

Úřední věstník

Evropské unie

C 280



České vydání

Informace a oznámení

Svazek 53

16. října 2010

Oznámení č.	Obsah	Strana
I Usnesení, doporučení a stanoviska		
STANOVISKA		
Evropský inspektor ochrany údajů		
2010/C 280/01	Stanovisko evropského inspektora ochrany údajů k podpoře důvěry v informační společnost prostřednictvím posílení ochrany údajů a soukromí.....	1
2010/C 280/02	Stanovisko evropského inspektora ochrany údajů k návrhu směrnice Evropského parlamentu a Rady o odpadních elektrických a elektronických zařízeních (OEEZ)	16
II Sdělení		
SDĚLENÍ ORGÁNŮ, INSTITUCÍ A JINÝCH SUBJEKTŮ EVROPSKÉ UNIE		
Evropská komise		
2010/C 280/03	Povolení státní podpory podle ustanovení článků 107 a 108 SFEU – Případy, k nimž Komise nevznáší námitku ⁽¹⁾	22
2010/C 280/04	Povolení státní podpory podle ustanovení článků 107 a 108 SFEU – Případy, k nimž Komise nevznáší námitku ⁽¹⁾	26

CS

Cena:
3 EUR

⁽¹⁾ Text s významem pro EHP, kromě produktů, na něž se vztahuje příloha I Smlouvy

(Pokračování na následující straně)

<u>Oznámení č.</u>	Obsah (pokračování)	Strana
2010/C 280/05	Povolení státní podpory podle ustanovení článků 107 a 108 SFEU – Případy, k nimž Komise nevznáší námitku ⁽¹⁾	29
2010/C 280/06	Povolení státní podpory podle ustanovení článků 107 a 108 SFEU – Případy, k nimž Komise nevznáší námitku ⁽¹⁾	30

IV *Informace*

INFORMACE ORGÁNŮ, INSTITUCÍ A JINÝCH SUBJEKTŮ EVROPSKÉ UNIE

Evropská komise

2010/C 280/07	Směnné kurzy vůči euru	31
2010/C 280/08	Rozhodnutí Komise ze dne 14. října 2010 o znovuzřízení skupiny na vysoké úrovni pro konkurenceschopnost a udržitelný růst automobilového průmyslu v Evropské unii – CARS 21	32

V *Oznámení*

ŘÍZENÍ TÝKAJÍCÍ SE PROVÁDĚNÍ POLITIKY HOSPODÁŘSKÉ SOUTĚŽE

Evropská komise

2010/C 280/09	Předběžné oznámení o spojení podniků (Věc COMP/M.5927 – BASF/Cognis) ⁽²⁾	35
2010/C 280/10	Předběžné oznámení o spojení podniků (Věc COMP/M.5982 – CVCII/Advance Properties/Huvepharma) – Věc, která může být posouzena zjednodušeným postupem ⁽²⁾	36
2010/C 280/11	Sdělení ministryně hospodářství Nizozemského království na základě čl. 3 odst. 2 směrnice Evropského parlamentu a Rady 94/22/ES o podmínkách udělování a užívání povolení k vyhledávání, průzkumu a těžbě uhlovodíků	37



⁽¹⁾ Text s významem pro EHP, kromě produktů, na něž se vztahuje příloha I Smlouvy

⁽²⁾ Text s významem pro EHP

I

(Usnesení, doporučení a stanoviska)

STANOVISKA

EVROPSKÝ INSPEKTOR OCHRANY ÚDAJŮ

Stanovisko evropského inspektora ochrany údajů k podpoře důvěry v informační společnost prostřednictvím posílení ochrany údajů a soukromí

(2010/C 280/01)

EVROPSKÝ INSPEKTOR OCHRANY ÚDAJŮ,

navazujeme vztahy a jak se vzděláváme. Jsou zásadní pro dnešní informační ekonomiku a obecně pro společnost.

s ohledem na Smlouvu o fungování Evropské unie, a zejména na článek 16 této smlouvy,

s ohledem na Listinu základních práv Evropské unie, a zejména na články 7 a 8 této listiny,

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

s ohledem na směrnici Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací ⁽²⁾,

s ohledem na nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů, a zejména na článek 41 tohoto nařízení ⁽³⁾,

PŘIJAL TOTO STANOVISKO:

I. ÚVOD

1. Informační a komunikační technologie (IKT) nabízejí obrovské možnosti prakticky ve všech ohledech našich životů – ovlivňují to, jak pracujeme, bavíme se,

2. Evropská unie je globální silou v pokročilých IKT a je rozhodnuta být jí i nadále. V rámci splnění tohoto úkolu se očekává, že Evropská komise brzy přijme evropskou digitální agendu, o které komisařka Kroesová potvrdila, že je její prioritou ⁽⁴⁾.

3. Evropský inspektor ochrany údajů uznává přínosy IKT a souhlasí, že by Evropská unie měla dělat co nejvíce pro posílení jejich rozvoje a rozsáhlého zavádění. Rovněž plně podporuje názor komisařek Kroesové a Redingové, že v jádru tohoto nového prostředí by měly být fyzické osoby ⁽⁵⁾. Fyzické osoby by měly mít možnost se spolehnout na schopnost IKT zaručit bezpečnost a kontrolu nad užíváním jejich informací a dále na skutečnost, že i v digitálním prostoru budou respektována jejich práva na ochranu soukromí a údajů. Respektování těchto práv je zásadní pro vytvoření důvěry spotřebitelů. A tato důvěra je rozhodující, mají-li občané využívat nové služby ⁽⁶⁾.

⁽⁴⁾ Odpovědi na dotazník Evropského parlamentu pro komisařku Neelie Kroesovou v souvislosti se slyšením Evropského parlamentu, které předcházelo jmenování komisařky.

⁽⁵⁾ Odpovědi na dotazník Evropského parlamentu pro komisařku Neelie Kroesovou v souvislosti se slyšením Evropského parlamentu, které předcházelo jmenování komisařky; projev komisařky Viviane Redingové Evropská digitální agenda pro nového digitálního spotřebitele přednesený na Fóru BEUC několika zainteresovaných stran na téma Soukromí spotřebitelů a on-line marketing: tržní trendy a perspektivy politik, v Bruselu dne 12. listopadu 2009.

⁽⁶⁾ Viz například zpráva Důvěra v informační společnost, zpráva poradního výboru, RISEPTIS (Výzkum a inovace v oblasti bezpečnosti, soukromí a důvěryhodnosti v informační společnosti). Dostupné na adrese <http://www.think-trust.eu/general/news-events/riseptis-report.html> Viz také: J. B. Horrigan, *Broadband Adoption and Use in America*, FCC Omnibus Broadband Initiative, OBI Working Paper Series No 1 (J. B. Horrigan, Přijetí a využití širokého pásma v Americe, Iniciativa pro souhrnné široké pásmo FCC, Pracovní dokument ISŠP, řada č. 1).

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

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

⁽³⁾ Úř. věst. L 8, 12.1.2001, s. 1.

4. EU má silný právní rámec v oblasti ochrany údajů a soukromí, jehož zásady zůstávají v digitálním věku platné v plném rozsahu. To však nelze považovat za dostačující. V mnoha případech IKT vzbuzují nové obavy, které nejsou ve stávajícím právním rámci zohledněny. Proto je potřeba podniknout určité kroky, aby se zajistilo, že práva fyzických osob zakotvená v právu EU budou i nadále poskytovat účinnou ochranu v tomto novém prostředí.

5. Toto stanovisko pojednává o opatřeních, která by Evropská unie mohla buď podpořit, nebo přijmout, aby zaručila ochranu soukromí a údajů fyzických osob v globalizovaném světě, ve kterém technologie bude i nadále hnací silou. Pojednává o legislativních i nelegislativních nástrojích.

6. Po představení IKT jako pokroku, který vytváří příležitosti, ale také přináší rizika, se toto stanovisko zabývá potřebou zohlednit ochranu údajů a soukromí v praxi, a to od samého počátku nových informačních a komunikačních technologií (což je označováno jako zásada „soukromí coby aspekt návrhu“). Dále toto stanovisko pojednává o potřebě zohlednění této zásady v právním rámci pro ochranu osobních údajů alespoň dvěma různými způsoby. Za prvé jejím začleněním jako obecné, závazné zásady a za druhé jejím začleněním do konkrétních oblastí IKT představujících specifická rizika pro ochranu údajů a soukromí, která mohou být zmírněna pomocí přiměřené technické architektury a návrhu. Těmito oblastmi jsou identifikace na základě rádiové frekvence (RFID), aplikace sociálních sítí a aplikace prohlížečů. Závěrem stanovisko předkládá návrhy týkající se dalších nástrojů a zásad zaměřených na ochranu soukromí a údajů fyzických osob v oblasti IKT.

7. Při řešení výše uvedených otázek se stanovisko podrobněji zabývá některými body zmíněnými pracovní skupinou zřízenou podle článku 29 v jejím příspěvku k veřejné konzultaci o budoucnosti soukromí⁽¹⁾. Dále navazuje na dřívější stanoviska evropského inspektora ochrany údajů, jako je stanovisko ze dne 25. července 2007 k provádění

směrnice o ochraně údajů, stanovisko ze dne 20. prosince 2007 k RFID a jeho dvě stanoviska ke směrnici o ochraně soukromí v odvětví elektronických komunikací⁽²⁾.

II. IKT NABÍZEJÍ NOVÉ PŘÍLEŽITOSTI, ALE PŘEDSTAVUJÍ TAKÉ NOVÁ RIZIKA

8. IKT jsou srovnávány s jinými důležitými objevy minulosti, jako je elektřina. I když je možná příliš brzy na hodnocení jejich skutečného historického dopadu, vazba mezi IKT a hospodářským růstem v rozvinutých zemích je jasná. IKT přinesly zaměstnanost, hospodářské přínosy a přispěly k celkovému blahobytu. Dopad IKT je širší než čistě ekonomický, protože hraje důležitou úlohu při posilování inovace a tvořivosti.

9. IKT dále změnily způsob, jak lidé pracují, navazují vztahy a vzájemně reagují. Lidé se například stále více opírají o IKT při sociálních a hospodářských interakcích. Fyzické osoby mohou využívat široký rozsah nových aplikací IKT, jako jsou elektronické aplikace ve zdravotnictví, dopravě a státní správě (eHealth, eTransport, eGovernment), jakož i inovační interaktivní systémy pro zábavu a učení.

10. S ohledem na tyto přínosy všechny evropské instituce vyjádřily svůj závazek podporovat IKT jako nezbytný nástroj ke zlepšení konkurenceschopnosti evropského průmyslu a zrychlení hospodářského zotavení v Evropě. V srpnu 2009 Komise přijala zprávu o digitální konkurenceschopnosti Evropy⁽³⁾ a zahájila veřejnou konzultaci o vhodných budoucích strategiích pro posílení IKT. Dne 7. prosince 2009 Rada předložila svůj příspěvek k této konzultaci nazvaný „Strategie navazující na i2010 – na cestě k otevřené, zelené a konkurenceschopné znalostní společnosti“⁽⁴⁾. Evropský

⁽¹⁾ Stanovisko 168 pracovní skupiny zřízené podle článku 29 k budoucnosti soukromí, společný příspěvek ke konzultaci Evropské komise k právnímu rámci pro základní právo na ochranu osobních údajů přijaté dne 1. prosince 2009.

⁽²⁾ Stanovisko ze dne 25. července 2007 ke sdělení Komise Evropskému parlamentu a Radě o pokračování pracovního programu pro lepší provádění směrnice o ochraně osobních údajů, Úř. věst. C 255, 27.10.2007, s. 1; Stanovisko ze dne 20. prosince 2007 ke sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů o identifikaci na základě rádiové frekvence (RFID) v Evropě: kroky k rámci politiky (KOM(2007) 96), Úř. věst. C 101, 23.4.2008, s. 1; Stanovisko ze dne 10. dubna 2008 k návrhu směrnice, kterou se mění mimo jiné směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích), Úř. věst. C 181, 18.7.2008, s. 1; Druhé stanovisko ze dne 9. ledna 2009 k přezkoumání směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací.

⁽³⁾ Zpráva o digitální konkurenceschopnosti Evropy – Hlavní úspěchy strategie i2010 v období 2005–2009 (SEK(2009) 1060).

⁽⁴⁾ Závěry Rady „Strategie navazující na i2010 – na cestě k otevřené, zelené a konkurenceschopné znalostní společnosti.“ (17107/09), přijato dne 18.12.2009.

parlament právě přijal zprávu, která má Komisi poskytnout vodítko při vymezení digitální agendy ⁽¹⁾.

11. Příležitosti a přínosy, které doprovázejí rozvoj IKT, jsou spojeny s novými riziky, zejména pro soukromí a ochranu osobních údajů fyzických osob. IKT často vedou k nárůstu množství informací, které jsou shromažďovány, tříděny, filtrovány, přenášeny nebo jinak uchovávány (a to způsoby, které jsou velmi často mimo dohled fyzických osob), a rizika pro takové údaje se proto násobí.
12. Například na (některých) spotřebních výrobcích jsou čárové kódy nahrazovány čipy RFID. Díky zlepšení informačního toku v dodavatelském řetězci (a v důsledku toho omezení potřeby disponovat „bezpečnostními“ zásobami, poskytováním přesnějších výhledů atd.) má nový systém znamenat přínosy pro podnik i spotřebitele. Současně to však vede ke znepokojující možnosti sledovatelnosti prostřednictvím označeného osobního majetku, a to pro různé účely a ze strany různých subjektů.
13. Dalším příkladem je „cloud computing“, v zásadě poskytování internetových služeb spotřebitelských a jiných než spotřebitelských úložných aplikací. Jejich rozsah se pohybuje od fotografických alb, kalendářů, internetových poštovních databází a databází spotřebitelů po složitější služby související s podnikáním. Přínosy pro podniky i fyzické osoby jsou jasné; snížení nákladů (náklady skokově rostou), omezení vazby na místo (snadný přístup k informacím kdekoli na světě), automatizace (není potřeba mít zvláštní zdroje pro informační technologie a údržbu aktuálního softwaru) atd. Současně však existují rizika poruch zabezpečení a hackerství, která jsou velmi reálná. Existuje také obava, že může dojít ke ztrátě přístupu k vlastním údajům a kontrole nad nimi.
14. Souběžná existence přínosů a rizik byla prokázána v dalších oblastech, kde dochází k využívání aplikací IKT. Vezměme si elektronickou aplikaci pro zdravotnictví (eHealth), která může zvýšit účinnost, snížit náklady, zvýšit přístupnost a obecně zlepšit kvalitu služeb zdravotní péče. Aplikace eHealth však často vede k otázce oprávněnosti sekundárního využití informací, které jsou v ní obsaženy, což vyžaduje pečlivou analýzu účelů potenciálního sekundárního využití ⁽²⁾. Navíc s rozsáhlejšíím využíváním elektronických zdravotních záznamů došlo ke skandálům u samotných systémů, které odhalily mnoho případů hackerství v oblasti elektronických zdravotních záznamů.

15. Celkem vzato je pravděpodobné, že bude přetrvávat určitý stupeň zbytkového rizika i po provedení správného vyhodnocení a přijetí nezbytných opatření. Situace nullového rizika by byla nerealistická. Jak je však uvedeno dále, lze a musí být provedena opatření ke snížení takového rizika na přiměřenou úroveň.

III. SOUKROMÍ COBY ASPEKT NÁVRHU JAKO KLÍČOVÝ NÁSTROJ PRO VYTVOŘENÍ DŮVĚRY FYZICKÝCH OSOB V IKT

16. Potenciální přínosy IKT lze v praxi využívat pouze, pokud jsou schopny vytvořit důvěru, jinými slovy, jestliže mohou zajistit ochotu uživatele být závislým na IKT kvůli jejich charakteristikám a přínosu. Taková důvěra se vytvoří pouze, pokud jsou IKT spolehlivé, bezpečné, pod kontrolou fyzických osob a pokud je zaručena ochrana jejich osobních údajů a soukromí.
17. Rozsáhlá rizika a selhání jako ta, která byla popsána výše, zejména pokud vedou ke zneužití nebo prolomení osobních údajů a odhalení soukromí fyzických osob, pravděpodobně naruší důvěru uživatele v informační společnost. To by mohlo vážně ohrozit rozvoj IKT a přínosy, které by mohly znamenat.
18. Řešením těchto rizik pro ochranu soukromí a údajů však nemůže být zrušení, vyloučení nebo odmítnutí využívání nebo podpory IKT. To by nebylo ani proveditelné, ani realistické; zabránilo by to fyzickým osobám využívat přínosy IKT a vážně by to omezilo celkové výhody, které lze získat.
19. Evropský inspektor ochrany údajů má za to, že pozitivnějším řešením je navrhovat a rozvíjet IKT způsobem, který bere ohled na ochranu soukromí a údajů. Proto je rozhodující, aby ochrana soukromí a údajů byla zapracována do celého cyklu životnosti technologie od velmi brzké etapy návrhu až do jejího zavedení a konečného odstranění. To se obvykle nazývá „soukromí coby aspekt návrhu“ a o tomto konceptu je dále pojednáno níže.
20. Soukromí coby aspekt návrhu může zahrnovat různé kroky v závislosti na konkrétním případě nebo aplikaci. V některých případech může například vyžadovat odstranění či omezení osobních údajů nebo zabránění zbytečnému a/nebo nežádoucímu zpracování. V jiných případech může soukromí coby aspekt návrhu zahrnovat nabídku nástrojů pro posílení kontroly fyzické osoby nad jejími osobními údaji. Taková opatření by měla být zvažována při definování norem anebo osvědčených

⁽¹⁾ Zpráva o vymezení nové digitální agendy pro Evropu: od i2010 po digital.eu (2009/2225 (INI)), přijatá dne 18.3.2010.

⁽²⁾ Například prodej nebo využití zdravotních informací shromážděných za účelem poskytování léčby nesmí být prováděno pro volbu míst satelitních klinik, pro zřizování středisek ambulantních ordinací ani jinak za účelem plánování budoucích činností s finančními dopady, což by vyžadovalo pečlivé zkoumání.

postupů. Tato opatření také mohou být zapracována do architektury informačních a komunikačních systémů nebo do organizačních struktur subjektů, které zpracovávají osobní údaje.

