

# EVROPSKÝ INSPEKTOR OCHRANY ÚDAJŮ

## Stanovisko evropského inspektora ochrany údajů ke sdělení Komise o akčním plánu zavádění inteligentních dopravních systémů v Evropě a k souvisejícími 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

(2010/C 47/02)

EVROPSKÝ INSPEKTOR OCHRANY ÚDAJŮ,

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

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

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

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

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

s ohledem na žádost o stanovisko v souladu s čl. 28 odst. 2 nařízení č. 45/2001 obdrženu od Evropské komise dne 11. února 2009,

PŘIJAL TOTO STANOVISKO:

### I. ÚVOD

1. Komise dne 16. prosince 2008 přijala sdělení, v němž definuje akční plán zavádění inteligentních dopravních systémů v Evropě (dále jen „sdělení“) <sup>(1)</sup>. Ke sdělení je připojen návrh směrnice Evropského parlamentu a Rady,

<sup>(1)</sup> KOM(2008) 886 v konečném znění. Rada přijala závěry k tomuto sdělení na 2935. zasedání Rady (Doprava, telekomunikace a energetika) ve dnech 30. a 31. března 2009.

kteřou se stanoví rámec pro zavedení inteligentních dopravních systémů v silniční dopravě a jejich styčné body s jinými druhy dopravy (dále jen „návrh“) <sup>(2)</sup>. Sdělení a připojený návrh zaslala Komise evropskému inspektorovi ochrany údajů ke konzultaci v souladu s čl. 28 odst. 2 nařízení (ES) č. 45/2001 <sup>(3)</sup>.

2. Evropský inspektor ochrany údajů vítá, že je konzultován, a doporučuje, aby byl v bodech odůvodnění návrhu uveden odkaz na tuto konzultaci, podobně jako je tomu v mnoha jiných legislativních textech, ohledně nichž byl evropský inspektor ochrany údajů v souladu s nařízením (ES) č. 45/2001 konzultován.

### 1.1 Sdělení Komise o akčním plánu zavádění ITS v Evropě

3. „Inteligentní dopravní systémy“ (ITS) jsou pokročilými aplikacemi, které využívají informační a komunikační technologie (IKT) zabudované v jednotlivých druzích dopravy pro účely vzájemné interakce. V oblasti silniční dopravy poskytnou ITS inovativní služby v souvislosti s druhy dopravy a řízením dopravy různým uživatelům, jako jsou cestující, uživatelé a provozovatelé silniční dopravní infrastruktury, správci vozových parků a provozovatelé tíšňových služeb.
4. V souvislosti s hodnocením rostoucího zavádění ITS v jednotlivých druzích dopravy <sup>(4)</sup> v Evropské unii Komise přijala akční plán s cílem urychlit zavádění a využívání aplikací a služeb ITS v oblasti silniční dopravy. Cílem akčního plánu je rovněž zajistit jejich součinnost s

<sup>(2)</sup> KOM(2008) 887 v konečném znění.

<sup>(3)</sup> 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.

<sup>(4)</sup> Na úrovni EU existuje mnoho iniciativ začleňujících ITS do jednotlivých druhů dopravy včetně letecké dopravy (SESAR), vodní dopravy (RIS), železniční dopravy (ERTMS, TAF-TSI), lodní dopravy (VTMIS, AIS, LRIT) a silniční dopravy (eToll, eCall), viz dokument KOM(2008) 886 v konečném znění, s. 3.

jinými druhy dopravy, čímž bude usnadněno poskytování multimodálních služeb. Soudržné zavádění ITS v Evropě přispěje k mnoha cílům Společenství, včetně účinnosti, udržitelnosti a bezpečnosti dopravy a posílení vnitřního trhu a konkurenceschopnosti EU. Vzhledem k různorodosti cílů v oblasti zavádění ITS je ve sdělení uvedeno šest prioritních oblastí činnosti na období let 2009 až 2014. Komise navrhuje, aby byl pro účely provedení plánu vymezen na úrovni EU právní rámec prostřednictvím směrnice, na jejímž základě bude definována řada opatření ve vybraných prioritních oblastech.

