s ochranou údajů a soukromí, kterými jsou správci údajů vázáni podle směrnice na ochranu údajů a vnitrostátních právních předpisů.

ii) Je možno předávat pouze takové údaje, které jsou „nezbytné“ a „relevantní“ pro příslušné účely, což znamená, že je třeba zajistit, aby všichni poskytovatelé přijímali pouze údaje požadované pro účely příslušné smlouvy. Jak je zřejmé z hlediska ochrany údajů, nebude povolen jakýkoli přesun FSD v celku. To bude pravděpodobně vyžadovat vhodné technické úpravy, aby byl systém eCall schopen vybírat pouze ty údaje, které budou pro jednotlivé poskytovatele služby relevantní. V tomto ohledu bude rovněž nezbytné zvážit, zda příslušné informace mají být předávány ve všech případech, jak je zmíněno výše, protože mohou nastat případy, kdy dojde k nehodě a bude spuštěn systém, ale nebude zapotřebí pohotovostních (lékařských) služeb.

iii) Kategorie informací zahrnutých do FSD by měly být jasně vymezeny zástupci automobilového odvětví a dotčenými zainteresovanými subjekty a vlastníkům vozidla musí být poskytnuty vhodné informace o fungování a provozu systému. Součástí těchto informací by měly být rovněž důsledky rozhodnutí vlastníka vozidla o odvolání svého souhlasu s přesunem FSD nebo jeho části; ještě jednou, odvolání souhlasu by nemělo být v neprospěch zájmů vlastníka vozidla.

iv) Pokud bude FSD obsahovat lékařské či jiné údaje citlivé povahy, bude třeba s těmito informacemi nakládat obzvláště opatrně. Kromě výslovného souhlasu vlastníka vozidla, bude nakládání s těmito údaji vyžadovat přijetí zvláštních bezpečnostních opatření, která jsou v některých případech upřesněna ve vnitrostátních právních předpisech.

v) Ustanovení týkající se budoucích přenosů údajů budou muset být dodržována, zejména pokud poskytovatel služby zapojí do zpracování (části) údajů orgány sídlící ve třetích zemích; užitečné informace viz doporučení obsažené v dokumentu WP74[11].

4. OSTATNÍ OTÁZKY SPOJENÉ SE SLUŽBOU ECALL

Z obecného hlediska existují rovněž obavy ohledně vytvoření databází telekomunikačními operátory, doby uchování shromážděných údajů a otázek spojených se zabezpečením uchovaných údajů.

4.1. Databáze

Další otázky ohledně ochrany údajů vyvstávají ve spojení s databázemi vytvořenými s cílem vyhnout se nesprávnému užití nebo zneužití systému, které by měly propojit informace o totožnosti vlastníka vozidla a SIM kartou systému eCall a jejichž hlavním účelem by bylo vyhledávat osoby, které systém zneužívají, např. řidiče, kteří zabloudili apod.

V případě nesprávného využití anebo zneužití systému, které by mohlo způsobit problémy centrům tísňového volání (např. pokud systém uskuteční několik tísňových volání bez platného důvodu), měla by tato centra zavést postup pro sledování zneužívání systému. Pro daný účel je možno využít dvou postupů: i) požadovat po operátorech mobilní sítě, aby identifikovali vlastníka zařízení (pomocí informací uchovaných v databázi SIM karty), jak je tomu nyní u tísňových volání na číslo 112, a ii) požadovat identifikaci po orgánu spravujícího identifikační číslo vozidla (VIN).

Jednou z hlavních obav pracovní skupiny zřízené podle článku 29 je potenciální riziko, že jakákoli třetí strana může mít z různých účelů k těmto databázím přístup. Proto si přeje zdůraznit, že by nemělo být umožněno jakékoli druhotné využití údajů, např. v rámci donucovacích postupů spojených s provozem, jelikož by to bylo v rozporu se zásadami směrnice na ochranu údajů.