III.1 Zásada soukromí coby aspekt návrhu použitelná v různých prostředích IKT a jejich dopad

21. Potřebu zásady soukromí coby aspekt návrhu lze nalézt v mnoha různých prostředích IKT. Odvětví zdravotnictví se například stále více opírá o infrastrukturu IKT, což často znamená centralizované uložení zdravotních informací pacientů. Uplatnění zásady soukromí coby aspekt návrhu v odvětví zdravotnictví by vyžadovalo hodnocení vhodnosti různých opatření, jako je možnost minimalizace centrálně ukládaných údajů nebo jejich omezení na seznam, používání šifrovacích nástrojů, omezené přidělování přístupových práv na „základě potřeby vědět“, anonymizace údajů, jakmile se již nepotřebují atd.
22. Podobně i dopravní systémy jsou stále více standardně dodávány s pokročilými aplikacemi IKT, které pro různé účely a funkce interagují s vozem a jeho prostředím. Například automobily jsou stále více vybavovány novými funkcemi IKT (GPS, GSM, síť čidel atd.), které v reálném čase informují nejen o jejich místě, ale i o jejich technických podmínkách. Tyto informace by se mohly použít například pro náhradu stávajícího systému silniční daně silničním poplatkem závislým na míře využívání. Uplatnění zásady soukromí coby aspekt návrhu v návrhu architektury takových systémů by mělo podpořit zpracovávání a další předávání co možná nejmenšího množství osobních údajů⁽¹⁾. V souladu s touto zásadou by před centralizovanými strukturami byly upřednostněny decentralizované nebo semidecentralizované architektury, které by omezovaly poskytování údajů o místě do centrálního bodu.
23. Výše uvedené příklady ukazují, že když jsou informační a komunikační technologie vytvářeny podle zásady soukromí coby aspekt návrhu, mohou být významně minimalizována rizika pro ochranu soukromí a údajů.

⁽¹⁾ Viz Stanovisko evropského inspektora ochrany údajů ze dne 22. července 2009 ke sdělení Komise o akčním plánu zavádění inteligentních dopravních systémů v Evropě a k souvisejícímu návrhu směrnice Evropského parlamentu a Rady, kterou se stanoví rámec pro zavedení inteligentních dopravních systémů v silniční dopravě a jejich styčné body s jinými druhy dopravy, dostupné na adrese: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-07-22_Intelligent_Transport_Systems_CS.pdf

III.2 Nedostačující zavádění IKT uplatňujících zásadu soukromí coby aspekt návrhu

24. Důležitou otázkou je, zda hospodářské subjekty, výrobci/poskytovatelé IKT a správci údajů mají zájem podporovat a uplatňovat zásadu soukromí coby aspekt návrhu u IKT. V této souvislosti je také důležité zhodnotit poptávku uživatelů.
25. V roce 2007 Komise vydala sdělení, kterým vyzývá podniky, aby využily svoji inovační kapacitu pro tvorbu a provádění technologií zvyšujících ochranu soukromí (PET) jako způsobu zlepšení ochrany soukromí a osobních údajů od samého počátku vývojového cyklu⁽²⁾.
26. Dostupné důkazy však ukazují, že ani výrobci IKT, ani správci údajů (v soukromém i veřejném sektoru) dosud nebyli schopni důsledně uplatňovat nebo obchodně prosazovat soukromí coby aspekt návrhu. Byly uváděny různé důvody, včetně chybějících ekonomických stimulů nebo institucionální podpory, nedostatečné poptávky atd.⁽³⁾.
27. Současně poptávka ze strany uživatelů po soukromí coby aspektu návrhu byla poměrně nízká. Uživatelé produktů a služeb IKT možná oprávněně předpokládají, že jejich soukromí a osobní údaje jsou *de facto* chráněny, zatímco v mnoha případech nejsou. V některých případech prostě nemohou učinit bezpečnostní opatření nutná pro ochranu buď svých vlastních osobních údajů, nebo osobních údajů jiných osob. V mnoha případech je to proto, že nemají úplné nebo dokonce ani částečné znalosti o těchto rizicích. Například obecně platí, že mládež přehlíží rizika pro soukromí spojená se zobrazováním osobních informací na sociálních sítích a často ignoruje nastavení pro ochranu soukromí. Další uživatelé mají povědomí o rizicích, ale možná nemají nezbytnou technickou odbornost pro zavádění bezpečnostních technologií pro ochranu jejich připojení na internet nebo změnu nastavení prohlížeče pro minimalizaci tvorby profilů na základě sledování jejich činnosti na internetu.
28. Rizika pro ochranu soukromí a údajů jsou velmi reálná. Pokud není ochrana soukromí a údajů zohledněna od samého počátku, je často příliš pozdě a příliš ekonomicky

⁽²⁾ Sdělení Komise Evropskému parlamentu a Radě ze dne 2.5.2007, KOM(2007) 228 v konečném znění, o podpoře ochrany osobních údajů prostřednictvím technologií zvyšujících ochranu soukromí (PET).

⁽³⁾ Studie o ekonomických přínosech technologií zvyšujících ochranu soukromí (PETS) jls/2008/D4/036.

obtížné zavedené systémy korigovat rovněž jako je příliš pozdě na nápravu již vzniklé škody. Narůstající počet případů narušení údajů v nedávné minulosti tento problém dokonale odhaluje a prohlubuje potřebu soukromí coby aspektu návrhu.

29. Výše uvedené jasně naznačuje, že výrobci a poskytovatelé IKT určených ke zpracování osobních údajů by měli mít spolu se správci údajů odpovědnost za jejich návrh se zabudovanou ochranou údajů a ochranou soukromí. V mnoha případech by to znamenalo, že by měly být navrženy s ochranou soukromí jako standardním nastavením.

30. V této souvislosti musíme zvážit, jaké kroky by měli učinit tvůrci politik pro podporu zásady soukromí coby aspektu návrhu při rozvoji IKT. První otázkou je, zda stávající právní rámec ochrany údajů obsahuje odpovídající ustanovení pro zajištění provádění zásady soukromí coby aspektu návrhu ze strany správců údajů i výrobců či vývojarů. Druhou otázkou je, co by se mělo udělat s ohledem na evropskou digitální agendu pro zajištění, aby odvětví IKT vzbuzovalo důvěru spotřebitelů.

IV. ZAPRACOVÁNÍ ZÁSADY SOUKROMÍ COBY ASPEKTU NÁVRHU DO PRÁVA A POLITIK EU

IV.1 Současný právní rámec ochrany údajů a soukromí

31. EU má silný právní rámec v oblasti ochrany údajů a soukromí obsažený ve směrnici 95/46/ES ⁽¹⁾, směrnici 2002/58/ES ⁽²⁾ a judikatuře Evropského soudu pro lidská práva ⁽³⁾ a Soudního dvora.

32. Směrnice o ochraně údajů se vztahuje na „jakýkoli úkon nebo soubor úkonů s osobními údaji“ (shromažďování, uchovávání, sdělení atd.). Ukládá nutnost vyhovění určitým zásadám a povinnostem ze strany těch, kteří zpracovávají osobní údaje („správci údajů“). Stanoví práva fyzických osob, jako je právo na přístup

k osobním údajům. Směrnice o soukromí a elektronických komunikacích se konkrétně zabývá ochranou soukromí v odvětví elektronických komunikací ⁽⁴⁾.

33. Stávající směrnice o ochraně údajů neobsahuje výslovný požadavek na soukromí coby aspektu návrhu. Obsahuje však ustanovení, která mohou v různých situacích nepřímo vyžadovat provedení zásady soukromí coby aspektu návrhu. Zvláště článek 17 vyžaduje, aby správci údajů přijali vhodná technická a organizační opatření, aby zabránili nedovolenému zpracování údajů ⁽⁵⁾. Zásada soukromí coby aspektu návrhu je proto zahrnuta velmi obecným způsobem. Ustanovení směrnice se navíc obrací hlavně na správce údajů a jejich zpracování osobních informací. Výslovně nevyžadují, aby informační a komunikační technologie vyhovovaly ochraně soukromí a údajů, což vyžaduje oslovení návrhářů a výrobců IKT i zahrnutí činností vykonávaných v etapě normalizace.

34. Směrnice o soukromí a elektronických komunikacích je jednoznačnější. Čl. 14 odst. 3 uvádí, že „V případě potřeby lze přijmout opatření, aby bylo zajištěno, že koncové zařízení je sestrojeno tak, že odpovídá právu uživatelů na ochranu a kontrolu využití jejich osobních údajů v souladu se směrnicí 1999/5/ES a rozhodnutím Rady 87/95/EHS ze dne 22. prosince 1986 o normalizaci v oblasti informačních technologií a telekomunikací“. Toto ustanovení však nikdy nebylo použito ⁽⁶⁾.

35. Zatímco výše uvedená ustanovení těchto dvou směrnic napomáhají podpoře zásady soukromí coby aspektu návrhu, v praxi tato zásada nebyla dostačující pro zajištění zohlednění ochrany soukromí v odvětví IKT.

36. V důsledku této situace platné právní předpisy dostatečně přesným způsobem nevyžadují, aby IKT byly navrhovány v souladu se zásadou soukromí coby aspektu návrhu.

⁽¹⁾ Směrnice Evropského parlamentu a Rady 95/46/ES (dále: směrnice o ochraně údajů).

⁽²⁾ Směrnice Evropského parlamentu a Rady 2002/58/ES (dále: směrnice o soukromí a elektronických komunikacích).

⁽³⁾ Interpretace hlavních prvků a podmínek stanovených v článku 8 Úmluvy o ochraně lidských práv a základních svobod (EÚLP) přijaté v Římě dne 4. listopadu 1950, které se uplatňují u různých.

⁽⁴⁾ Lisabonská smlouva takovou ochranu posílila tím, že v článku 7 a 8 Listiny základních práv Evropské unie uznala úctu k soukromému životu a ochranu osobních údajů jako samostatná základní práva. Listina základních práv Evropské unie se stala závaznou, když vstoupila v platnost Lisabonská smlouva.

⁽⁵⁾ Článek 17 má toto znění: „Členské státy stanoví, že správce musí přijmout vhodná technická a organizační opatření na ochranu osobních údajů proti náhodnému nebo nedovolenému zničení, náhodné ztrátě, úpravám, neoprávněnému sdělování nebo přístupu, zejména pokud zpracování zahrnuje předávání údajů v síti, jakož i proti jakékoli jiné podobě nedovoleného zpracování.“ Bod odůvodnění 46 to doplňuje tím, že uvádí „Vzhledem k tomu, že ochrana práv a svobod subjektů údajů v souvislosti se zpracováním osobních údajů vyžaduje, aby byla přijata příslušná technická a organizační opatření jak při přípravě systému zpracování, tak v průběhu vlastního zpracování, s cílem zajistit především bezpečnost a tím také zabránit jakémukoli neoprávněnému zpracování“.

⁽⁶⁾ Komise ohlásila plány aktualizovat směrnici 1999/5/ES koncem roku 2010.

Úřady na ochranu údajů také nemají dostatek pravomocí pro zajištění zapracování této zásady, což vede k její neúčinnosti. Například úřady na ochranu údajů mohou uložit sankce, když nedojde k odpovědi na žádost o přístup ze strany fyzických osob, a budou mít kompetence na to, aby vyžadovaly provedení určitých opatření pro zabránění nedovoleného zpracování údajů. Přesto není vždy dostatečně jasné, zda se jejich pravomoci vztahují na to, aby požadovaly, že systém má být navržen tak, aby usnadňoval uplatňování práva fyzických osob na ochranu údajů⁽¹⁾. Například na základě stávajících právních ustanovení není jasné, zda by mohlo být požadováno, aby architektura informačního systému byla navržena tak, aby usnadňovala reakci společností na žádosti o přístup ze strany fyzických osob způsobem, který by znamenal automatické a rychlejší zpracování těchto žádostí. Navíc pozdější pokusy o změnu technologie poté, co byla vytvořena nebo zavedena, mohou vést k nedokonalým řešením, která kromě ekonomické nevýhodnosti nemusí být plně funkční.

37. Podle názoru evropského inspektora ochrany údajů, který sdílí s pracovní skupinou zřízenou podle článku 29⁽²⁾, současný právní rámec ponechává prostor pro jednoznačnější podporu zásady soukromí coby aspektu návrhu.

IV.2 Zapracování zásady soukromí coby aspektu návrhu na různých úrovních

38. Ve světle výše uvedeného evropský inspektor ochrany údajů doporučuje Komisi, aby provedla čtyři kroky:

a) navrhla zahrnout obecné ustanovení o soukromí coby aspektu návrhu do právního rámce pro ochranu údajů;

b) podrobně popsala toto obecné ustanovení ve specifických ustanoveních, až budou navrženy konkrétní právní nástroje v různých odvětvích. Tato specifická ustanovení by již nyní mohla být zahrnuta do právních nástrojů, a to na základě článku 17 směrnice o ochraně údajů (a dalších stávajících právních předpisů);

c) zahrnula soukromí coby aspekt návrhu jako vedoucí zásadu do evropské digitální agendy;

d) zavedla soukromí coby aspekt návrhu jako zásadu do dalších iniciativ EU (zejm. nelegislativní povahy).

Obecné ustanovení o soukromí coby aspektu návrhu

39. Evropský inspektor ochrany údajů navrhuje jednoznačně a výslovně zahrnout zásadu soukromí coby aspekt návrhu do stávajícího právního rámce ochrany údajů. To by zajistilo, že tato zásada bude silnější, zřetelnější a že si kromě zajištění větší oprávněnosti donucovacích orgánů vyžadovat její *de facto* uplatňování v praxi vynutí účinné provádění. To je zejména nutné s ohledem na výše popsané skutečnosti, nejen kvůli důležitosti samotné zásady jako nástroje podpory důvěry, ale také jako stimulu pro zainteresované strany, aby prováděly zásadu soukromí coby aspekt návrhu a prohloubily záruky, které jsou již obsaženy ve stávajícím právním rámci.

40. Tento návrh navazuje na doporučení pracovní skupiny zřízené podle článku 29 zavést zásadu „soukromí coby aspekt návrhu“ jako obecnou zásadu do právního rámce ochrany údajů, a to zejména směrnice o ochraně údajů. Jak uvádí pracovní skupina zřízená podle článku 29: „Tato zásada by měla být závazná pro návrháře a výrobce technologií i pro správce údajů, kteří musí rozhodovat o pořízení a využívání IKT. Měli by mít povinnost zohlednit technologickou ochranu údajů již v etapě plánování informačních a technologických postupů a systémů. Poskytovatelé takových systémů nebo služeb i správci by měli prokázat, že přijali všechna opatření vyžadovaná pro vyhovění těmto požadavkům“.

41. Evropský inspektor ochrany údajů také vítá podporu zásady soukromí coby aspekt návrhu ze strany komisařky Viviane Redingové vyjádřenou v souvislosti s oznámením o přezkoumání směrnice o ochraně údajů⁽³⁾.

42. Tím se dostáváme k obsahu takové regulace. Prvním a nejdůležitějším ohledem je, že zásada soukromí coby aspekt návrhu by měla být nezávislá na technologii. Tato zásada by neměla regulovat technologii, tedy neměla by předepisovat konkrétní technická řešení. Místo toho by

⁽¹⁾ Viz zpráva úřadu komisaře Spojeného království pod názvem: „Privacy by Design“ (Soukromí coby aspekt návrhu), zveřejněná v listopadu 2008.

⁽²⁾ Viz Stanovisko 168 pracovní skupiny zřízené podle článku 29 k budoucnosti soukromí, společný příspěvek ke konzultaci Evropské komise k právnímu rámci pro základní právo na ochranu osobních údajů přijaté dne 1. prosince 2009.

⁽³⁾ „Soukromí coby aspekt návrhu je zásada, která je v zájmu občanů i podniků. Soukromí coby aspekt návrhu povede k lepší ochraně pro fyzické osoby i k důvěře v nové služby a výrobky, která zase povede ke kladnému dopadu na hospodářství. Existují některé povzbudivé příklady, ale je třeba udělat ještě daleko více“ Hlavní projev v Den ochrany osobních údajů, 28. ledna 2010, Evropský parlament, Brusel.

měla nařizovat, aby stávající zásady ochrany soukromí a údajů byly začleněny do informačních a komunikačních systémů a řešení. To by umožnilo zainteresovaným stranám, výrobcům, správcům údajů a úřadům na ochranu údajů vykládat význam této zásady v každém jednotlivém případě. Za druhé by vyhovění této zásadě bylo povinné v různých etapách, od vytvoření norem a návrhu architektury po jejich provedení ze strany správce údajů.

Ustanovení ve specifických právních předpisech

43. Zásadu soukromí coby aspekt návrhu bude nutno začlenit do stávajících i budoucích právních předpisů, a to na základě současného právního rámce a – po jeho přijetí – na základě výše zmíněného obecného ustanovení. Například podle současných iniciativ týkajících se inteligentních dopravních systémů Komise bude mít konkrétní počáteční odpovědnost při vymezení opatření, normalizačních iniciativ, postupů a osvědčené praxe. Při provádění těchto úkolů by zásada soukromí coby aspekt návrhu měla být vedoucí zásadou.

44. Evropský inspektor ochrany údajů dále poznamenává, že zásada soukromí coby aspekt návrhu má také specifický význam v oblasti svobody, bezpečnosti a práva, zejména ve vztahu k cílům strategie pro správu informací, jak se předpokládají ve Stockholmském programu ⁽¹⁾. Ve svém stanovisku týkajícím se Stockholmského programu evropský inspektor ochrany údajů zdůraznil, že architektura pro výměnu informací by měla být založena na „soukromí coby aspektu návrhu“ ⁽²⁾: „Konkrétněji to znamená, že by informační systémy, které jsou navrhovány za účelem veřejné bezpečnosti, měly být vždy vytvářeny v souladu se zásadou soukromí coby aspekt návrhu“.

45. Stanovisko pracovní skupiny zřízené podle článku 29 k budoucnosti soukromí ⁽³⁾ ještě přesněji zdůrazňuje, že v oblasti svobody, bezpečnosti a práva, kde jsou hlavními aktéry veřejné orgány a kde opatření ke zvýšení dohledu mají přímý dopad na základní práva na ochranu soukromí a údajů, by požadavky soukromí coby aspektu návrhu měly být povinné. Zavedením těchto požadavků do informačních systémů by vlády také podpořily soukromí coby aspekt návrhu jako první zákazníci.

⁽¹⁾ Stockholmský program – Otevřená a bezpečná Evropa, která slouží občanům a chrání je, schválený Evropskou radou v prosinci 2009.

⁽²⁾ Stanovisko ze dne 10. července 2009 ke sdělení Komise Evropskému parlamentu a Radě o prostoru svobody, bezpečnosti a práva ve službách občanům, Úř. věst. C 276, 17.11.2009, s. 8, bod 60.

⁽³⁾ Stanovisko 168 pracovní skupiny zřízené podle článku 29 k budoucnosti soukromí, společný příspěvek ke konzultaci Evropské komise k právnímu rámci pro základní právo na ochranu osobních údajů, přijaté dne 1. prosince 2009.

Soukromí coby aspekt návrhu jako vedoucí zásada v evropské digitální agendě

46. Informační a komunikační technologie jsou stále složitější a nesou s sebou větší rizika pro ochranu soukromí a údajů. Obecně platí, že digitalizované informace, ke kterým lze snadněji přistupovat, kopírovat je a předávat, jsou vystaveny daleko větším rizikům než informace na papíru. Na cestě k sítím vzájemně propojených objektů se tato rizika budou zvyšovat. Čím větší jsou rizika pro ochranu soukromí a údajů, tím větší bude poptávka po vylepšených zárukách ochrany údajů a soukromí. Proto je ospravedlnění potřeby provádění soukromí coby aspektu návrhu závažnější v odvětví IKT. Kromě toho, jak bylo uvedeno výše, důvěra jednotlivců v IKT je zásadní, pokud mají občané přijmout tyto nové služby, a klíčovými prvky této důvěry je ochrana soukromí a údajů.