### 1.2 Návrh směrnice, kterou se stanoví rámec pro zavedení ITS v silniční dopravě a jejich styčné body s jinými druhy dopravy

- Návrhem se stanoví rámec pro nadnárodní zavádění aplikací ITS, který má usnadnit poskytování harmonizovaných přeshraničních služeb, zejména v oblasti dopravních a cestovních informací a řízení dopravy. Od členských států návrh vyžaduje, aby přijaly některá technická opatření za účelem usnadnění výměny údajů mezi uživateli, veřejnými orgány, zúčastněnými stranami a poskytovateli služeb ITS a za účelem integrace systémů ITS, které souvisí s bezpečností, do vozidel a dopravní infrastruktury. Technické specifikace pro aplikace a systémy ITS ve čtyřech z prioritních oblastí<sup>(5)</sup> uvedených v akčním plánu budou definovány postupem projednávání ve výborech<sup>(6)</sup>, jehož hlavní prvky jsou uvedeny v příloze II. Konkrétní účely využití ITS v těchto oblastech však nejsou zřejmé. Zavedení ITS se navíc může rozšířit do mnohem většího počtu oblastí než jsou uvedené čtyři oblasti původně zvolené pro vypracování harmonizovaných technických specifikací. Návrh je zaměřen především na zavádění budoucích aplikací a služeb ITS, avšak bude-li to možné, bude se vztahovat i na stávající technologie v dané oblasti nebo technologie, jejichž vývoj v současnosti probíhá (například eCall, eToll a další).

- Návrh byl zaslán Evropskému parlamentu, který přijal stanovisko v prvním čtení<sup>(7)</sup> dne 23. dubna 2009. V návaznosti na žádost o konzultaci, kterou Rada předlo-

<sup>(5)</sup> Článek 4 návrhu stanoví vymezení technických opatření v těchto oblastech: i) optimální využití silničních, dopravních a cestovních údajů, ii) kontinuita služeb ITS v oblasti řízení provozu a nákladní dopravy v evropských dopravních koridorech a v aglomeracích, iii) bezpečnost a zajištění silničního provozu, iv) integrace vozidla do dopravní infrastruktury.

<sup>(6)</sup> Návrh stanoví použití regulativního postupu s kontrolou v souladu s čl. 5a odst. 1 až 4 a článkem 7 rozhodnutí 1999/468/ES.

<sup>(7)</sup> Legislativní usnesení Evropského parlamentu ze dne 23. dubna 2009 o 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, T6-0283/2009.

žila dne 29. ledna 2009, přijal Evropský hospodářský a sociální výbor stanovisko k návrhu dne 13. května 2009<sup>(8)</sup>.

### 1.3 Zaměření stanoviska

- EIOÚ vítá, že je v souvislosti s navrhovaným plánem zavedení ITS předloženým Komisí konzultován. Není to poprvé, co se EIOÚ otázkami obsaženými v akčním plánu ITS zabývá. EIOÚ vydal stanovisko k návrhu Komise o usnadnění přeshraničního vymáhání právních předpisů v oblasti bezpečnosti silničního provozu<sup>(9)</sup> a přispěl k práci pracovní skupiny zřízené podle článku 29 v souvislosti s pracovním dokumentem o eCall<sup>(10)</sup>.
- Inteligentní dopravní systémy jsou založeny na shromažďování, zpracovávání a výměně velmi různorodých údajů z veřejných i soukromých zdrojů; jedná se tedy o oblast, která s údaji intenzivně pracuje. Zavedení ITS bude ve velké míře závislé na geolokalizačních technologiích, jako je družicové určování polohy a bezkontaktní technologie, například RFID, což usnadní poskytování širokého spektra veřejných nebo komerčních služeb založených na lokalizaci (například dopravní informace v reálném čase, eFreight, eCall, eToll, rezervace parkování a další). Některé informace, jež budou zpracovávány prostřednictvím ITS, jsou souhrnné povahy a nevztahují se k žádným osobám, například informace o dopravě, nehodách a možnostech, zatímco jiné informace se týkají identifikovaných nebo identifikovatelných osob, a jsou proto považovány za osobní údaje ve smyslu čl. 2 písm. a) směrnice 95/46/ES.
- EIOÚ přikládá zásadní význam tomu, aby akce plánované pro zavedení ITS byly v souladu se stávajícím právním rámcem, jak je uveden v návrhu, zejména se směrnicí 95/46/ES o ochraně údajů<sup>(11)</sup> a směrnicí 2002/58/ES o soukromí a elektronických komunikacích<sup>(12)</sup>.

<sup>(8)</sup> Stanovisko Evropského hospodářského a sociálního výboru k 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, TEN/382, 13. května 2009.