4.2. Otázky zabezpečení

Další obavy se týkají otázek zabezpečení; toho, zda je systém eCall dostatečně zajištěn proti neautorizovaným vstupům. Aby mohl být provozován důvěryhodný systém a bylo možno se vyhnout neautorizovanému přístupu různých třetích stran k osobním údajům systému eCall, je potřeba zajistit dostatečnou úroveň zabezpečení systému uvnitř vozidla a v přenosovém protokolu[12].

---

[11] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp74_en.pdf

[12] Plánuje se, že automobiloví výrobci původního vybavení by zajišťovali dostatečnou úroveň zabezpečení údajů uchovávaných v systému uvnitř vozidla. Dostatečná úroveň bezpečnosti přenosového protokolu by pak byla zajištěna jeho standardizací ETSI.

4.3. Proporcionalita

Při využití služby eCall bude pro zpracování nouzové situace přenášen minimální soubor údajů (MSD). Pracovní skupina zřízená podle článku 29 má za to, že stávající požadavek, aby MSD obsahoval celé číslo VIN, lze považovat s ohledem na daný účel za nepřiměřený.

Pracovní skupina zřízena podle článku 29 se zabývá skutečností že vzhledem k tomu, že v některých členských státech v současné době uspokojivě funguje stávající systém tísňového volání, nemusí být zavedení služby eCall ve všech případech nezbytné. Tento argument je důležitý, jelikož se týká otázky proporcionality, tzn. je adekvátní zavést systém pro tísňové volání založený na určení polohy i v těch zemích, kde systém tísňového volání již uspokojivě funguje?

4.4. Povaha správce údajů

Správcem údajů v případě služby eCall bude centrum tísňového volání, které by mělo zavést protokoly pro uchovávání osobních údajů, jejich zpracování a ochranu, které budou obdobné jako protokoly užívané pro jakákoli jiná tísňová volání. Operátoři mobilní sítě budou přenášet minimální soubor údajů transparentním způsobem a měli by zajišťovat, aby údaje v rámci služby eCall nebyly uchovávány v jinou dobu, než je nezbytné pro zajištění jejich adekvátního přenos příslušnému centru tísňového volání. Poté by měl být soubor minimálních údajů vymazán.

Pokud jde o identifikaci volající linky a informace o poloze předávaná centru tísňového volání, měly by být zavedeny protokoly obdobné jako ty, které se používají pro zpracování místních tísňových volání E112 (rozšíření místních služeb tísňového volání) podle směrnice o univerzální službě a doporučení Komise o zpracovávání informací o místě volajícího v elektronických komunikačních sítích pro účely rozšíření místních služeb tísňového volání.

4.5. Doba uchování

Pracovní skupina zřízena podle článku 29 by ráda zdůraznila, že přiměřená doba uchování údajů o tísňovém volání by měla být definována pro různé strany v rámci služby eCall. Vnitrostátní orgány budou dohlížet na to, aby tyto lhůty byly stanoveny a řádně dodržovány.

5. ZAVERY

Pracovní skupina zřízena podle článku 29 při analýze obav spojených s důsledky zavedení služby eCall na ochranu soukromí upřednostňuje a doporučuje pro možné zavedení služby eCall přístup založený na dobrovolné bázi.

Z hlediska ochrany údajů je tísňové volání, které je odesláno automaticky zařízením nebo spuštěno manuálně, poté přenášeno přes mobilní sítě a ústící v informace, kde došlo k nouzové situaci, v zásadě přijatelné, a to za podmínky, že bude existovat zvláštní právní základ a bude zajištěno dostatečné zabezpečení ochrany údajů. Nicméně je třeba vždy zohlednit účely tísňového volání a přiměřenost údajů, které mají být zpracovány, zejména pokud zpracování zahrnuje tzv. úplný soubor údajů.

V Bruselu dne 26. září 2006

Za pracovní skupinu
místopředseda
Jose Luis Piñar Mañas

Věstník Úřadu pro ochranu osobních údajů

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

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

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

ISSN 1213-3442