47. Výše uvedené zdůrazňuje, že strategie pro rozvoj IKT musí potvrdit nutnost, aby tyto technologie byly navrhovány se začleněním prvku ochrany soukromí a údajů, tedy při zohlednění zásady soukromí coby aspekt návrhu.

48. Proto by evropská digitální agenda měla výslovně schválit zásadu soukromí coby aspekt návrhu jako nezbytný prvek pro zajištění důvěry občanů v IKT a on-line služby. Měla by uznat, že soukromí a důvěra jdou ruku v ruce a že soukromí coby aspekt návrhu by mělo být vedoucím faktorem při rozvoji důvěryhodného odvětví IKT.

Soukromí coby aspekt návrhu jako zásada v dalších iniciativách EU

49. Komise by měla zajistit, aby soukromí coby aspekt návrhu bylo vedoucí zásadou při provádění politik, činností a iniciativ ve specifických odvětvích IKT, včetně elektronických aplikací pro zdravotnictví, zadávání veřejných zakázek, sociálního zabezpečení, učení (eHealth, eProcurement, eSocial Security, eLearning) atd. Mnohé z těchto iniciativ budou prováděny v rámci evropské digitální agendy.

50. To například znamená, že iniciativy k zajištění efektivnějších a modernějších aplikací státní správy umožňující vzájemnou komunikaci s fyzickými osobami by měly zahrnovat potřebu jejich navrhování a provozu v souladu se zásadou soukromí coby aspekt návrhu. Totéž platí pro politiky a činnosti Komise, které se zabývají rychlejším internetem, digitálním obsahem nebo celkovou podporou pevné či bezdrátové komunikace a přenosu údajů.

51. Výše uvedené také zahrnuje oblasti, kde je Komise odpovědná za rozsáhlé systémy informační technologie, jako je SIS a VIS, i ty případy, kdy je odpovědnost Komise omezena na rozvoj a údržbu společné infrastruktury takového systému, jako je Evropský informační systém rejstříků trestů (ECRIS).
52. Jak přesně bude rozvinuta zásada soukromí coby aspekt návrhu, bude záviset na každém konkrétním odvětví a situaci. Pokud například iniciativy Komise doprovází návrhy právních předpisů v konkrétním odvětví IKT, bude v mnoha případech vhodné zahrnout výslovný odkaz na tuto zásadu do návrhu konkrétní aplikace nebo systému IKT. Rovněž navržené akční plány pro specifickou oblast by měly systematicky zajišťovat uplatňování právního rámce a konkrétněji zaručit, aby příslušná IKT byla vytvořena při zohlednění zásady soukromí coby aspektu návrhu.
53. Pokud se týká výzkumu, sedmý rámcový program a následující programy by se měly používat jako nástroj pro podporu projektů majících za cíl analýzu norem, IKT a architektury, které lépe slouží ochraně soukromí, a zejm. zásadě soukromí coby aspektu návrhu. Navíc by tato zásada měla také být nezbytným prvkem, který je třeba brát v úvahu u širších projektů IKT, jejichž cílem je zpracovávání osobních údajů fyzických osob.

Oblasti, které vyžadují zvláštní pozornost

54. V důsledku zvláštních rizik pro ochranu soukromí a údajů fyzických osob nebo v důsledku dalších faktorů (jako např. nevěle výrobců poskytovat produkty vycházející ze zásady soukromí coby aspekt návrhu, poptávka spotřebitelů atd.) může být v některých případech nutné vymezit konkrétnější a specifická opatření pro soukromí coby aspekt návrhu, která musí být zapracována do daného typu informačního a komunikačního produktu nebo technologie, a to v legislativních či jiných nástrojích.
55. Evropský inspektor ochrany údajů určil různé oblasti (RFID, aplikace tvorby sociálních sítí a prohlížečů), které si podle jeho názoru v této etapě zasluhují pečlivé zvážení ze strany Komise a praktický přístup nastíněný výše. O těchto třech oblastech je dále pojednáno v následujícím textu.

V. IDENTIFIKACE NA ZÁKLADĚ RÁDIOVÉ FREKVENCE – RFID

56. Štítky RFID mohou být použity u předmětů, zvířat a lidí. Mohou se používat pro sběr a ukládání osobních údajů,

jako jsou lékařské záznamy, ke sledování pohybů lidí nebo tvorbě profilu jejich chování pro různé účely. To vše lze provádět, aniž by o tom fyzická osoba věděla ⁽¹⁾.

57. Pro důvěru veřejnosti v RFID a budoucí internet věcí jsou rozhodující účinné záruky týkající se ochrany údajů, soukromí a všech souvisejících etických aspektů. Pouze pak bude tato technologie schopná přinášet četné ekonomické a společenské přínosy.

V.1 Mezery v použitelném právním rámci ochrany údajů

58. Směrnice o ochraně údajů a směrnice o soukromí a elektronických komunikacích se vztahuje na shromažďování údajů prováděné prostřednictvím aplikací RFID ⁽²⁾. Mezi jiným vyžadují, aby byly zavedeny vhodné záruky ochrany soukromí při provozu aplikací RFID ⁽³⁾.
59. Tento právní rámec se však nezabývá všemi oblastmi vzbuzujícími obavy v oblasti ochrany údajů a soukromí a které přináší tato technologie. Je to tím, že směrnice nejsou dostatečně podrobné, pokud jde o typ ochranných

⁽¹⁾ RFID je zkratkou pro identifikaci na základě rádiové frekvence. Hlavními složkami technologie *nebo* infrastruktury identifikace na základě rádiové frekvence je štítek (tj. mikročip), čtečka a aplikace spojená se štítky a čtečkami prostřednictvím integračního softwaru (middleware) a zpracování generovaných údajů. Štítek se skládá z elektronického obvodu, který ukládá údaje, a antény, která předává údaje prostřednictvím rádiových vln. Čtečka má anténu a demodulátor, který převádí příchozí analogové informace z rádiového spojení na digitální údaje. Tyto informace lze pak zasílat přes síť do databází a na servery za účelem počítačového zpracování.

⁽²⁾ Směrnice o soukromí a elektronických komunikacích odkazuje na RFID v článku 3: „Tato směrnice se vztahuje na zpracování osobních údajů ve spojení s poskytováním veřejně dostupných služeb elektronických komunikací ve veřejných komunikačních sítích ve Společenství, včetně veřejných komunikačních sítí podporujících zařízení pro shromažďování a identifikaci údajů“. To je doplněno bodem odůvodnění 56: „Technologický pokrok umožňuje vývoj nových aplikací na bázi zařízení pro shromažďování a identifikaci údajů, což mohou být bezkontaktní zařízení využívající rádiové frekvence. Například rádiová identifikační zařízení (RFID) využívají rádiové frekvence na zachycení údajů z jedinečně označených štítků, které lze poté přenášet přes stávající komunikační síť. Široké využívání těchto technologií může přinést značné hospodářské a společenské výhody, a významně tak přispět k vnitřnímu trhu, je-li jejich používání pro občany přijatelné. Aby toho bylo dosaženo, je třeba zajistit ochranu základních práv jednotlivců, a zejména práva na soukromí a ochranu údajů. Jsou-li tato zařízení připojena k veřejně přístupným sítím elektronických komunikací nebo využívají-li služby elektronických komunikací jako základní infrastrukturu, měla by se použít příslušná ustanovení směrnice 2002/58/ES (směrnice o soukromí a elektronických komunikacích), včetně ustanovení o bezpečnosti, provozních a lokalizačních údajích a důvěrnosti“.

⁽³⁾ Například článek 17 směrnice o ochraně údajů ukládá povinnost přijmout vhodná technická a organizační opatření na ochranu osobních údajů proti náhodnému nebo nedovolenému zničení nebo neoprávněnému sdělování.

opatření, které by měly být zavedeny u aplikací RFID. Stávající pravidla je třeba doplnit dalšími, která by ukládala konkrétní opatření, a to zejména povinnost zapracovat technická řešení (soukromí coby aspekt návrhu) do RFID technologie. To platí pro štítky, které ukládají osobní informace, jež by měly obsahovat příkazy ke zničení, a pro používání šifrování u štítků, které uchovávají určité typy osobních informací.

V.2 Samoregulace jako první krok

60. V březnu 2007 Komise přijala sdělení⁽¹⁾, kterým mimo jiné uznala potřebu nezbytných pokynů k praktickému provádění RFID a vhodnost přijetí konstrukčních kritérií pro zamezení rizikům pro soukromí a bezpečnost.
61. Pro dosažení těchto cílů Komise v květnu 2009 přijala doporučení o zavedení zásad ochrany soukromí a údajů v RFID aplikacích⁽²⁾. U maloobchodně prodávaných RFID aplikací to vyžaduje deaktivaci štítků v místě prodeje, pokud fyzické osoby neudělily souhlas k jejich používání. Toto pravidlo platí v případě že, zhodnocení dopadu na ochranu soukromí a údajů neprokáže, že štítky pravděpodobně nepředstavují hrozbu pro soukromí nebo ochranu osobních údajů. V takovém případě by štítky zůstaly aktivní s tím, že by se fyzické osoby mohly rozhodnout pro bezplatnou deaktivaci.
62. Evropský inspektor ochrany údajů souhlasí s přístupem Komise použít samoregulační nástroje. Jak je však popsáno níže, lze si představit, že samoregulace nepřinese očekávané výsledky, proto vyzývá Komisi, aby byla připravena přijmout alternativní opatření.

V.3 Problematické oblasti a případná další opatření, pokud samoregulace selže

63. Evropský inspektor ochrany údajů má obavy, že organizace provozující RFID aplikace v maloobchodě mohou přehlédnout možnost, že RFID štítky jsou sledovány nežádoucími třetími stranami. Při takovém sledování může dojít k vyzrazení případných osobních údajů uložených na štítku, ale mohlo by také umožnit třetí straně, aby sledovala nebo časem identifikovala určitou osobu na základě pouhého využití jedinečných identifikátorů obsažených v jednom nebo několika štítcích, které fyzická osoba má při sobě, a to dokonce v prostředí, které je mimo provozní okruh RFID aplikace. Dále má obavy, že provozovatelé RFID aplikací mohou mít tendenci spoléhat

se bez řádného důvodu na výše zmíněnou výjimku, a ponechávat tak provozuschopné štítky i za místem prodeje.

64. Pokud k tomu dojde, může být příliš pozdě na zmírnění rizik pro ochranu údajů a soukromí fyzických osob, které již mohly být postiženy. Navíc když vezmeme v úvahu povahu samoregulace, vnitrostátní donucovací orgány mohou mít slabší postavení, když vyžadují, aby organizace provozující RFID aplikace uplatňovaly konkrétní opatření týkající se soukromí coby aspektu návrhu.
65. Ve světle výše uvedeného evropský inspektor ochrany údajů vyzývá Komisi, aby byla připravena navrhnout právní předpisy regulující hlavní problémy použití RFID v případě, že selže účinné provádění stávajícího právního rámce. Hodnocení Komise by nemělo být bez řádného důvodu odkládáno; odkládání by ohrozilo fyzické osoby a bylo by také kontraproduktivní pro průmysl, protože právní nejistota je příliš vysoká a související problémy by mohly být komplikovanější a jejich náprava nákladnější.
66. V rámci opatření, která bude možná nezbytné navrhnout, evropský inspektor ochrany údajů doporučuje stanovit zásadu rozhodnutí pro deaktivaci v místě prodeje, podle které by všechny RFID štítky, které jsou připojeny ke spotřebním výrobkům, byly standardně deaktivovány v místě prodeje. Nemusí být nutné nebo vhodné, aby Komise stanovila konkrétní technologii, která by měla být použita. Místo toho musí právo Unie stanovit právní povinnost získat souhlas k ponechání aktivace, čímž by se provozovatelům poskytl prostor pro rozhodnutí, jak tomuto požadavku vyhovět.

V.4 Další otázky ke zvážení: Správa internetu věcí

67. Informace generované RFID štítky – například informace o výrobku – mohou být nakonec propojeny do globální sítě komunikační infrastruktury. Tomu se obvykle říká „internet věcí“. S ním vyvstávají otázky ochrany údajů/soukromí, protože předměty reálného světa lze identifikovat pomocí RFID štítků, které kromě informací o výrobku mohou zahrnovat osobní údaje.
68. Existuje mnoho otevřených otázek o tom, kdo bude řídit ukládání informací týkajících se položek opatřených štítky. Jak budou uspořádány? Kdo k nim bude mít přístup? V červnu 2009 Komise přijala sdělení o internetu věcí⁽³⁾, které výslovně zmínilo potenciální problémy ochrany údajů a soukromí spojené s tímto jevem.

⁽¹⁾ Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů ze dne 15.3.2007 o identifikaci na základě rádiové frekvence (RFID) v Evropě: kroky k rámci politiky, KOM(2007) 96 v konečném znění.

⁽²⁾ Doporučení Komise ze dne 12.5.2009 o zavedení zásad ochrany soukromí a údajů v aplikacích podporovaných identifikací na základě rádiové frekvence (C(2009) 3200 v konečném znění).

⁽³⁾ Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů: Internet věcí – akční plán pro Evropu, 18.6.2009, KOM(2009) 278 v konečném znění.

69. Evropský inspektor ochrany údajů by rád zdůraznil některé z otázek zmíněných v tomto sdělení, které si podle jeho názoru s rozvojem internetu věci zaslouhují zvýšenou pozornost. Za prvé potřeba decentralizované architektury může být nápomocná z hlediska odpovědnosti a vynutitelnosti právního rámce EU. Za druhé by mělo být v co největší možné míře zachováno právo fyzické osoby na to, aby sledována. Jinými slovy, měly by existovat jen velmi omezené případy, kdy dochází ke sledování fyzických osob prostřednictvím RFID štítků bez jejich souhlasu. Takový souhlas by měl být výslovný. To se obvykle nazývá „mlčení čipů“ a právo na nerušený soukromý život. A konečně při navrhování internetu věcí by měla být vedoucí zásadou zásada soukromí coby aspekt návrhu. To by například vyžadovalo, aby konkrétní RFID aplikace, které mají zabudované mechanismy pro poskytnutí kontroly uživatelům, byly konstruovány se standardním nastavením ochrany soukromí.

70. Evropský inspektor ochrany údajů očekává, že bude konzultován, jakmile bude Komise zavádět opatření zmíněná v tomto sdělení, a to zejména ohledně návrhu sdělení o soukromí a důvěře ve všudypřítomnou informační společnost.

VI. SOCIÁLNÍ SÍTĚ A POTŘEBA IMPLICITNÍHO NASTAVENÍ SOUKROMÍ

71. Sociální sítě jsou trendem poslední doby, přičemž se zdá, že překonaly popularitu e-mailů. Spojují lidi navzájem na základě podobných zájmů či aktivit. Lidé mohou mít své profily na internetu a sdílet mediální soubory, jako jsou videa, fotografie, hudba, i své profesní profily.

72. Mládež rychle přijala tvorbu sociálních sítí a tento trend pokračuje. Průměrný věk uživatele internetu v Evropě v několika posledních letech poklesl: mladí ve věku 9–10 let se nyní připojují několikrát týdně; mladí ve věku 12–14 let jsou on-line každý den, často po dobu jedné až tří hodin.

VI.1 Sociální sítě a použitelný právní rámec pro ochranu údajů a soukromí

73. Rozvoj sociálních sítí umožnil uživatelům nahrávat na internet informace o nich samotných a o třetích stranách.

Přitom podle pracovní skupiny zřízené podle článku 29 ⁽¹⁾ uživatelé internetu ve vztahu údajům, které nahrávají ⁽²⁾, vystupují jako správci údajů podle čl. 2 písm. d) směrnice o ochraně údajů. Ve většině případů však takové zpracování patří do výjimky pro domácí činnosti podle čl. 3 odst. 2 směrnice. Současně jsou služby tvorby sociálních sítí považovány za správce údajů, pokud poskytují prostředky pro zpracování údajů uživatelů a všechny základní služby týkající se správy uživatelů (např. registraci a vymazání účtů).

74. V právním smyslu to znamená, že uživatelé internetu a služby tvorby sociálních sítí sdílejí společnou odpovědnost za zpracování osobních údajů jako „správci údajů“ ve smyslu čl. 2 písm. d) směrnice, třebaže do různého stupně a při odlišných povinnostech.

75. Podobně by uživatelé měli vědět a chápat, že na základě zpracovávání svých osobních údajů i osobních údajů dalších osob se na ně vztahují ustanovení právních předpisů EU týkající se ochrany údajů, která mimo jiné vyžadují získání informovaného souhlasu osob, jejichž informace jsou nahrávány, a poskytnutí práv na opravu, námitku atp. Také služby tvorby sociálních sítí musí mezi jiným přijmout vhodná technická a organizační opatření pro zabránění nedovoleného zpracování při zohlednění rizik spojených se zpracováním a s povahou údajů. To zase znamená, že služby tvorby sociálních sítí by měly zajistit standardní nastavení, které umožňuje ochranu soukromí, včetně nastavení, které omezuje přístup k profilu na kontakty, které si uživatel sám zvolil. Před tím, než by byl jakýkoli profil přístupný pro jiné třetí strany, by nastavení také vyžadovalo potvrzující souhlas uživatele a profily se zakázaným přístupem by nemělo být možné vyhledat vnitřními vyhledávacími.

76. Bohužel sama existence výše zmíněných právními požadavky nestačí k zajištění jejich dodržování. Přestože jsou uživatelé internetu z právního hlediska považováni za správce údajů a jsou vázáni právním rámcem EU pro ochranu údajů a soukromí, ve skutečnosti často nemají o této úloze žádné povědomí. Obecně nedostatečně rozumí skutečnosti, že zpracovávají osobní údaje a že se zveřejňováním takových informací jsou spojena rizika pro ochranu soukromí a údajů. Zejména mládež zveřejňuje obsah on-line a podceňuje přitom důsledky pro sebe i pro jiné, například v souvislosti s následným studiem nebo žádostmi o pracovní místo.

⁽¹⁾ Viz Stanovisko 163, 5/2009 pracovní skupiny zřízené podle článku 29 k tvorbě internetových sociálních sítí přijaté dne 12. června 2009.

⁽²⁾ „Správcem“ se rozumí fyzická či právnická osoba, veřejný orgán, agentura nebo jakýkoli jiný orgán, který sám nebo společně s jinými rozhoduje o účelech a prostředcích zpracování osobních údajů; kde účely a prostředky zpracování stanoví vnitrostátní zákony nebo předpisy nebo zákony či předpisy Společenství, může být správce nebo specifická kritéria pro jeho jmenování stanoveny vnitrostátním právem nebo právem Společenství.

77. Poskytovatelé sociální sítě současně často předem zavádějí standardní nastavení na základě možnosti netrvat na ochraně soukromí a tím napomáhají poskytování osobních informací. Někteří umožňují, aby profily byly přístupné pro běžné vyhledávače. To vede k otázkám, zda fyzické osoby skutečně souhlasily s poskytnutím údajů i zda sociální sítě vyhovely článku 17 směrnice (popsanému výše), který po nich vyžaduje, aby přijaly vhodná technická a organizační opatření pro zabránění nedovolenému zpracování.