<sup>(9)</sup> Stanovisko evropského inspektora ochrany údajů k návrhu směrnice Evropského parlamentu a Rady o usnadnění přeshraničního vymáhání právních předpisů v oblasti bezpečnosti silničního provozu, 2008/C 310/02, Úř. věst. C 310, 5.12.2008, s. 9.

<sup>(10)</sup> Pracovní dokument pracovní skupiny zřízené podle článku 29 o ochraně údajů a dopadech na soukromí v souvislosti s iniciativou eCall, WP 125, 26. září 2006. [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2006/wp125\\_cs.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp125_cs.pdf)

<sup>(11)</sup> 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.

<sup>(12)</sup> Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích), Úř. věst. L 201, 31.7.2002, s. 37.

10. Nevyřešené otázky související s ochranou soukromí a údajů představují podle Komise jednu z hlavních překážek podpory ITS. Tyto otázky budou v tomto stanovisku rozpracovány takto:

— v kapitole II bude z hlediska ochrany údajů analyzován právní rámec, který Komise pro účely zavedení ITS předložila,

— v kapitole III budou zdůrazněny záležitosti týkající se ochrany údajů, jimiž je třeba se dále zabývat za účelem řádného zavedení ITS:

— v prvním bodě se stanovisko zaměří na potřebu, aby součástí vývoje ITS bylo „soukromí coby aspekt návrhu“, a dále budou uvedeny důležité otázky, které je třeba vyřešit při navrhování aplikací a systémů zpracování údajů v rámci ITS,

— druhý bod se zaměří na některé otázky týkající se soukromí, kterými je třeba se dále zabývat pro účely poskytování služeb ITS.

## II. ANALÝZA PRÁVNÍHO RÁMCE NAVRŽENÉHO PRO ZAVEDENÍ ITS

11. Návrh směrnice předložený Komisí obsahuje dvě ustanovení (9. bod odůvodnění a článek 6), jejichž předmětem je soukromí, bezpečnost a opakované použití informací. Ustanovení čl. 6 odst. 1 návrhu Komise vyžaduje, aby provoz ITS probíhal v souladu s pravidly pro ochranu údajů uvedenými mimo jiné ve směrnici 95/46/ES a směrnici 2002/58/ES. V čl. 6 odst. 2 návrhu Komise se stanoví konkrétní opatření na ochranu údajů zaměřená především na bezpečnost: Článek 6 odst. 2 stanoví, že „Členské státy [...] zajistí, aby jejich údaje a záznamy o ITS byly chráněny proti zneužití, včetně nedovoleného přístupu, úprav nebo ztráty“. V čl. 6 odst. 3 návrhu Komise je pak stanoveno, že se „použije směrnice 2003/98/ES“.

12. Evropský parlament navrhnul v prvním čtení několik změn článku 6. Zejména byly do čl. 6 odst. 1 vloženy tři nové odstavce týkající se případného využívání anonymních

údajů, zpracovávání citlivých údajů pouze s informovaným souhlasem subjektu údajů a zajištění toho, aby osobní údaje byly zpracovávány pouze „pokud je to nezbytné pro provoz aplikací nebo služeb ITS“. Dále byl změněn čl. 6 odst. 2, v němž bylo doplněno, že údaje a záznamy o ITS nesmí „být použity pro jiné účely, než které jsou uvedeny v této směrnici“.

13. EIOÚ vítá skutečnost, že ochrana údajů byla při práci na návrhu zohledněna a že je předkládána jako obecná podmínka řádného zavedení ITS v Evropě. EIOÚ uznává, že je třeba soudržným způsobem harmonizovat zpracovávání údajů na úrovni EU za účelem zajištění proveditelnosti aplikací a služeb ITS v celé Evropě.

14. EIOÚ však poznamenává, že navrhovaný právní rámec je pro účely odpovídajícího řešení obav, jež v souvislosti s ochranou soukromí a údajů vzbuzuje zavádění ITS v členských státech, příliš široký a obecný. Není zřejmé, kdy povede poskytování služeb ITS ke shromažďování a zpracovávání údajů, jaké jsou konkrétní účely zpracovávání údajů ani na základě jakého právního základu je toto zpracovávání odůvodněno. Kromě toho se s využíváním lokalizačních technologií pro zavádění ITS zvyšuje riziko, že dojde k vytvoření služeb narušujících soukromí, pokud tyto služby vyžadují shromažďování a výměnu osobních údajů. V návrhu navíc chybí jasné rozdělení úloh a povinností jednotlivých provozovatelů zapojených do zavádění ITS a není proto zřejmé, kteří provozovatelé budou správci údajů a budou odpovídat<sup>(13)</sup> za dodržování povinností spojených s ochranou údajů. Nebudou-li tyto otázky právně vyřešeny, budou provozovatelé ITS čelit značným problémům, neboť právě oni budou nakonec pověřeni uplatňováním opatření stanovených v navrhované směrnici.