VI.2 Rizika generovaná sociálními sítěmi a navrhované kroky k jejich řešení

78. Výše uvedené vede ke zvýšenému riziku pro ochranu soukromí a údajů fyzické osoby. Vystavuje uživatele internetu a osoby, jejichž údaje byly nahrány, zřejmým porušením jejich ochrany soukromí a údajů.

79. V této souvislosti je otázkou, kterou by se Komise měla zabývat, co by mělo a mohlo být uděláno pro řešení této situace. Toto stanovisko neposkytuje vyčerpávající odpověď na tuto otázku, místo toho předkládá řadu návrhů k dalšímu zvážení.

Investování do vzdělání uživatelů internetu

80. Prvním návrhem je investovat do vzdělání uživatelů. V tomto ohledu by instituce EU a vnitrostátní orgány měly investovat do vzdělávání a zvyšování povědomí o hrozbách, které představují internetové stránky tvorby sociálních sítí. Například generální ředitelství pro informační společnost a média provádí program bezpečnějšího internetu, který má posílit a chránit děti a mládež například prostřednictvím činností ke zvyšování povědomí⁽¹⁾. Instituce EU nedávno zahájily kampaň „Mysli, než něco dáš na net!“ ke zvýšení povědomí o rizicích sdílení osobních informací s cizími lidmi.

81. Evropský inspektor ochrany údajů vyzývá Komisi, aby i nadále podporovala tento typ činnosti. Samotní poskytovatelé sociálních sítí by však také měli hrát aktivní úlohu, protože mají právní a sociální odpovědnost za vzdělávání uživatelů o tom, jak využívat jejich služby bezpečně a při zajištění soukromí.

82. Jak bylo popsáno výše, když jsou informace zveřejňovány na sociálních sítích, mohou být tyto informace implicitně zpřístupněny řadou různých způsobů. Například informace mohou být přístupné pro širokou veřejnost, včetně

vyhledávačů, které je mohou opatřit indexy a poskytovat tak na ně přímé odkazy. Na druhé straně informace mohou být omezeny na „vybrané přátele“ nebo mohou být uchovávány jako zcela soukromé. Je jasné, že povolení profilů a používaná terminologie se liší podle dané sítě.

83. Jak však bylo popsáno výše, velmi málo uživatelů služeb tvorby sociálních sítí má povědomí o tom, jak ovládat přístup na informace, které zveřejňují, tím méně jak měnit standardní nastavení ochrany soukromí. Toto nastavení obvykle zůstává beze změny, protože uživatelé nemají povědomí o jeho dopadech nebo nevědí, jak to udělat. Nezměněné nastavení ochrany soukromí tedy velmi často neznamená, že by fyzické osoby učinily informované rozhodnutí přijmout sdílení informací. V této souvislosti je zejména důležité, aby třetí strany jako vyhledávače neodkazovaly na jednotlivé profily na základě předpokladu, že uživatelé implicitně souhlasili (tím, že nezměnili nastavení soukromí) s neomezeným zpřístupněním informací.

84. I když vzdělání uživatelů může pomoci řešit tuto situaci, nebude fungovat samo o sobě. Jak doporučuje pracovní skupina zřízená podle článku 29 ve svém stanovisku k sociálním sítím, poskytovatelé sociálních sítí by měli standardně a bezplatně nabízet taková nastavení, která zajišťují ochranu soukromí. To by zajistilo větší povědomí uživatelů a umožnilo jim lépe se rozhodovat o tom, zda chtějí sdílet informace a s kým.

Úloha pro samoregulaci

85. Komise uzavřela dohodu s dvaceti poskytovateli sociálních sítí pod názvem Bezpečnější zásady tvorby sociálních sítí pro EU⁽²⁾. Cílem této dohody je zlepšit bezpečnost nezávislých při používání internetových stránek pro tvorbu sociálních sítí v Evropě. Tyto zásady zahrnují mnoho požadavků odvozených z uplatňování právního rámce ochrany údajů popsaného výše. Zahrnují například požadavek posílit postavení uživatelů pomocí technologie s cílem zajistit kontrolu nad využitím a šířením jejich osobních informací. Dohoda zahrnuje také potřebu poskytování standardního nastavení ochrany soukromí.

86. Na začátku ledna 2010 Komise zpřístupnila zprávu hodnotící provádění těchto zásad⁽³⁾. Evropský inspektor ochrany údajů má obavy, že tato zpráva ukazuje, že

⁽¹⁾ Informace o tomto programu jsou dostupné na adrese: http://ec.europa.eu/information_society/activities/sip/index_en.htm

⁽²⁾ Tato dohoda je dostupná na adrese: http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

⁽³⁾ Zpráva o hodnocení provádění Bezpečnějších zásad tvorby sociálních sítí pro EU, dostupná na adrese: http://ec.europa.eu/information_society/activities/social_networking/docs/final_report_first_part.pdf

zatímco některé kroky byly učiněny, mnoho dalších nebylo. Například zpráva zjistila problémy se sdělováním bezpečnostních opatření a nástrojů, které jsou dostupné na internetových stránkách. Zjistila také, že méně než polovina signatářů dohody omezuje přístup k profilům nezletilých pouze na jejich přátele.

Potřeba povinného standardního nastavení ochrany soukromí

87. V této souvislosti je klíčovou otázkou, zda jsou nezbytná další politická opatření, aby se zajistilo, že služby sociálních sítí budou obsahovat standardní nastavení ochrany soukromí. Tento problém zmínila bývalá komisařka pro informační společnost, Viviane Redingová, která zdůraznila, že může dojít k nutnosti regulace ⁽¹⁾. Podobně i Evropský hospodářský a sociální výbor uvedl, že spolu se samoregulací by měly být minimální normy ochrany uloženy závazným právním předpisem ⁽²⁾.

88. Jak bylo poznamenáno výše, povinnost poskytovatelů sociálních sítí zavádět standardní nastavení soukromí lze nepřímo odvodit z článku 17 směrnice o ochraně údajů ⁽³⁾, která ukládá správcům údajů přijmout vhodná technická a organizační opatření („jak při přípravě systému zpracování, tak v průběhu vlastního zpracování“) s cílem zajistit bezpečnost a zabránit neoprávněnému zpracování při zohlednění rizik, která představují zpracování a povaha údajů.

89. Tento článek je však příliš obecný a také v této souvislosti postrádá specifickou. Neuvádí jasně, co je míněno vhodnými technickými a organizačními opatřeními v souvislosti se sociálními sítěmi. Současná situace je tak situací právní nejistoty, což způsobuje problémy pro regulační orgány i fyzické osoby, jejichž soukromí a ochrana údajů nejsou plně chráněny.

90. S ohledem na výše uvedené evropský inspektor ochrany údajů vyzývá Komisi, aby navrhla právní předpisy, které by jako minimum upravovaly obecnou povinnost vyžadující povinné nastavení soukromí spolu s přesnějšími požadavky:

- a) na poskytování nastavení omezujícího přístup k profilům uživatelů na vlastní kontakty zvolené uživatelem. Toto nastavení by také vyžadovalo potvrzující souhlas uživatele před tím, než by byl jakýkoli profil přístupný pro třetí strany;

- b) na zajištění, aby profily s omezeným přístupem nemohly být nalezeny vnitřními a vnějšími vyhledávači.

91. Kromě zajištění povinného standardního nastavení ochrany soukromí zůstává otázkou, zda by také nebyla vhodná další specifická opatření ochrany údajů a jiná opatření (například týkající se ochrany nezletilých). To vede k další otázce, totiž zda by bylo užitečné vytvořit specifický rámec pro tyto typy služeb, který by kromě uložení povinného nastavení soukromí reguloval další aspekty. Evropský inspektor ochrany údajů žádá Komisi, aby tuto otázku zvažila.

VII. STANDARDNÍ NASTAVENÍ OCHRANY SOUKROMÍ U PROHLÍZEČŮ PRO ZARUČENÍ INFORMOVANÉHO SOUHLASU PRO PŘIJÍMÁNÍ REKLAMY

92. Poskytovatelé sítí inzerce využívají cookies a další nástroje pro sledování chování jednotlivých uživatelů, když se pohybují na internetu, s cílem vytvářet seznam jejich zájmů a profily. Tyto informace se pak používají k zasílání cílené reklamy ⁽⁴⁾.

VII.1 Další výzvy a rizika v souvislosti se stávajícím právním rámcem v oblasti ochrany údajů a soukromí

93. Toto zpracování je upraveno ve směrnici o ochraně údajů (pokud se jedná o osobní údaje) a také v čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích. Tento článek konkrétně vyžaduje, aby byl uživatel informován a dostal příležitost reagovat souhlasem nebo odmítnutím týkajícím se ukládání nástrojů, jako jsou cookies atd. na jeho počítač nebo jiná zařízení ⁽⁵⁾.

94. Až dosud provozovatelé reklamní sítě spoléhali na nastavení prohlížečů a na politiky soukromí, aby uživatele informovali a umožnili jim poskytnout souhlas nebo odmítnout cookies. V politikách soukromí vydavatelů

⁽¹⁾ Viviane Redingová, členka Evropské komise odpovědná za informační společnost a média. Myslí, než něco dáš na net! Jak zajistit bezpečnější internetové stránky tvorby sociálních sítí pro děti a dospívající? Den pro bezpečnější internet, Štrasburk 9. února 2010.

⁽²⁾ Stanovisko Evropského hospodářského a sociálního výboru k dopadu internetových stránek sociálních sítí na občany/spotřebitele, 4. listopadu 2009.

⁽³⁾ Podrobněji popsáno také v bodu 33 tohoto dokumentu.

⁽⁴⁾ Cookies pro sledování jsou malé textové soubory, které obsahují jedinečný identifikátor. Poskytovatelé sítí inzerce (stejně jako provozovatelé internetových stránek nebo vydavatelé) obvykle umístí cookies na pevný disk návštěvníka, zejména do prohlížeče uživatelů internetu, když uživatelé poprvé vstoupí na internetové stránky, které nabízejí inzeráty, které jsou součástí jejich sítě. Cookie umožní poskytovateli sítě inzerce poznat dřívějšího návštěvníka, který se na tyto internetové stránky vrací nebo navštíví jakoukoli partnerskou internetovou stránku sítě inzerce. Takové opakované návštěvy umožní poskytovateli sítě inzerce vytvořit profil návštěvníka.

⁽⁵⁾ Čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích byl nedávno změněn, aby posílil ochranu před zachycováním komunikace uživatelů prostřednictvím použití například spywaru a cookies uložených na počítači nebo jiných zařízeních uživatele. Podle nové směrnice by měly být uživatelům nabídnuty lepší informace a snadnější způsoby, jak ovládat, zda chtějí mít cookies uloženy na svém koncovém zařízení.

vysvětlovali, jak úplně zamezit přijímání cookies nebo jak je přijímat případ od případu. Tímto způsobem měli v úmyslu vyhovět své povinnosti nabídnout uživateli právo odmítnout cookies.

95. Zatímco teoreticky by tato metoda (prostřednictvím prohlížeče) mohla skutečně účinně zajistit smysluplný informovaný souhlas, realita je velmi odlišná. Obecně platí, že uživatelé nemají základní ponětí o shromažďování jakýchkoli údajů, tím méně údajů poskytnutých třetími stranami, hodnotě takových údajů, jejich využití, fungování příslušné technologie, a zejména toho, jak a kde zabránit přijímání cookies. Zdá se, že kroky, které musí uživatelé učinit, aby přijímání zabránili, jsou nejen komplikované, ale také nepřiměřené (nejdříve musí nastavit svůj prohlížeč na přijímání cookies, pak provést volbu zabránění přijímání).
96. V důsledku toho v praxi dochází k tomu, že velmi málo lidí provádí volbu zabránění přijímání cookies, nikoli proto, že by učinili informované rozhodnutí přijímat cílenou reklamu, ale spíše proto, že si neuvědomují, že když tuto volbu neprovedou, pak vlastně poskytují souhlas.
97. Zatímco tedy z právního hlediska čl. 5 odst. 3 směrnice o soukromí a elektronických komunikacích stanoví účinnou právní ochranu, v praxi se má za to, že uživatelé internetu souhlasí se sledováním pro účely zasílání reklamy na základě jejich chování, když vlastně v mnoha, ne-li ve většině případů vůbec nevědí o tom, že dochází ke sledování.
98. Pracovní skupina zřízená podle článku 29 připravuje stanovisko s cílem upřesnit právní požadavky pro využívání cílené reklamy, což se vítá. Samotný výklad však nemusí být dostačující pro vyřešení této situace a může být nezbytné, aby Evropská unie učinila další kroky.

VII.2 Potřeba dalšího kroku, zejména stanovení povinného standardního nastavení ochrany soukromí

99. Jak bylo popsáno výše, internetové prohlížeče běžně umožňují určitou úroveň kontroly nad určitými druhy cookies. V současnosti je standardním nastavením většiny internetových prohlížečů přijímat všechny cookies. Jinými slovy, prohlížeče jsou implicitně nastaveny tak, aby přijímaly všechny cookies bez ohledu na účel dané cookie. Pouze pokud uživatel změní nastavení své aplikace prohlížeče tak, aby odmítl cookies, což, jak bylo výše popsáno, provede jen velmi málo uživatelů, nebude cookies přijímat. Navíc neexistuje žádný software pro ochranu soukromí při první instalaci nebo aktualizaci aplikací prohlížečů.
100. Tento problém by šlo zmírnit dodáváním prohlížečů se standardním nastavením ochrany soukromí. Jinými slovy, pokud by prohlížeče byly dodávány s nastavením „nepřijímat cookies třetích stran“. Jako doplnění a účinnější

zajištění by prohlížeče měly vyžadovat, aby při první instalaci nebo aktualizaci prohlížeče uživatelé prošli softwarem pro ochranu soukromí. Existuje potřeba podrobnějších a srozumitelnějších informací o typech cookies a užitečnosti některých z nich. Uživatelé, kteří by byli ochotni být sledováni pro účely přijímání cílené reklamy, by o tom byli řádně informováni a museli by změnit nastavení svého prohlížeče. To by jim poskytlo zvýšenou kontrolu nad jejich osobními údaji a soukromím, což by podle názoru evropského inspektora ochrany údajů bylo účinným způsobem, jak respektovat a zachovat souhlas uživatelů⁽¹⁾.

101. Když vezmeme v úvahu na jedné straně rozšířenost tohoto problému, jinými slovy počet uživatelů internetu, kteří jsou v současnosti sledováni na základě zdánlivého souhlasu, a na druhé straně závažnost dotčeného zájmu, potřeba dalších ochranných opatření se stává ještě naléhavější. Provedení zásady soukromí coby aspekt návrhu u aplikací internetových prohlížečů by mohlo znamenat významný rozdíl při poskytování kontroly ve prospěch fyzických osob nad praktikami shromažďování údajů pro účely cílené.
102. Z těchto důvodů evropský inspektor ochrany údajů naléhá na Komisi, aby zvážila legislativní opatření, která by vyžadovala povinné standardní nastavení ochrany soukromí v prohlížečích a poskytování příslušných informací.

VIII. DALŠÍ ZÁSADY ZAMĚŘENÉ NA OCHRANU SOUKROMÍ / OCHRANU ÚDAJŮ FYZICKÝCH OSOB

103. I když má zásada soukromí coby aspekt návrhu velký potenciál pro zlepšení ochrany osobních údajů a soukromí fyzických osob, je pro zajištění důvěry spotřebitelů v IKT nezbytné zakončení doplňujících zásad v příslušných právních předpisech. V této souvislosti se evropský inspektor ochrany údajů zabývá zásadou odpovědnosti a dokončením právního rámce týkajícího se narušení bezpečnosti, který bude použitelný napříč odvětvími.

VIII.1 Zásada odpovědnosti pro zajištění vyhovění zásadě soukromí coby aspekt návrhu

104. Dokument pracovní skupiny zřízené podle článku 29 pod názvem Budoucnost soukromí⁽²⁾ doporučil, aby byla zásada odpovědnosti zahrnuta do směrnice o ochraně

⁽¹⁾ Evropský inspektor ochrany údajů si současně uvědomuje, že by to tento problém úplně nevyřešilo, protože existují cookies, které nelze ovládat prostřednictvím prohlížeče, jako v případě tak zvaných flash cookies. Pro ně by bylo nutné, aby vývojáři při vydávání nových prohlížečů implicitně začlenili ovládání typu flash do jejich ovládání cookies.

⁽²⁾ Stanovisko 168 pracovní skupiny zřízené podle článku 29 k budoucnosti soukromí, společný příspěvek ke konzultaci Evropské komise k právnímu rámci pro základní právo na ochranu osobních údajů přijaté dne 1. prosince 2009.

údajů. Tato zásada, která je uznávána v některých nadnárodních nástrojích v oblasti ochrany údajů⁽¹⁾, vyžaduje, aby organizace přijaly postupy směřující k respektování stávajících právních předpisů a vytvořily metody pro jejich hodnocení a prokázání.

105. Evropský inspektor ochrany údajů plně podporuje doporučení pracovní skupiny zřízené podle článku 29. Má za to, že tato zásada bude vysoce významná pro podporu účinného uplatňování zásad a povinností týkajících se ochrany údajů. Odpovědnost bude vyžadovat, aby správci údajů prokázali, že zavedli nezbytné mechanismy za účelem zaručení souladu s platnými právními předpisy v oblasti ochrany údajů. To pravděpodobně přispěje k účinnému provádění zásady soukromí coby aspekt návrhu u IKT jako zvláště vhodného prvku pro prokázání odpovědnosti.
106. Pro stanovení a prokázání odpovědnosti by správci údajů mohli využívat vnitřní postupy a třetí strany, které mohou provádět audity nebo jiné typy kontrol a ověření a které by pak na jejich základě mohly udělovat pečetě nebo ceny. V této souvislosti evropský inspektor ochrany údajů vyzývá Komisi, aby zvážila, zda by kromě obecné zásady odpovědnosti bylo užitečné, aby byla stanovena konkrétní opatření jako je potřeba vytvářet hodnocení dopadu ochrany soukromí a údajů a za jakých podmínek.

VIII.2 Narušení bezpečnosti: dokončení právního rámce

107. Loňské změny směrnice o soukromí a elektronických komunikacích zavedly požadavek oznamovat narušení údajů dotčeným fyzickým osobám a také příslušným orgánům. Narušení údajů je široce definováno jako jakékoli narušení, které vede ke zničení, ztrátě, vyrazení atd. osobních údajů přenášených, uchovávaných nebo jinak zpracovávaných v souvislosti se službou. Oznamování fyzickým osobám se bude vyžadovat, pokud by narušení údajů pravděpodobně nepříznivě ovlivnilo jejich osobní údaje nebo soukromí. To by mohlo nastat, jestliže by narušení mohlo vést ke krádeži totožnosti nebo významnému ponížení či poškození pověsti. Oznamování příslušným orgánům bude vyžadováno u každého narušení údajů bez ohledu, zda existuje riziko pro fyzické osoby.

Uplatňování povinností týkajících se narušení bezpečnosti napříč odvětvími

108. Tato povinnost se bohužel vztahuje pouze na poskytovatele veřejně přístupných služeb elektronických komunikací, jako jsou telefonní společnosti, poskytovatelé přístupu na internet, poskytovatelé internetových stránek atd. Evropský inspektor ochrany údajů vyzývá Komisi, aby předložila návrhy týkající se narušení bezpečnosti, které

by se uplatňovaly napříč odvětvími. Pokud se jedná o obsah takového rámce, evropský inspektor ochrany údajů má za to, že právní rámec týkající se narušení bezpečnosti přijatý ve směrnici o soukromí a elektronických komunikacích nalézá vhodnou rovnováhu mezi ochranou práv fyzických osob, včetně jejich práv na ochranu osobních údajů a soukromí, a povinnostmi, které se ukládají výše zmíněným subjektům. Současně se jedná o efektivní právní rámec, protože se opírá o smysluplná donucovací ustanovení, která poskytují orgánům dostatečné pravomoci provádět šetření a ukládat sankce.

109. Evropský inspektor ochrany údajů také vyzývá Komisi, aby přijala návrh právního předpisu, který by podle potřeby s vhodnými úpravami uplatňoval tento rámec napříč odvětvími. Navíc by to zajistilo, že jsou napříč odvětvími uplatňovány stejné normy a postupy.

Dokončení právního rámce obsaženého ve směrnici o soukromí a elektronických komunikacích prostřednictvím projednávání ve výboru

110. Revidovaná směrnice o soukromí a elektronických komunikacích zmocňuje Komisi, aby přijala technická prováděcí opatření, tj. podrobná opatření týkající se oznamování narušení bezpečnosti prostřednictvím postupu projednávání ve výboru⁽²⁾. Toto zmocnění je odůvodněno nutností zajistit jednotné provádění a uplatňování příslušného právního rámce. Jednotné provádění má za cíl zajistit, aby fyzické osoby v celém Společenství měly stejně vysokou úroveň ochrany a aby výše zmíněné subjekty nebyly zatěžovány odlišnými požadavky na oznamování.
111. Směrnice o soukromí a elektronických komunikacích byla přijata v listopadu 2009. Zdá se, že neexistuje žádný důvod, který by ospravedlňoval odkládání zahájení činnosti směřující k přijetí technických prováděcích opatření. Evropský inspektor ochrany údajů uspořádal dva semináře zaměřené na sdílení a sběr zkušeností o oznamování při narušení údajů. Rád by se podělil o výsledky těchto akcí a těší se na spolupráci s Komisí a dalšími zainteresovanými stranami při vyladování celkového právního rámce týkajícího se narušení údajů.
112. Evropský inspektor ochrany údajů vyzývá Komisi, aby v krátkém časovém horizontu učinila nezbytné kroky. Před přijetím technických prováděcích opatření se Komise musí zapojit do širokých konzultací zahrnujících ENISA, evropského inspektora ochrany údajů a pracovní skupinu zřízenou podle článku 29. Tyto konzultace musí dále zapojovat další „příslušné zainteresované strany“, zejména s cílem získání informací o nejlepších dostupných technických a ekonomických prostředcích provedení.

⁽¹⁾ Pokyny OHSR z roku 1980 k ochraně soukromí a přeshraničním tokům osobních údajů; Madridská deklarace o soukromí: Globální normy soukromí pro globální svět ze dne 3. listopadu 2009.

⁽²⁾ Projednávání ve výboru zahrnuje přijetí technických prováděcích opatření prostřednictvím výboru zástupců členských států, kterému předsedá Komise. Na směrnici o soukromí a elektronických komunikacích se vztahuje tak zvaný regulativní postup s kontrolou, což znamená, že Evropský parlament i Rada se mohou postavit proti opatřením navrženým Komisí. Další podrobnosti naleznete na adrese: http://europa.eu/scadplus/glossary/comitology_en.htm

IX. ZÁVĚRY

113. Důvěra nebo spíše její nedostatek byl určen jako základní problém pro vznik a úspěšné zavádění informačních a komunikačních technologií. Pokud by lidé neměli důvěru v IKT, tyto technologie by selhaly. Důvěra v IKT závisí na různých faktorech, přičemž klíčovým faktorem je zajištění, že tyto technologie nebudou poškozovat základní práva fyzických osob na soukromí a ochranu osobních údajů.

114. Aby došlo k dalšímu posílení právního rámce ochrany údajů a soukromí jako zásad, které zůstávají v informační společnosti zcela platné, evropský inspektor ochrany údajů navrhuje Komisi, aby na různých úrovních tvorby právních předpisů a politiky začlenila zásadu soukromí coby aspekt návrhu.

115. Evropský inspektor ochrany údajů navrhuje Komisi provést čtyři následující kroky:

- a) navrhnout zahrnutí obecného ustanovení o soukromí coby aspektu návrhu do právního rámce ochrany údajů. Toto ustanovení by mělo být neutrální z hlediska technologie a jeho respektování by mělo být povinné v různých etapách;
- b) podrobně rozpracovat toto obecné ustanovení ve specifických ustanoveních, až budou navrženy konkrétní právní nástroje v různých odvětvích. Tato specifická ustanovení by již nyní mohla být zahrnuta do právních nástrojů, a to na základě článku 17 směrnice o ochraně údajů (a dalších právních předpisů);
- c) zahrnout soukromí coby aspekt návrhu jako vedoucí zásadu do evropské digitální agendy;
- d) zavést soukromí coby aspekt návrhu jako zásadu do dalších iniciativ EU (hlavně jiné než legislativní povahy).

116. U tří určených oblastí IKT evropský inspektor ochrany údajů doporučuje Komisi, aby zhodnotila potřebu předložit návrhy, které by prováděly zásadu soukromí coby aspekt návrhu konkrétními způsoby:

a) ve vztahu k RFID navrhnout právní opatření regulující hlavní problémy použití RFID v případech, že selže účinné provádění stávajícího právního rámce prostřednictvím samoregulace. Zejména stanovit zásadu rozhodnutí pro aktivaci v místě prodeje, podle které by všechny RFID štítky, které jsou připojeny ke spotřebním výrobkům, byly standardně deaktivovány v místě prodeje;

b) ve vztahu k sociálním sítím navrhnout právní předpisy, které by jako minimum zahrnovaly širokou povinnost vyžadující povinné nastavení ochrany soukromí spolu s přesnějšími požadavky o omezení přístupu k profilům uživatelů na vlastní kontakty zvolené uživatelem a stanovení, že profily s omezeným přístupem nemohou být nalezeny vnitřními a vnějšími vyhledávači;

c) ve vztahu k cílené reklamě zvážit právní předpisy ukládající nastavení prohlížečů, které by standardně odmítalo přijímání cookies třetích stran a vyžadovalo, aby uživatelé při první instalaci nebo aktualizaci prohlížeče prošli softwarem pro ochranu soukromí.

117. A konečně evropský inspektor ochrany údajů doporučuje Komisi, aby:

- a) zvážila provedení zásady odpovědnosti ve stávající směrnici o ochraně údajů a
- b) vytvořila rámec pravidel a postupů pro provedení ustanovení o oznamování narušení bezpečnosti ve směrnici o soukromí a elektronických komunikacích a rozšířila je tak, aby se vztahovala na všechny správce údajů.

V Bruselu dne 18. března 2010.

Peter HUSTINX
evropský inspektor ochrany údajů

Stanovisko evropského inspektora ochrany údajů k návrhu směrnice Evropského parlamentu a Rady o odpadních elektrických a elektronických zařízeních (OEEZ)

(2010/C 280/02)

EVROPSKÝ INSPEKTOR OCHRANY ÚDAJŮ,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na článek 16 této smlouvy,

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

s ohledem na směrnici Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, a zejména na článek 17 této směrnice,

s ohledem na nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů, a zejména na článek 41 tohoto nařízení,

PŘIJAL TOTO STANOVISKO:

I. ÚVOD

1. Dne 3. prosince 2008 přijala Komise návrh směrnice Evropského parlamentu a Rady o odpadních elektrických a elektronických zařízeních (OEEZ), (dále jen „návrh“) ⁽¹⁾. Cílem návrhu je přepracování směrnice 2002/96/ES o odpadních elektrických a elektronických zařízeních (OEEZ) přijaté dne 27. ledna 2003 (dále jen „směrnice“) ⁽²⁾ beze změny jak pohnutek, tak důvodů pro sběr a recyklaci OEEZ.
2. Evropský inspektor ochrany údajů nebyl konzultován, jak vyžaduje čl. 28 odst. 2 nařízení (ES) č. 45/2001 ⁽³⁾. Z vlastní iniciativy proto evropský inspektor ochrany údajů na základě čl. 41 odst. 2 téhož nařízení přijal toto stanovisko. Evropský inspektor ochrany údajů doporučuje, aby byl odkaz na toto stanovisko zahrnut do preambule návrhu.

⁽¹⁾ KOM(2008) 810 v konečném znění.

⁽²⁾ Úř. věst. L 37, 13.2.2003, s. 24.

⁽³⁾ 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.

3. Evropský inspektor ochrany údajů si je vědom skutečnosti, že jeho doporučení přicházejí v pozdní fázi legislativního procesu, přesto však považuje za vhodné a užitečné toto stanovisko vydat, neboť návrh vyvolává závažné otázky týkající se ochrany údajů, kterým se text návrhu nevěnuje. Toto stanovisko si neklade za cíl měnit hlavní účel a obsah návrhu, jehož „těžiště“ ⁽⁴⁾ zůstává v ochraně životního prostředí, ale pouze vnést další rozměr, který se pro naši informační společnost stává stále důležitějším ⁽⁵⁾.

4. Evropský inspektor ochrany údajů si je také vědom omezené působnosti postupu přepracování, přesto naléhavě vyzývá zákonodárce, aby tato doporučení zohlednil v souladu s bodem 8 interinstitucionální dohody o postupu přepracování (který stanoví možnost změny dalších ustanovení) ⁽⁶⁾.

II. SOUVISLOSTI A POZADÍ NÁVRHU A JEHO RELEVANCE PRO OCHRANU ÚDAJŮ

5. Účelem návrhu je aktualizovat stávající směrnici týkající se odstraňování, opětovného použití a recyklace OEEZ. Technické, právní a administrativní problémy v prvních letech provádění směrnice vedly k vypracování návrhu, jak se předpokládalo v čl. 17 odst. 5 směrnice.
6. Elektrické a elektronické zařízení (EEZ) je širokou skupinou výrobků, která zahrnuje rozmanitý soubor médií schopných ukládat osobní údaje – jako jsou zařízení informačních technologií a telekomunikační zařízení (např. osobní počítače, notebooky, elektronické komunikační terminály) – charakterizované v současných technickoekonomických souvislostech stále rychlejšími inovačními cykly a díky sbližování technologií rovněž dostupností víceúčelových přístrojů. Rozvoj elektronických úložných médií se prudce zrychluje, zejména ve vztahu k úložné kapacitě a velikosti,

⁽⁴⁾ Viz Rozsudek Soudního dvora ze dne 23.2.1999, C-42/97 *Evropský parlament – Rada Evropské unie*, Sb. rozh. 1999, s. I 869, odst. 43.

⁽⁵⁾ Viz také mezi jiným Rozsudek soudního dvora ze dne 30.1.2001, C-36/98 *Španělsko – Rada*, Sb. rozh. 2001, s. I 779, odst. 59: „Pokud přezkum aktu Společenství ukazuje, že tento akt sleduje dvojí účel nebo že má dvě složky, a pokud jeden z těchto účelů nebo jednu z těchto složek je možno identifikovat jako hlavní nebo převažující, zatímco druhý nebo druhá je pouze vedlejší, musí být akt založen na jediném právním základu, a sice na tom, který si vyžaduje hlavní nebo převažující účel nebo složka“.

⁽⁶⁾ Interinstitucionální dohoda ze dne 28. listopadu 2001 o systematictějšímu využívání metody přepracování právních aktů, Úř. věst. C 77, 28.3.2002, s. 1.

a proto tržní síly způsobují, že se obrat EEZ (obsahujících velká množství často citlivých osobních údajů) zrychluje podobným způsobem. Výsledkem je nejen to, že OEEZ „se považuje za nejrychleji rostoucí tok odpadů v EU“ (7), ale i to, že také v případě nevhodného odstraňování dochází k očividnému zvýšenému riziku ztráty a šíření osobních údajů uložených na tomto typu EEZ.

7. Politiky o životním prostředí a udržitelném rozvoji Evropské unie se po dlouhou dobu zaměřovaly na snižování plýtvání přírodními zdroji a zavádění opatření pro zamezení znečištění.
8. Do tohoto rámce je zahrnuto odstraňování, opětovné použití a recyklace OEEZ. Cílem těchto opatření je zabránit odstraňování elektrického a elektronického zařízení spolu se smíšeným odpadem a uložit výrobcům povinnost zajistit odstraňování způsobem, který předepisuje směrnice.
9. Z nejrůznějších opatření stanovených směrnicí stojí za zdůraznění zejména ta opatření, která jsou určena k *opětovnému použití* (tj. jakýkoli způsob, kterým jsou OEEZ nebo jejich konstrukční části použity k témuž účelu, pro který byly určeny, včetně dalšího použití zařízení nebo jeho konstrukčních částí, které byly vráceny do sběrných míst, distributorům, k recyklaci nebo výrobcům), *recyklaci* (tj. přepracování odpadních materiálů ve výrobním procesu pro původní nebo pro jiné účely) a nalezení dalších forem využití OEEZ ke snížení odstraňování odpadu (viz článek 1 a čl. 3 písm. d) a písm. e) směrnice).
10. Tyto operace, zejména opětovné použití a recyklace OEEZ, zvláště zařízení informačních technologií a telekomunikační zařízení, mohou ve větší míře než v minulosti představovat riziko, že ti, kteří shromažďují OEEZ nebo prodávají a nakupují použité nebo recyklované přístroje, by mohli získat povědomí o jakýchkoli v nich uložených osobních údajích. Takové údaje mohou být často citlivé nebo odkazovat na velké počty fyzických osob.
11. Ze všech těchto důvodů evropský inspektor ochrany údajů zastává názor, že je naléhavě důležité, aby byly všechny zainteresované strany (uživatelé a výrobci EEZ) informovány o rizicích týkajících se osobních údajů, a to zejména v závěrečné fázi cyklu životnosti EEZ. I když jsou EEZ hospodářsky méně hodnotná, v této fázi budou

pravděpodobně obsahovat velké množství osobních údajů, a proto bude pravděpodobné, že budou mít vysokou „vnitřní“ hodnotu pro subjekty údajů a/nebo další osoby.

III. ANALÝZA NÁVRHU

III.1 Použitelnost směrnice 95/46/ES

12. Evropský inspektor ochrany údajů nemá žádné připomínky k obecnému cíli návrhu a plně podporuje přijatou iniciativu, která má zlepšit politiku příznivé pro životní prostředí v oblasti OEEZ.
13. Návrh se však stejně jako směrnice zaměřuje pouze na rizika pro životní prostředí související s odstraňováním OEEZ. Nebere v úvahu další rizika pro fyzické osoby a/nebo organizace, která mohou vyplývat z operací odstraňování, opětovného použití nebo recyklace OEEZ, zejména těch, které se týkají pravděpodobnosti nesprávného nabytí, vyzrazení nebo šíření osobních údajů uložených na OEEZ.
14. Je důležité poznamenat, že směrnice 95/46/ES (8) se vztahuje na „jakýkoli úkon nebo soubor úkonů s osobními údaji“, včetně jejich „výmazu nebo likvidace“ (čl. 2 písm. b)). Odstraňování EEZ může zahrnovat úkony zpracování údajů. Z toho důvodu dochází k překrývání mezi návrhem a právě zmíněnou směrnicí, a proto by se pravidla ochrany údajů mohla vztahovat na činnosti zahrnuté do návrhu.

III.2 Odstraňování OEEZ a bezpečnostní opatření

15. Evropský inspektor ochrany údajů má v úmyslu zdůraznit významná rizika, která mohou mít dopad na fyzické osoby a/nebo organizace působící jako „správci údajů“ (9), když v době odstraňování OEEZ, zejména zařízení informačních technologií a telekomunikační zařízení, obsahují osobní údaje jejich uživatelů a/nebo třetích osob. Neoprávněný přístup nebo vyzrazení takových osobních informací, které někdy představují zvláštní kategorie údajů odhalující rasový nebo etnický původ, politické názory, náboženské nebo filozofické přesvědčení, odborovou příslušnost, jakož i údaje týkající se zdraví nebo sexuálního života (tzv. „citlivé údaje“) (10), může skutečně narušit soukromí a důstojnost osob, kterých se tyto informace týkají, i další oprávněné zájmy těchto fyzických osob/organizací (např. hospodářské zájmy).

(7) Viz Pracovní dokument útvarů Komise připojený k návrhu směrnice Evropského parlamentu a Rady o odpadních elektrických a elektronických zařízeních (OEEZ), (přepracování). Posouzení dopadů, 3.12.2008 (KOM(2008) 810 v konečném znění) SEK(2008) 2933, s. 17.

(8) Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, Úř. věst. L 281, 23.11.1995, s. 31.

(9) Definice „správce“ viz čl. 2 písm. d) směrnice 95/46/ES.

(10) Viz článek 8, směrnice 95/46/ES.

16. Evropský inspektor ochrany údajů má obecně za to, že je nutné zdůraznit význam přijetí vhodných bezpečnostních opatření v každé fázi (od počátku do konce) zpracování osobních údajů, jak se opakovaně uvádí v jiných stanoviscích⁽¹¹⁾. To platí *a fortiori* v citlivé fázi, ve které má správce údajů v úmyslu provést likvidaci přístrojů obsahujících osobní údaje.
17. Dodržování bezpečnostních opatření je skutečně často nutnou podmínkou pro účinné zaručení práva na ochranu osobních údajů.
18. Proto by bylo nedůsledné uložit povinnost zavádět (někdy nákladná) bezpečnostní opatření při běžných operacích zpracování osobních údajů (jak se předpokládá v článku 17 směrnice 95/46/ES, když je použitelný⁽¹²⁾) a poté jednoduše opominout úvahu o zavedení přiměřených ochranných prostředků týkajících se odstraňování OEEZ.
19. Podobně nedůsledné by bylo přikládat důležitost otázce bezpečnosti údajů do rozsahu, do kterého muselo být prostřednictvím článku 3 směrnice 2009/136/ES⁽¹³⁾ zavedeno oznamování o narušení bezpečnosti, a pak neposkytnout žádnou záruku nebo ochranu při odstraňování, opětovného použití nebo recyklace OEEZ.
20. Evropský inspektor ochrany údajů vyjadřuje politování, že návrh nebere v úvahu potenciálně škodlivý dopad odstraňování OEEZ na ochranu osobních údajů uložených na „použitém“ zařízení.
21. Tento aspekt také nebyl zohledněn v posouzení dopadů provedeném Komisí⁽¹⁴⁾, ačkoli zkušenost ukázala, že
- nepřijetí vhodných bezpečnostních opatření v případě odstraňování OEEZ by mohlo ohrozit ochranu osobních údajů⁽¹⁵⁾. Vzhledem ke složitosti dotčených otázek (například velkému počtu povolených metod, technologií a zúčastněných stran v cyklu odstraňování OEEZ) je evropský inspektor ochrany údajů toho názoru, že by u procesů odstraňování OEEZ bylo vhodné provést „posouzení dopadů na soukromí a ochranu údajů“.
22. Evropský inspektor ochrany údajů nicméně důrazně doporučuje, aby v této oblasti byly vyvinuty „nejlepší dostupné techniky“ pro soukromí, ochranu údajů a bezpečnost.
23. Jako další důkaz je možné považovat skutečnost, že v průběhu veřejné konzultace před přepracováním směrnice zainteresované strany, zejména společnosti z oblasti informačních technologií a elektronických komunikací občas zmiňovaly otázky týkající se bezpečnosti a ochrany osobních údajů⁽¹⁶⁾.
24. Na závěr je třeba zdůraznit, že některé vnitrostátní úřady ochrany údajů zveřejnily pokyny pro minimalizaci rizik, která by mohla vzniknout, pokud by nebyla přijata nezbytná bezpečnostní opatření, zejména při odstraňování materiálů, na které se vztahuje směrnice⁽¹⁷⁾.
- ⁽¹¹⁾ Viz např. internetový článek BBC „Children's files on eBay computer“ (Soubory dětí na počítači na eBay), 4. května 2007, ve kterém se uvádí, že na eBay byl prodán počítač obsahující osobní údaje o pěstounské péči a adopci dětí (http://news.bbc.co.uk/2/hi/uk_news/england/6627265.stm); viz také internetový článek BBC „Bank customer data sold on eBay“ (Na eBay prodány údaje zákazníků bank), 26. srpna 2008, ve kterém se uvádí, že na eBay byl prodán pevný disk obsahující osobní údaje jednoho milionu zákazníků bank (http://news.bbc.co.uk/2/hi/uk_news/7581540.stm).
- ⁽¹²⁾ Viz HP, Konzultace zainteresovaných stran o přezkoumání směrnice Evropského parlamentu a Rady 2002/96/ES o odpadních elektrických a elektronických zařízeních (OEEZ), s. 7–8; DELL (návrh připomínek), Možnosti přezkoumání politik OEEZ při konzultaci zainteresovaných stran o přezkoumání směrnice Evropského parlamentu a Rady 2002/96/ES o odpadních elektrických a elektronických zařízeních (OEEZ), s. 2, bod 1.1. a 4, bod 1.3. (3.6.2008); Postoj a návrh Royal Philips Electronics, Konzultace zainteresovaných stran o revizi směrnice OEEZ, s. 12 (5.6.2008) (http://circa.europa.eu/Public/irc/env/weee_2008_review/library). Viz také Odpověď na konzultace o OEEZ, Shrnutí odpovědí a odpověď vlády na čtvrtou konzultaci o provádění směrnic 2002/96/ES a 2003/108/ES o odpadních elektrických a elektronických zařízeních, prosinec 2006, s. 30: „Data protection and security. Some waste management companies would like there to be some guidance issued on data protection and security, particularly in light of the fact they will be handling sensitive data“ (Ochrana údajů a bezpečnost. Některé společnosti z oblasti řízení odpadů by chtěly, aby byl vydán nějaký pokyn o ochraně údajů a bezpečnosti, zejména s ohledem na skutečnost, že budou nakládat s citlivými údaji), (<http://www.berr.gov.uk/files/file35961.pdf>).
- ⁽¹³⁾ Směrnice Evropského parlamentu a Rady 2009/136/ES ze dne 25. listopadu 2009, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování zákonů na ochranu zájmů spotřebitele, Úř. věst. L 337, 18.12.2009, s. 11.
- ⁽¹⁴⁾ Pracovní dokument útvarů Komise připojený k návrhu směrnice Evropského parlamentu a Rady o odpadních elektrických a elektronických zařízeních (OEEZ) (přepracování), SEK(2008) 2933, 3.12.2008, ale viz Univerzita Organizace spojených národů, Přezkoumání směrnice 2002/96/ES o odpadních elektrických a elektronických zařízeních (OEEZ) v roce 2008, Evropská komise, Belgie, 2007, s. 273 (http://ec.europa.eu/environment/waste/weee/pdf/final_rep_unu.pdf); „Data security is also an issue — removing personal data from a hard-drive“ (Bezpečnost údajů je také otázkou – odstranění osobních údajů z pevného disku).
- ⁽¹⁵⁾ Landesbeauftragter für Datenschutz und Informationsfreiheit Bremen, Entwicklung eines Konzeptes zur Löschung und Datenträggvernichtung durch Behörden und Unternehmen, 16. Mai 2007 (<http://www.datenschutz-bremen.de/rtf/datenloeschung.rtf>); Garante per la protezione dei dati personali, Elektrický a elektronický odpad a ochrana údajů, 13. října 2008, (<http://www.garanteprivacy.it/garante/doc.jsp?ID=1583482>), zmíněno také ve Dvanácté výroční zprávě pracovní skupiny pro ochranu údajů zřízené podle článku 29, 16. června 2009, s. 57; viz také Mezinárodní pracovní skupina pro ochranu údajů a telekomunikace, Doporučení o ochraně údajů a e-odpadu, Sofie 12–13.3.2009 (<http://www.datenschutz-berlin.de/attachments/650/675.38.14.pdf?1264671551>).

25. Evropský inspektor ochrany údajů opakuje, že směrnice 95/46/ES je použitelná ve fázi odstraňování OEEZ obsahujících osobní údaje. Správci údajů, zejména ti, kteří používají IT přístroje a komunikační přístroje, proto musí vyhovět svým povinnostem týkajícím se bezpečnosti, aby zabránili neoprávněnému vyzrazení nebo šíření osobních údajů. Za tím účelem a s cílem vyhnout se odpovědnosti za porušení bezpečnostních opatření, by správci údajů ve veřejném nebo soukromém sektoru ve spolupráci s inspektory ochrany údajů (kde jsou přítomni) měli přijmout vhodné politiky pro odstraňování OEEZ obsahujících osobní údaje.

26. Když správci údajů, kteří odstraňují OEEZ, nemají požadované dovednosti a/nebo technické know-how, jak vymazat dotčené osobní údaje, mohou svěřit tento úkol kvalifikovaným zpracovatelům (např. asistenčním centrům, výrobcům a distributorům zařízení), a to za podmínek uvedených v čl. 17 odst. 2, 3 a 4 směrnice 95/46/ES. Tito zpracovatelé pak ověří výkon daných operací a/nebo je provedou.

27. Na základě těchto úvah evropský inspektor ochrany údajů dochází k závěru, že přepracování směrnice by mělo přidat zásady ochrany údajů do ustanovení věnovaných ochraně životního prostředí.

28. Evropský inspektor ochrany údajů proto doporučuje, aby Rada a Evropský parlament zahrnuly do současného návrhu konkrétní ustanovení, které by uvádělo, že směrnice se vztahuje na odstraňování OEEZ, aniž by byla dotčena směrnice 95/46/ES.

III.3 Opětovné použití nebo recyklace OEEZ a bezpečnostní opatření

29. Vzhledem k tomu, že osoby odpovědné za operace odstraňování jsou v situaci, která jim umožňuje přijímat nezávislá rozhodnutí týkající se údajů uložených na EEZ, mohou být považovány za „správce údajů“⁽¹⁸⁾. Musí proto přijmout vnitřní postupy k zamezení zbytečným operacím zpracování jakýchkoli osobních údajů uložených na OEEZ,

zejména jiným operacím než těm, které jsou výhradně nutné pro ověření účinného odstranění údajů, které OEEZ obsahují.

30. Navíc nesmí umožnit fyzickým osobám bez oprávnění, aby získaly znalosti o údajích uložených na EEZ nebo aby je zpracovávaly. Zejména když jsou úložná média recyklována nebo opětovně použita a vstupují tak znovu na trh, dochází ke zvýšenému riziku neoprávněného vyzrazení nebo šíření osobních údajů a tím k potřebě zabránit neoprávněnému přístupu k osobním údajům.

31. Evropský inspektor ochrany údajů proto doporučuje Radě a Evropskému parlamentu, aby do stávajícího návrhu zahrnuly konkrétní ustanovení s cílem zakázat uvádění na trh použitých přístrojů, u kterých před tím nebyla uplatněna vhodná bezpečnostní opatření v souladu s moderními technickými normami (např. opakovaného přepisování) za účelem vymazání veškerých osobních údajů, které mohou obsahovat.

III.4 Soukromí a bezpečnost „coby aspekt návrhu“

32. Budoucí právní rámec o elektronickém odpadu by neměl jen zahrnovat konkrétní ustanovení týkající se širší „zásady ekodesignu“ zařízení (viz článek 4 návrhu týkající se „návrhu výrobku“), ale také, jak bylo dříve zmíněno v jiných stanoviscích evropského inspektora ochrany údajů⁽¹⁹⁾, zásadu „soukromí coby aspekt návrhu“⁽²⁰⁾ nebo v této oblasti přesněji zásadu „bezpečnost coby aspekt návrhu“⁽²¹⁾. Soukromí a ochrana údajů by měly být v co možná nejvyšší míře „implicitně“ začleněny do návrhu elektrického a elektronického zařízení s cílem umožnit uživateli v případě odstranění přístrojů vymazat osobní údaje, které se na nich mohou vyskytovat, a to při využití jednoduchých prostředků a zdarma⁽²²⁾.

⁽¹⁹⁾ Viz např. Evropský inspektor ochrany údajů a vědecký a technický rozvoj EU, politický dokument, 28. dubna 2008, s. 2; stanovisko evropského inspektora ochrany údajů k zavádění inteligentních dopravních systémů (Úř. věst. C 47, 25.2.2010, s. 6); stanovisko evropského inspektora ochrany údajů k farmakovigilanci (Úř. věst. C 229, 23.9.2009, s. 19).

⁽²⁰⁾ Ve prospěch širokého uplatnění zásady viz Pracovní skupina pro ochranu údajů zřízená podle článku 29 – Pracovní skupina pro policii a spravedlnost, Budoucnost soukromí. Společný příspěvek ke konzultaci Evropské komise o právním rámci pro základní právo na ochranu osobních údajů, WP 168, přijato dne 1. prosince 2009, s. 3 a 12; viz také Doporučení Komise o zavedení zásad ochrany soukromí a údajů v aplikacích podporovaných identifikací na základě rádiové frekvence, K(2009) 3200 v konečném znění, s. 8.

⁽²¹⁾ Viz Sdělení Komise, Evropský program výzkumu a inovací v oblasti bezpečnosti – prvotní postoj Komise ke klíčovým zjištěním a doporučením fóra pro evropský výzkum a inovace v oblasti bezpečnosti, KOM(2009) 691 v konečném znění, s. 6 a 14.

⁽²²⁾ Viz také Evropský inspektor ochrany údajů, stanovisko ze dne 18. března 2010 k propagaci důvěry v informační společnost podporou ochrany údajů a soukromí.

⁽¹⁸⁾ „The concept of controller is [...] functional, in the sense that it is intended to allocate responsibilities where the factual influence is, and thus based on a factual rather than a formal analysis“ (Koncept správce je [...] funkční ve smyslu, že má přidělit odpovědnost tam, kde je faktický vliv, a vychází tak z faktické spíše než formální analýzy): viz Pracovní skupina pro ochranu údajů zřízená podle článku 29, WP 169, Stanovisko 1/2010 ke konceptům „správce“ a „zpracovatele“, přijaté dne 16. února 2010.

33. Tento přístup jasně podporuje čl. 3 odst. 3 písm. c) směrnice 1999/5/ES⁽²³⁾ o návrhu rádiových a telekomunikačních koncových zařízení a článek 14 odst. 3 směrnice 2002/58/ES⁽²⁴⁾.

34. Proto by výrobci měli „zabudovat“ ochranu soukromí a bezpečnosti prostřednictvím technologických řešení⁽²⁵⁾. V tomto rámci by také měly být propagovány a podporovány iniciativy informování dotčených osob o potřebě vymazat veškeré osobní údaje před odstraněním OEEZ (včetně výrobců, kteří vytvářejí bezplatný software, který je k dispozici pro tyto účely)⁽²⁶⁾.

IV. ZÁVĚRY

35. Při zohlednění výše uvedeného evropský inspektor ochrany údajů doporučuje, aby orgány ochrany údajů, zejména prostřednictvím pracovní skupiny zřízené podle článku 29 a evropský inspektor ochrany údajů byly úzce zapojeny do iniciativ týkajících se odstraňování OEEZ, a to prostřednictvím konzultací v dostatečně rané fázi před vytvořením příslušných opatření.

36. Při zohlednění souvislostí, ve kterých jsou zpracovávány osobní údaje, evropský inspektor ochrany údajů doporučuje, aby návrh obsahoval konkrétní ustanovení, které:

— uvádí, že směrnice o OEEZ se uplatňuje, aniž by byla dotčena směrnice 95/46/ES,

— zakazuje uvádění na trh použitých přístrojů, u kterých před tím nebyla uplatněna vhodná bezpečnostní

opatření v souladu s moderními technickými normami za účelem vymazání veškerých osobních údajů, které mohou obsahovat,

— pokud se jedná o zásadu „soukromí coby aspekt návrhu“ nebo „bezpečnost coby aspekt návrhu“ stanoví, že: soukromí a ochrana údajů by v co možná nejvyšší míře měly být „implicitně“ začleněny do návrhu elektrického a elektronického zařízení s cílem umožnit uživateli v případě odstranění přístrojů vymazat osobní údaje, které se na nich mohou vyskytovat, a to při využití jednoduchých prostředků a zdarma.

37. Evropský inspektor ochrany údajů proto důrazně doporučuje, aby návrh byl v souladu se směrnicí 95/46/ES změněn takto:

— Bod odůvodnění 11: „Tato směrnice by se měla použít, aniž by byly dotčeny právní předpisy o ochraně údajů, zejména směrnice 95/46/ES. Vzhledem k tomu, že elektrické a elektronické zařízení (EEZ) je širokou skupinou výrobků, která zahrnuje rozmanitý soubor médií schopných ukládat osobní údaje (jako jsou zařízení informačních technologií a telekomunikační zařízení), operace odstraňování, které se k nim vztahují, zejména opětovné použití a recyklace, mohou představovat riziko neoprávněného přístupu k osobním údajům uloženým na OEEZ. Proto by do návrhu elektrického a elektronického zařízení umožňujícího ukládání osobních údajů měla být v co možná nejvyšší míře“ implicitně „začleněna opatření na ochranu soukromí a ochranu údajů s cílem umožnit uživatelům jednoduše a zdarma vymazat veškeré takové údaje existující v době jeho odstranění.“

— Čl. 2 odst. 3: „Tato směrnice se použije, aniž jsou dotčeny právní předpisy o ochraně údajů, zejména směrnice 95/46/ES.“

38. Kromě toho Evropský inspektor ochrany údajů považuje za vhodné, aby byly zohledněny tyto změny:

— čl. 4 odst. 2: „Členské státy podpoří opatření podporující návrhy a výrobu elektrického a elektronického zařízení, které napomáhá vymazání veškerých osobních údajů obsažených v EEZ v době jeho odstranění“,

— čl. 8 odst. 7: „Členské státy zajistí, aby veškerá shromážděná OEEZ, která obsahují osobní údaje a která jsou podrobena úpravě s cílem recyklace nebo opětovného použití, nebyla uváděna na trh, pokud takové údaje nebyly nejdříve odstraněny za použití nejlepších dostupných technik“,

⁽²³⁾ Viz čl. 3 odst. 3 směrnice Evropského parlamentu a Rady 1999/5/ES ze dne 9. března 1999 o rádiových zařízeních a telekomunikačních koncových zařízeních a vzájemném uznávání jejich shody (Úř. věst. L 91, 7.4.1999, s. 10): „[...] Komise může rozhodnout, aby přístroje v určitých třídách zařízení nebo přístroje určitých typů byly konstruovány takovým způsobem [...] zajišťujícím ochranu osobních údajů a soukromí uživatele a účastníka“.

⁽²⁴⁾ „V případě potřeby lze přijmout opatření, aby bylo zajištěno, že koncové zařízení je sestaveno tak, že odpovídá právu uživatelů na ochranu a kontrolu využití jejich osobních údajů v souladu se směrnicí 1999/5/ES a rozhodnutím Rady 87/95/EHS ze dne 22. prosince 1986 o normalizaci v oblasti informačních technologií a telekomunikací“. Viz také bod odůvodnění 46 stejné směrnice zmíněný v poznámce pod čarou 13.

⁽²⁵⁾ Viz také ve prospěch této politické perspektivy V. Redingová, Hlavní projev v Den ochrany osobních údajů, 28. ledna 2010, Evropský parlament, Brusel, SPEECH/10/16: „Businesses must use their power of innovation to improve the protection of privacy and personal data from the very beginning of the development cycle. Privacy by Design is a principle that is in the interest of both citizens and businesses. Privacy by Design will lead to better protection for individuals, as well as to trust and confidence in new services and products that will in turn have a positive impact on the economy. I have seen some encouraging examples, but much more needs to be done“. (Podniky musí využívat své síly inovace ke zlepšení ochrany soukromí a osobních údajů od samého začátku rozvojového cyklu. Soukromí coby aspekt návrhu je zásada, která je v zájmu občanů i podniků. Soukromí coby aspekt návrhu povede k lepší ochraně fyzických osob i k důvěře v nové služby a výrobky, která zase povede ke kladnému dopadu na hospodářství. Existují některé povzbudivé příklady, ale je třeba udělat ještě daleko více).

⁽²⁶⁾ Viz například, Royal Canadian Mounted Police, B2-002 — IT Media Overwrite and Secure Erase Products (Přepisování médií informační technologie a výrobky pro bezpečné vymazání), (05/2009), na adrese: <http://www.rcmp-grc.gc.ca/ts-st/pubs/it-ti-sec/index-eng.htm>

- čl. 14 odst. 6: „Členské státy mohou požadovat, aby uživatelé EEZ obsahujícího osobní údaje obdrželi od výrobců a/nebo distributorů informace týkající se potřeby vymazání osobních údajů, které mohou být obsaženy v EEZ před jeho odstraněním, a to např. v pokynech pro použití nebo v místě prodeje“.

V Bruselu dne 14. dubna 2010.

Peter HUSTINX
Evropský inspektor ochrany údajů

II

(Sdělení)

SDĚLENÍ ORGÁNŮ, INSTITUCÍ A JINÝCH SUBJEKTŮ EVROPSKÉ UNIE

EVROPSKÁ KOMISE

Povolení státní podpory podle ustanovení článků 107 a 108 SFEU**Případy, k nimž Komise nevznáší námitku**

(Text s významem pro EHP, kromě produktů, na něž se vztahuje příloha I Smlouvy)

(2010/C 280/03)

Datum přijetí rozhodnutí	6.7.2010
Odkaz na číslo státní pomoci	N 42/10
Členský stát	Finsko
Region	—
Název (a/nebo jméno příjemce)	Tuki maataloustuotannon lopettamiseen
Právní základ	Laki maatalouden harjoittamisesta luopumisen tukemisesta (612/2006), sellaisena kuin se on viimeksi muutettuna lailla (1787/2009); Valtioneuvoston asetus maatalouden harjoittamisesta luopumisen tukemisesta (25/2007).
Název opatření	Podpora na předčasný odchod do důchodu
Cíl	Rozvoj odvětví
Forma podpory	Přímá dotace
Rozpočet	184 milionů EUR
Míra podpory	proměnlivá
Délka trvání programu	1.1.2011–31.12.2014
Hospodářská odvětví	Prvovýroba zemědělských produktů
Název a adresa orgánu poskytujícího podporu	Maa- ja metsätalousministeriö PL 30 FI-00023 Valtioneuvosto Helsinki SUOMI/FINLAND
Další informace	—

Rozhodnutí v autentickém znění po odstranění všech informací, jež jsou předmětem obchodního tajemství, najdete na adrese:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_cs.htm

Datum přijetí rozhodnutí	20.7.2010
Odkaz na číslo státní pomoci	N 131/10
Členský stát	Bulharsko
Region	—
Název (a/nebo jméno příjemce)	Държавна помощ за компенсирание на загуби, понесени от селскостопанските производители в напълно опустошени райони вследствие на природни бедствия или неблагоприятни климатични условия (нотификация на изменение)
Právní základ	Чл. 12, ал. 1, т. 2 и чл. 12, ал. 2, т. 1, буква „а“ от Закона за подпомагане на земеделските производители, ДВ 58/98 Указания за предоставяне на държавна помощ за компенсирание на загуби в следствие на природни бедствия и неблагоприятни климатични условия
Název opatření	Režim podpory
Cíl	Nepříznivé povětrnostní podmínky, přírodní katastrofy nebo mimořádné události.
Forma podpory	Přímá dotace
Rozpočet	Celkový rozpočet: 600 mil. BGN
Míra podpory	80 %
Délka trvání programu	Do 31.12.2013
Hospodářská odvětví	Zemědělství
Název a adresa orgánu poskytujícího podporu	Държавен фонд „Земеделие“ Бул. „Цар Борис III“ № 136 1618 София/Sofia БЪЛГАРИЯ/BULGARIA
Další informace	—

Rozhodnutí v autentickém znění po odstranění všech informací, jež jsou předmětem obchodního tajemství, najdete na adrese:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_cs.htm

Datum přijetí rozhodnutí	9.7.2010
Odkaz na číslo státní pomoci	N 133/10
Členský stát	Itálie
Region	Provincia autonoma di Bolzano
Název (a/nebo jméno příjemce)	Disciplina degli aiuti regionali in materia di foreste
Právní základ	Legge Provinciale del 21.10.1996 «Ordinamento Forestale» decreto del Presidente della Giunta provinciale 31 luglio 2000, n. 29 Regolamento all'ordinamento forestale 2000; Programma di sviluppo rurale 2007-2013, misure 111, 122, 123 settore Foreste, 125 Settore Foreste, 226, 227
Název opatření	Režim podpory
Cíl	Podpora odvětví lesnictví
Forma podpory	Přímá dotace

Rozpočet	Celková maximální částka: 30 milionů EUR
Míra podpory	Nejvýše 100 % způsobilých nákladů
Délka trvání programu	2010–2013
Hospodářská odvětví	Odvětví lesnictví
Název a adresa orgánu poskytujícího podporu	Provincia Autonoma di Bolzano Ripartizione Foreste Ufficio economia montana Via Brennero 6 39100 Bolzano BZ ITALIA
Další informace	—

Rozhodnutí v autentickém znění po odstranění všech informací, jež jsou předmětem obchodního tajemství, najdete na adrese:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_cs.htm

Datum přijetí rozhodnutí	4.6.2010
Odkaz na číslo státní pomoci	N 148/10
Členský stát	Itálie
Region	Provincia autonoma di Trento
Název (a/nebo jméno příjemce)	Ricostituzione del potenziale forestale e interventi preventivi
Právní základ	Piano di sviluppo rurale della Provincia autonoma di Trento 2007-2013 (Misura 226)
Název opatření	Režim podpory
Cíl	Podpora odvětví lesnictví
Forma podpory	Přímá dotace
Rozpočet	Roční maximální výdaje: 3,25 milionu EUR Celková maximální částka: 13 milionů EUR
Míra podpory	Až do výše 100 % způsobilých nákladů
Délka trvání programu	Do 31.12.2013
Hospodářská odvětví	Odvětví lesnictví
Název a adresa orgánu poskytujícího podporu	Provincia autonoma di Trento Piazza Dante 5 38122 Trento TN ITALIA
Další informace	Neuplatňuje se

Rozhodnutí v autentickém znění po odstranění všech informací, jež jsou předmětem obchodního tajemství, najdete na adrese:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_cs.htm

Datum přijetí rozhodnutí	17.6.2010
Odkaz na číslo státní pomoci	N 209/10
Členský stát	Francie
Region	Départements de Charente-Maritime, Vendée et Gironde
Název (a/nebo jméno příjemce)	Aides aux exploitants agricoles victimes des inondations marines causées par la tempête Xynthia du 28 février 2010.
Právní základ	— Articles L 361-1 et s. du code rural (le budget nécessaire aux aides d'État affectées à ce dispositif sera prélevé sur le fonds national de garantie des calamités agricoles). — Articles 1511-2 à 1511-6 du code général des collectivités territoriales et L 3231-2 et suivants pour les aides des collectivités territoriales. — Arrêté interministériel du 1^{er} mars 2010 de reconnaissance de catastrophe naturelle. — Arrêté interministériel du 11 mars 2010 de reconnaissance de catastrophe naturelle.
Název opatření	Režim podpory
Cíl	Podpora určená na kompenzaci škod v oblasti zemědělské produkce
Forma podpory	Přímá dotace
Rozpočet	Maximálně 43 000 000 EUR
Míra podpory	Maximálně 60 %
Délka trvání programu	4 roky
Hospodářská odvětví	Zemědělství
Název a adresa orgánu poskytujícího podporu	Ministère de l'alimentation, de l'agriculture et de la pêche 78 rue de Varenne 75349 Paris 07 SP FRANCE
Další informace	—

Rozhodnutí v autentickém znění po odstranění všech informací, jež jsou předmětem obchodního tajemství, najdete na adrese:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_cs.htm

Povolení státní podpory podle ustanovení článků 107 a 108 SFEU**Případy, k nimž Komise nevznáší námitku**

(Text s významem pro EHP, kromě produktů, na něž se vztahuje příloha I Smlouvy)

(2010/C 280/04)

Datum přijetí rozhodnutí	16.7.2010
Odkaz na číslo státní pomoci	N 414/09
Členský stát	Francie
Region	—
Název (a/nebo jméno příjemce)	Aides de l'Agence de l'eau Artois-Picardie aux engagements agro-environnementaux dans le bassin Artois Picardie (EAEAP)
Právní základ	Loi n° 2006-1772 du 30 décembre 2006 sur l'eau et les milieux aquatiques (JORF n° 303 du 31 décembre 2006). Proposition de dispositif pour des aides agro-environnementales de l'agence de l'eau Artois-Picardie.
Název opatření	Režim podpory
Cíl	Podpora na agro-environmentální opatření
Forma podpory	Přímá dotace
Rozpočet	Roční výdaje: 21,33 milionu EUR Celkový rozpočet: 64 milionů EUR
Míra podpory	Maximálně do 100 % způsobilých nákladů
Délka trvání programu	2010–2012
Hospodářská odvětví	Zemědělství
Název a adresa orgánu poskytujícího podporu	Agence de l'eau Artois-Picardie 200 rue Marceline BP 818 59508 Douai FRANCE
Další informace	—

Rozhodnutí v autentickém znění po odstranění všech informací, jež jsou předmětem obchodního tajemství, najdete na adrese:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_cs.htm

Datum přijetí rozhodnutí	3.2.2010
Odkaz na číslo státní pomoci	N 582/09
Členský stát	Itálie
Region	Sardegna
Název (a/nebo jméno příjemce)	Ristrutturazione dell'azienda «Cooperativa viticoltori della Planargia»

Právní základ	Legge regionale 19 gennaio 1998, n. 4 «Interventi a favore di aziende agricole in difficoltà» Legge regionale 29 maggio 2007, n. 2 «Legge finanziaria 2007» — articolo. 21 Decreto dell'Assessore n. 2532/DecA/105 del 13.10.2009
Název opatření	Jednotlivá podpora
Cíl	Restrukturalizace podniku v obtížích
Forma podpory	Přímá dotace
Rozpočet	294 540 EUR
Míra podpory	75 %
Délka trvání programu	Po schválení podpory Komisí
Hospodářská odvětví	Zemědělství (odvětví vína)
Název a adresa orgánu poskytujícího podporu	Assessorato dell'agricoltura e riforma agro-pastorale Via Pessagno 4 09126 Cagliari CA ITALIA
Další informace	—

Rozhodnutí v autentickém znění po odstranění všech informací, jež jsou předmětem obchodního tajemství, najdete na adrese:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_cs.htm

Datum přijetí rozhodnutí	20.7.2010
Odkaz na číslo státní pomoci	NN 26/10
Členský stát	Česká republika
Region	—
Název (a/nebo jméno příjemce)	Vrácení části spotřební daně na pohonné hmoty spotřebované při zemědělské produkci (změna režimu podpory č. N 678/07)
Právní základ	Zákon č. 353/2003 Sb., o spotřebních daních, ve znění pozdějších předpisů Vyhláška 48/2008 Sb., o způsobu výpočtu nároku na vrácení spotřební daně zaplacené v cenách některých minerálních olejů spotřebovaných v zemědělské prvovýrobě
Název opatření	Režim podpory
Cíl	Podpora související s osvobozením od daně podle směrnice 2003/96/ES
Forma podpory	Daňové zvýhodnění
Rozpočet	Celkem: 6 800 milionů CZK (přibližně 272 milionů EUR) Ročně: 1 700 milionů CZK (přibližně 68 milionů EUR)
Míra podpory	60 % způsobilých výdajů
Délka trvání programu	Do 31. prosince 2013

Hospodářská odvětví	Odvětví zemědělství
Název a adresa orgánu poskytujícího podporu	Ministerstvo zemědělství Těšnov 17 117 05 Praha 1 ČESKÁ REPUBLIKA
Další informace	—

Rozhodnutí v autentickém znění po odstranění všech informací, jež jsou předmětem obchodního tajemství, najdete na adrese:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_cs.htm

Datum přijetí rozhodnutí	16.7.2010
Odkaz na číslo státní pomoci	N 213/10
Členský stát	Estonsko
Region	—
Název (a/nebo jméno příjemce)	Eesti maaelu arengukava 2007–2013 meede 2.7 „Natura 2000 toetus erametsamaale“
Právní základ	Eesti maaelu arengukava 2007–2013, peatükk 5.3.2.2; Põllumajandusministri 11.3.2010. aasta määrus nr 26 „Natura 2000 alal asuva erametsamaa kohta antava toetuse saamise nõuded, toetuse taotlemise ja taotluse menetlemise täpsem kord“; Euroopa Liidu ühise põllumajanduspoliitika rakendamise seadus.
Název opatření	Podpora v odvětví lesnictví
Cíl	Lesnictví
Forma podpory	Přímá dotace
Rozpočet	Celkový rozpočet ve výši 326 milionů EEK (přibližně 20,8 milionu EUR)
Míra podpory	Až do výše 100 % způsobilých nákladů
Délka trvání programu	Od data rozhodnutí Komise do 31. prosince 2013
Hospodářská odvětví	Lesnictví
Název a adresa orgánu poskytujícího podporu	Põllumajanduse Registrite ja Informatsiooni Amet Narva 3 51009 Tartu EESTI/ESTONIA
Další informace	—

Rozhodnutí v autentickém znění po odstranění všech informací, jež jsou předmětem obchodního tajemství, najdete na adrese:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_cs.htm

Povolení státní podpory podle ustanovení článků 107 a 108 SFEU**Případy, k nimž Komise nevznáší námitku****(Text s významem pro EHP, kromě produktů, na něž se vztahuje příloha I Smlouvy)****(2010/C 280/05)**

Datum přijetí rozhodnutí	12.8.2010
Odkaz na číslo státní pomoci	N 83/10
Členský stát	Itálie
Region	Sardegna
Název (a/nebo jméno příjemce)	Aiuto alla ristrutturazione a favore dell'Unione Pastori Società Cooperativa Agricola, registrata nella Z.I Taccu — Nurri Cagliari
Právní základ	Legge regionale 19 gennaio 1998 «Interventi a favore delle aziende agricole in difficoltà» Articolo 21 della legge regionale 29 maggio 2007, n. 2 Decreto regionale n. 343/DecA/7 del 4 febbraio 2010
Název opatření	Jednotlivá podpora
Cíl	Restrukturalizace podniku střední velikosti
Forma podpory	Přímá dotace
Rozpočet	1 milion EUR
Míra podpory	33,3 % z celkových nákladů na restrukturalizaci (3 miliony EUR)
Délka trvání programu	Podpora <i>ad hoc</i>
Hospodářská odvětví	Zemědělství
Název a adresa orgánu poskytujícího podporu	Regione Autonoma Sardegna Assessorato dell'Agricoltura Via Pessagno 4 09125 Cagliari CA ITALIA
Další informace	—

Rozhodnutí v autentickém znění po odstranění všech informací, jež jsou předmětem obchodního tajemství, najdete na adrese:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_cs.htm

Povolení státní podpory podle ustanovení článků 107 a 108 SFEU**Případy, k nimž Komise nevznáší námitku****(Text s významem pro EHP, kromě produktů, na něž se vztahuje příloha I Smlouvy)****(2010/C 280/06)**

Datum přijetí rozhodnutí	7.4.2010
Odkaz na číslo státní pomoci	N 716/09
Členský stát	Řecko
Region	Περιοχές που επλήγησαν από τις πυρκαγιές του 2009
Název (a/nebo jméno příjemce)	Πρόγραμμα κρατικών οικονομικών ενισχύσεων για την αντιστάθμιση ζημιών από πυρκαγιές έτους 2009
Právní základ	Σχέδιο ΚΥΑ για τη λήψη μέτρων υπέρ των παραγωγών της χώρας των οποίων οι γεωργοκτηνοτροφικές τους εκμεταλλεύσεις ζημιώθηκαν από πυρκαγιές κατά το έτος 2009
Název opatření	Νάहरα škod za ztráty na prostředcích zemědělské produkce způsobené výjimečnou událostí
Cíl	Вýjimečné události
Forma podpory	Пřímá dotace
Rozpočet	Celkový rozpočet ve výši 8 000 000 EUR
Míra podpory	Nárok na podporu mají producenti, kteří utrpěli škodu v výši nejméně 30 %. Intenzita podpory závisí na povaze poškozeného objektu a pohybuje se mezi 50 %–80 %.
Délka trvání programu	Ode dne schválení režimu podpory do 31. prosince 2013.
Hospodářská odvětví	Земědělství
Název a adresa orgánu poskytujícího podporu	α. Υπουργείο Αγροτικής Ανάπτυξης και Τροφίμων Αχαρνών 2 101 76 Αθήνα/Athens ΕΛΛΑΔΑ/GREECE β. ΕΛΓΑ Μεσογείων 45 115 10 Αθήνα/Athens ΕΛΛΑΔΑ/GREECE
Další informace	—

Rozhodnutí v autentickém znění po odstranění všech informací, jež jsou předmětem obchodního tajemství, najdete na adrese:

http://ec.europa.eu/community_law/state_aids/state_aids_texts_cs.htm

IV

(Informace)

INFORMACE ORGÁNŮ, INSTITUCÍ A JINÝCH SUBJEKTŮ EVROPSKÉ UNIE

EVROPSKÁ KOMISE

Směnné kurzy vůči euru ⁽¹⁾

15. října 2010

(2010/C 280/07)

1 euro =

měna	směnný kurz	měna	směnný kurz
USD americký dolar	1,4089	AUD australský dolar	1,4142
JPY japonský jen	114,28	CAD kanadský dolar	1,4165
DKK dánská koruna	7,4564	HKD hongkongský dolar	10,9300
GBP britská libra	0,87750	NZD novozélandský dolar	1,8565
SEK švédská koruna	9,2230	SGD singapurský dolar	1,8244
CHF švýcarský frank	1,3423	KRW jihokorejský won	1 564,64
ISK islandská koruna		ZAR jihoafrický rand	9,5833
NOK norská koruna	8,0925	CNY čínský juan	9,3568
BGN bulharský lev	1,9558	HRK chorvatská kuna	7,3355
CZK česká koruna	24,515	IDR indonéská rupie	12 530,82
EEK estonská koruna	15,6466	MYR malajsijský ringgit	4,3443
HUF maďarský forint	274,18	PHP filipínské peso	60,847
LTL litevský litas	3,4528	RUB ruský rubl	42,5650
LVL lotyšský latas	0,7097	THB thajský baht	42,015
PLN polský zlotý	3,9050	BRL brazilský real	2,3369
RON rumunský lei	4,2765	MXN mexické peso	17,4580
TRY turecká lira	1,9808	INR indická rupie	62,1320

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

ROZHODNUTÍ KOMISE

ze dne 14. října 2010

o znovuzřízení skupiny na vysoké úrovni pro konkurenceschopnost a udržitelný růst automobilového průmyslu v Evropské unii – CARS 21

(2010/C 280/08)

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie,

vzhledem k těmto důvodům:

- (1) Článek 173 Smlouvy o fungování Evropské unie ukládá Evropské unii a členským státům úkol zajistit podmínky nezbytné pro konkurenceschopnost průmyslu Unie. Článek 191 Smlouvy stanoví, že politika Unie v oblasti životního prostředí přispívá k zachování, ochraně a zlepšování kvality životního prostředí a boji proti změně klimatu.
- (2) Proces CARS 21 („Systém právní úpravy pro konkurenceschopnost automobilového průmyslu ve 21. století“), který byl jako součást průmyslové politiky Komise původně zahájen v roce 2005, přinesl doporučení pro krátkodobou, střednědobou a dlouhodobou veřejnou politiku v rámci právní úpravy pro automobilový průmysl v Evropské unii, který zvyšuje globální konkurenceschopnost a zaměstnanost a zároveň podporuje další pokrok v oblasti bezpečnosti a ochrany životního prostředí za cenu, která je pro spotřebitele přijatelná.
- (3) Komise ve svém sdělení „EVROPA 2020 – Strategie pro inteligentní a udržitelný růst podporující začlenění“⁽¹⁾ předkládá návrhy na modernizaci dopravy a snížení produkce uhlíku v tomto sektoru a podporu nových technologií včetně elektromobilů. Cílem stěžejní iniciativy „Průmyslová politika pro věk globalizace“ je vytvořit průmyslovou politiku, která připraví to nejlepší prostředí pro udržení a rozvoj silné, konkurenceschopné a diverzifikované průmyslové základny v Evropě, a prosazovat udržitelnost podporou přechodu výrobních odvětví k větší účinnosti využívání energie a zdrojů. Stěžejní iniciativa „Evropa méně náročná na zdroje“ podpoří rozsáhlá opatření v oblasti infrastruktury, jako je zavádění síťových infrastruktur pro elektrickou mobilitu, inteligentní řízení dopravy a především podpora nových technologií včetně elektromobilů a hybridních automobilů.
- (4) Sdělení Komise „Evropská strategie pro čistá a energeticky účinná vozidla“⁽²⁾ vytyčuje střednědobé až dlouhodobé cíle pro podporu výzkumu a inovace, hledání řešení v oblasti výroby a distribuce energie, stimulaci zaměstnanosti a podporu zájmu spotřebitelů o ekologická vozidla.

- (5) Proto je nutné na základě procesu CARS 21 zřídit skupinu odborníků pro oblast konkurenceschopnosti a udržitelného růstu automobilového průmyslu v Evropské unii a definovat její úkoly a strukturu.
- (6) Skupina by měla pomáhat při stanovování strategií a opatření, které posílí konkurenceschopnost a udržitelný růst automobilového průmyslu v Evropské unii a které budou uskutečněny na úrovni Evropské unie, na vnitrostátní úrovni a ostatními zúčastněnými stranami.
- (7) Skupinu by měli tvořit zástupci Evropského parlamentu, Komise, členských států a příslušných zúčastněných stran z průmyslu a občanské společnosti, zejména zástupci spotřebitelů, odborů a nevládních organizací.
- (8) Měla by být stanovena pravidla týkající se zveřejňování informací ze strany členů skupiny, aniž by byla dotčena bezpečnostní pravidla Komise uvedená v příloze rozhodnutí Komise 2001/844/ES, ESUO, Euratom ze dne 29. listopadu 2001, kterým se mění její jednací řád⁽³⁾.
- (9) Osobní údaje by se měly zpracovávat podle 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⁽⁴⁾.
- (10) Je vhodné stanovit období použitelnosti tohoto rozhodnutí. Komise včas zváží účelnost jeho prodloužení,

ROZHODLA TAKTO:

Článek 1

Skupina

Znovu se zřizuje skupina na vysoké úrovni pro konkurenceschopnost a udržitelný růst automobilového průmyslu v Evropské unii (dále jen „skupina“), která dříve existovala na neformálním základě jako „Systém právní úpravy pro konkurenceschopnost automobilového průmyslu ve 21. století“.

⁽¹⁾ KOM(2010) 2020.⁽²⁾ KOM(2010) 186.⁽³⁾ Úř. věst. L 317, 3.12.2001, s. 1.⁽⁴⁾ Úř. věst. L 8, 12.1.2001, s. 1.

Článek 2

Úkoly

Úkolem skupiny je:

- 1) napomáhat Komisi v otázkách týkajících se konkurenceschopnosti a udržitelného růstu automobilového průmyslu;
- 2) provádět ekonomickou a statistickou analýzu faktorů určujících strukturální změny v automobilovém průmyslu a rovněž dalších faktorů, které ovlivňují konkurenceschopnost automobilového průmyslu Evropské unie;
- 3) pomáhat Komisi s prováděním politiky stanovené strategií EVROPA 2020, její stěžejní iniciativou týkající se Evropy méně náročné na zdroje, její stěžejní iniciativou týkající se průmyslové politiky pro věk globalizace a sdělením o čistých a energeticky účinných vozidlech (KOM(2010) 186), aby byl dosažen cíl zachovat konkurenceschopný a udržitelný automobilový průmysl Evropské unie;
- 4) přispívat k zajištění hladkého a vyváženého hospodářského a sociálního přechodu, prostřednictvím aktivního předvídání a řízení procesů restrukturalizace, potřebných dovedností a souvisejících potřebných kvalifikací, s ohledem na výsledky „Evropského partnerství pro předvídání změn v automobilovém průmyslu“;
- 5) formulovat soubor strategických doporučení pro toto odvětví, určených tvůrcům politik na úrovni Evropské unie a na vnitrostátní úrovni, a také průmyslu a organizacím občanské společnosti;
- 6) rozvíjet zásady řádného chování, aby byla podporována transparentnost obchodních a smluvních vztahů mezi stranami vertikálních dohod v odvětví motorových vozidel;
- 7) poskytovat poradenství ohledně specifických hledisek provádění strategie Komise pro inteligentní a udržitelný růst podporující začlenění – EVROPA 2020.

Článek 3

Členství – jmenování členů

1. Skupina má nejvýše 40 členů.
2. Členové jsou jednotlivci jmenovaní za svou osobu. Každý člen jmenuje osobního zástupce do stálé přípravné podskupiny (dále jen „přípravná podskupina“).
3. Členy skupiny jmenuje Komise z řad zúčastněných stran na vysoké úrovni s odbornými znalostmi a zodpovědností v oblastech, které mají vztah ke konkurenceschopnosti a udržitelnému růstu automobilového průmyslu EU. Složení skupiny odpovídá vyváženému zastoupení různých zúčastněných stran. Skupinu by měli tvořit zástupci Evropského parlamentu, Komise, členských států, aktérů, kteří jsou součástí průmyslového hodnotového řetězce, odborů a občanské společnosti (nevládních organizací a spotřebitelů).

4. Členové jsou jmenováni na dva roky. Ve funkci zůstávají, dokud nejsou nahrazeni, nebo do konce svého funkčního období. Jejich funkční období lze prodloužit.

5. Členové, kteří již nejsou schopni účinně přispívat k práci skupiny, kteří odstoupí nebo kteří nesplňují podmínky stanovené v článku 339 Smlouvy, mohou být na zbývající část svého funkčního období nahrazeni.

6. Jména jednotlivců jmenovaných za svou osobu se zveřejní v rejstříku skupin odborníků a ostatních podobných subjektů Komise (dále jen „rejstřík“).

7. Osobní údaje se shromažďují, zpracovávají a zveřejňují v souladu s nařízením (ES) č. 45/2001.

Článek 4

Fungování skupiny

1. Skupině předsedá zástupce Komise.
2. Přípravná podskupina připravuje jednání, zprávy o postojích a konzultace k činnosti a strategickým opatřením, které má skupina doporučit. K tomuto účelu úzce spolupracuje s příslušnými útvary Komise.
3. Skupina může na základě dohody s útvary Komise zřídit kromě přípravné podskupiny i pracovní skupiny, které se budou zabývat specifickými otázkami souvisejícími s úkoly skupiny, a to na základě mandátu stanoveného skupinou. Tyto pracovní skupiny budou rozpuštěny, jakmile splní své pověření.
4. Zástupce Komise může *ad hoc* přizvat k práci ve skupině nebo podskupině odborníky nebo pozorovatele se zvláštní odborností týkající se určitého předmětu, kteří běžně ve skupině nebo podskupině nepracují. Zástupce Komise může navíc udělit status pozorovatele jednotlivcům, organizacím stanoveným v pravidle 8(3) horizontálních pravidel pro skupiny odborníků, agenturám EU a přistupujícím zemím.

5. Členové skupin odborníků a jejich zástupci, jakož i přizvaní odborníci a pozorovatelé splňují povinnost profesního tajemství stanovenou Smlouvami a jejich prováděcími pravidly, jakož i bezpečnostní předpisy Komise o ochraně utajovaných skutečností EU stanovené v příloze rozhodnutí 2001/844/ES, ESUO, Euratom. Pokud členové tyto povinnosti nedodržují, může Komise přijmout veškerá vhodná opatření.

6. Informace získané při účasti na jednáních nebo práci skupiny, skupin *ad hoc* či podskupin nesmějí být sdělovány, pokud se Komise domnívá, že se týkají důvěrných záležitostí.

7. Skupiny, přípravné podskupiny a pracovní skupiny zasedají v prostorách Komise. Komise zajišťuje sekretářské služby. Jednání skupiny, přípravné podskupiny a pracovních skupin se mohou účastnit další úředníci Komise, kteří mají zájem na projednávání otázkách.

8. Skupina přijme svůj jednací řád na základě vzorového jednacího řádu přijatého Komisí ⁽¹⁾.

9. Komise zveřejňuje příslušné informace o činnosti skupiny jejich umístěním buď v rejstříku nebo na určené internetové stránce dostupné odkazem z rejstříku. Závěrečná zpráva se zveřejní co nejdříve po závěrečném zasedání skupiny.

Článek 5

Výdaje na zasedání

1. Účastníkům podílejícím se na činnostech skupiny nepřísluší za poskytované služby odměna.

2. Cestovné a náklady na pobyt vzniklé účastníkům v souvislosti s činností skupiny hradí Komise v souladu s předpisy platnými v rámci Komise.

3. Tyto náklady se nahrazují v mezích disponibilních prostředků, které jsou přiděleny v rámci ročního postupu pro přidělení zdrojů.

Článek 6

Použitelnost

Toto rozhodnutí se použije do dne 14. října 2012.

V Bruselu dne 14. října 2010.

Za Komisi
Antonio TAJANI
místopředseda

⁽¹⁾ Úř. věst. L 55/61, 5.3.2010, s. 61.

V

(Oznámení)

ŘÍZENÍ TÝKAJÍCÍ SE PROVÁDĚNÍ POLITIKY HOSPODÁŘSKÉ SOUTĚŽE

EVROPSKÁ KOMISE

Předběžné oznámení o spojení podniků**(Věc COMP/M.5927 – BASF/Cognis)****(Text s významem pro EHP)**

(2010/C 280/09)

1. Komise dne 8. října 2010 obdržela oznámení o navrhovaném spojení podle článku 4 nařízení Rady (ES) č. 139/2004 ⁽¹⁾, kterým podnik BASF SE („BASF“, Německo) získává ve smyslu čl. 3 odst. 1 písm. b) nařízení ES o spojování nákupem akcií výlučnou kontrolu nad podnikem Cognis GmbH („Cognis“, Německo).
2. Předmětem podnikání příslušných podniků je:
 - podniku BASF: chemické látky, plasty, výkonné produkty, zemědělské produkty a funkční roztoky, ropa a plyn,
 - podniku Cognis: speciální chemické látky a výživové složky.
3. Komise po předběžném posouzení zjistila, že by oznamovaná transakce mohla spadat do působnosti nařízení (ES) o spojování. Konečné rozhodnutí v tomto ohledu však zůstává vyhrazeno.
4. Komise vyzývá zúčastněné třetí strany, aby jí předložily své případné připomínky k navrhované transakci.

Připomínky musí být Komisi doručeny nejpozději do deseti dnů po zveřejnění tohoto oznámení. Připomínky lze Komisi zaslat faxem (+32 22964301), e-mailem na adresu COMP-MERGER-REGISTRY@ec.europa.eu nebo poštou s uvedením čísla jednacího COMP/M.5927 – BASF/Cognis na adresu Generálního ředitelství pro hospodářskou soutěž Evropské komise:

European Commission
Directorate-General for Competition
Merger Registry
J-70
1049 Bruxelles/Brussel
BELGIQUE/BELGIË

⁽¹⁾ Úř. věst. L 24, 29.1.2004, s. 1 („nařízení ES o spojování“).

Předběžné oznámení o spojení podniků
(Věc COMP/M.5982 – CVCII/Advance Properties/Huvepharma)
Věc, která může být posouzena zjednodušeným postupem
(Text s významem pro EHP)
(2010/C 280/10)

1. Komise dne 8. října 2010 obdržela oznámení o navrhovaném spojení podle článku 4 a na základě postoupení podle čl. 4 odst. 5 nařízení Rady (ES) č. 139/2004 ⁽¹⁾, kterým podnik Citigroup Venture Capital International Investment G.P. Limited („CVCII“, Jersey), kontrolovaný podnikem Citigroup, Inc. (USA), a podnik Advance Properties OOD („Advance Properties“, Bulharsko) získávají ve smyslu čl. 3 odst. 1 písm. b) nařízení ES o spojování nákupem akcií společnou kontrolu nad podnikem Huvepharma AD („Huvepharma“, Bulharsko), který je v současné době pod výlučnou kontrolou podniku Advance Properties.

2. Předmětem podnikání příslušných podniků je:

- podniku Citigroup: poskytování finančních služeb včetně bankovních a zprostředkovatelských služeb a správy soukromých investičních fondů,
- podniku Advance Properties: investice v oblasti léčiv, nemovitostí, energií a lodní přepravy,
- podniku Huvepharma: léčiva se zaměřením na veterinární a potravinové výrobky.

3. Komise po předběžném posouzení zjistila, že by oznamovaná transakce mohla spadat do působnosti nařízení (ES) o spojování. Konečné rozhodnutí v tomto ohledu však zůstává vyhrazeno. V souladu se sdělením Komise o zjednodušeném postupu ohledně některých spojování podle nařízení (ES) o spojování ⁽²⁾ je třeba uvést, že tato věc může být posouzena podle postupu stanoveného sdělením.

4. Komise vyzývá zúčastněné třetí strany, aby jí předložily své případné připomínky k navrhované transakci.

Připomínky musí být Komisi doručeny nejpozději do deseti dnů po zveřejnění tohoto oznámení. Připomínky lze Komisi zaslat faxem (+32 22964301), e-mailem na adresu COMP-MERGER-REGISTRY@ec.europa.eu či poštou s uvedením čísla jednacího COMP/M.5982 – CVCII/Advance Properties/Huvepharma na adresu Generálního ředitelství pro hospodářskou soutěž Evropské Komise:

European Commission
Directorate-General for Competition
Merger Registry
J-70
1049 Bruxelles/Brussel
BELGIQUE/BELGIË

⁽¹⁾ Úř. věst. L 24, 29.1.2004, s. 1 („nařízení ES o spojování“).

⁽²⁾ Úř. věst. C 56, 5.3.2005, s. 32 („sdělení o zjednodušeném postupu“).

Sdělení ministryně hospodářství Nizozemského království na základě čl. 3 odst. 2 směrnice Evropského parlamentu a Rady 94/22/ES o podmínkách udělování a užívání povolení k vyhledávání, průzkumu a těžbě uhlovodíků

(2010/C 280/11)

Ministryně hospodářství Nizozemského království sděluje, že obdržela žádost o povolení k vyhledávání uhlovodíků v části bloku P18 na mapě, která je přiložena jako příloha 3 vyhlášky o těžbě (Mijnbouwregeling) (úřední věstník (Staatscourant) 2002, č. 245). Tento dílčí blok ponese označení P18b.

S odvoláním na směrnici uvedenou v záhlaví a na článek 15 horního zákona (Mijnbouwwet) (sbírka zákonů (Staatsblad) 2002, č. 542) vyzývá ministryně hospodářství zúčastněné subjekty k podání konkurenční žádosti o povolení k těžbě uhlovodíků v dílčím bloku P18b nizozemského kontinentálního šelfu.

Dílčí blok P18b je vymezen rovnoběžkami mezi dvojicemi bodů A–B a H–I, poledníky mezi dvojicemi bodů B–C, G–H a A–I, ortodromami mezi dvojicemi bodů C–D a E–F, kruhovým obloukem 1 procházejícím body D a E a kruhovým obloukem 2 procházejícím body F a G.

Tyto body mají následující souřadnice:

bod	°	'	" východní délky	°	'	" severní šířky
A	3	40	0,000	52	10	0,000
B	3	47	0,000	52	10	0,000
C	3	47	0,000	52	4	21,072
D	3	47	16,385	52	4	16,801
E	3	51	32,620	52	6	15,485
F	3	51	40,829	52	6	37,449
G	4	0	0,000	52	4	48,172
H	4	0	0,000	52	0	0,000
I	3	40	0,000	52	0	0,000

Kruhový oblouk 1 má střed v souřadnicích 3° 54' 0,000" východní délky, 52° 1' 30,000" severní šířky a poloměr 5 námořních mil.

Kruhový oblouk 2 má střed v souřadnicích 3° 53' 34,000" východní délky, 52° 1' 46,000" severní šířky a poloměr 5 námořních mil.

Poloha výše uvedených bodů je udána v zeměpisných souřadnicích vypočítaných podle Evropského terestrického referenčního systému.

Rozloha dílčího bloku P18b činí 313,2 km².

Ministryně hospodářství představuje příslušný orgán pro udělování povolení. Kritéria, podmínky a požadavky stanovené v čl. 5 odst. 1, čl. 5 odst. 2 a v čl. 6 odst. 2 výše uvedené směrnice jsou blíže uvedeny v horním zákoně (Mijnbouwwet) (sbírka zákonů (Staatsblad) 2002, č. 542).

Žádosti je možné podávat po dobu třinácti týdnů od zveřejnění této výzvy v *Úředním věstníku Evropské unie* a je třeba je zaslat ministryni hospodářství na tuto adresu:

De Minister van Economische Zaken
ter attentie van J. C. De Groot, directeur Energiemarkt
ALP/562
Bezuidenhoutseweg 30
Postbus 20101
2500 EJ Den Haag
NEDERLAND

Žádosti obdržené po uplynutí uvedené lhůty nebudou brány v potaz.

O žádostech bude rozhodnuto nejpozději do dvanácti měsíců od uplynutí uvedené lhůty.

Další informace je možné získat od p. E. J. Hoppela na telefonním čísle +31 703797088.

OPRAVY**Oprava zveřejnění žádosti o uznání tradičního výrazu podle článku 33 nařízení Komise (ES) č. 607/2009**

(Úřední věstník Evropské unie C 275 ze dne 12. října 2010)

(2010/C 280/12)

Strana 11, 13 a 15: výraz „Příslušný orgán členského státu.“ se vypouští.

Opravy

2010/C 280/12

Oprava zveřejnění žádosti o uznání tradičního výrazu podle článku 33 nařízení Komise (ES) č. 607/2009 (Úř. věst. C 275 ze dne 12.10.2010) 39



CENY PŘEDPLATNÉHO NA ROK 2010 (bez DPH, včetně poštovního za obvyklou zásilku)

Úřední věstník EU, řady L + C, pouze tištěné vydání	22 úředních jazyků EU	1 100 EUR ročně
Úřední věstník EU, řady L + C, tištěné vydání + roční CD-ROM	22 úředních jazyků EU	1 200 EUR ročně
Úřední věstník EU, řada L, pouze tištěné vydání	22 úředních jazyků EU	770 EUR ročně
Úřední věstník EU, řady L + C, měsíční CD-ROM (souhrnný)	22 úředních jazyků EU	400 EUR ročně
Dodatek k Úřednímu věstníku (řada S), CD-ROM, 2 vydání týdně	mnohojazyčné: 23 úředních jazyků EU	300 EUR ročně
Úřední věstník EU, řada C – Výběrová řízení	jazyky, kterých se týká výběrové řízení	50 EUR ročně

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

Každá jazyková verze má samostatné předplatné.

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

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

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

Nosiče CD-ROM budou během roku 2010 nahrazeny nosiči DVD.

Prodej a předplatné

Předplatné různých placených periodik, jako například předplatné *Úředního věstníku Evropské unie*, lze získat u našich distributorů. Seznam distributorů se nachází na této internetové adrese:

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

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

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



Úřad pro publikace Evropské unie
2985 Lucemburk
LUCEMBURSKO

CS