15. Vzniká proto riziko, že nejasnosti v souvislosti s navrhovaným právním rámcem povedou k odlišnostem v provádění ITS v Evropě, což namísto zmenšování rozdílů mezi členskými státy povede ke značné nejistotě, roztříštěnosti a rozporům, a to v důsledku odlišných úrovní ochrany údajů v celé Evropě. Může to vést rovněž k nedodržování základních záruk ochrany údajů. EIOÚ zdůrazňuje, že je nutné tyto otázky na úrovni EU dále harmonizovat. EIOÚ tak navrhuje provést změny navrhovaného právního rámce z hlediska ochrany údajů. Důrazně doporučuje, aby Parlament a Rada do návrhu vložily navrhované změny a případně i další ustanovení za účelem vyjasnění nedořešených otázek (například definice a povinnosti subjektů v oblasti ITS, vypracování harmonizovaných smluv pro poskytování služeb ITS a další).

<sup>(13)</sup> V souladu s čl. 2 písm. d), čl. 6 odst. 2 a článkem 23 směrnice 95/46/ES, uvedené v poznámce pod čarou 11.

Dále zdůrazňuje, že členské státy rovněž ponесou odpovědnost za řádné provádění směrnice, aby tak provozovatelé mohli vytvořit systémy a služby nabízející odpovídající úroveň ochrany údajů v celé Evropě.

### II.1 Činnosti související se zpracováním údajů musí být založeny na vhodném právním základu

16. Není zřejmé, kdy dojde po integraci vybavení ITS do vozidla k zahájení zpracování osobních údajů a na základě jakých právních důvodů bude toto zpracování probíhat. Provozovatelé se pro účely zpracování údajů mohou opírat o různé právní základy, například jednoznačný souhlas uživatelů, smlouvu či právní závazek, který musí správce dodržet. Právní základ, podle něhož bude probíhat zpracování údajů prostřednictvím ITS, je třeba harmonizovat, aby bylo zajištěno, že systémy budou funkční v celé Evropě a uživatelé nebudou poškozeni v důsledku rozdílů ve způsobu zpracování v jednotlivých zemích EU.
17. V řadě případů budou systémy ITS do vozidel integrovány automaticky. Jedná se zejména o systémy ITS týkající se bezpečnosti a zajištění silničního provozu, jež podle návrhu ve vozidlech zabudovány být musí. Návrh však nestanoví, co se rozumí pojmem „systémy ITS týkající se bezpečnosti a zajištění silničního provozu“; mělo by být proto dále vyjasněno, o které konkrétní aplikace a systémy ITS, jež musí být ve vozidlech zabudovány, se jedná. Dále je třeba objasnit, zda bude aktivace a používání daného zařízení pro uživatele dobrovolná, nebo povinná. K povinnému zpracování údajů by se mělo přistoupit pouze pro konkrétní účely a na základě přesvědčivých důvodů (například sledování zboží pro účely řízení provozu) a za použití odpovídajících záruk týkajících se zpracování údajů o osobách. Pokud se ITS používá na dobrovolném základě, měly by být zavedeny odpovídající záruky s cílem zabránit domněnce, že uživatelé z důvodu pouhé přítomnosti systému ve vozidle implicitně souhlasí s jeho používáním.
18. EIOÚ se přiklání k tomu, aby služby ITS byly poskytovány na dobrovolném základě. To znamená, že uživatelé musí mít možnost svobodně souhlasit s používáním systému a s konkrétními účely pro jeho použití. Pokud se poskytovaná služba opírá o lokalizační údaje, musí být uživatelům poskytnuty příslušné informace (zejména v souladu s článkem 9 směrnice 2002/58/ES) a uživatel musí mít možnost svůj souhlas odvolat. V praxi to vyžaduje zavedení jednoduchého způsobu deaktivace zařízení nebo funkce, pokud uživatel již nesouhlasí s používáním daného systému nebo konkrétní funkce, a to aniž by to pro něj představovalo technické nebo finanční omezení<sup>(14)</sup>. Je třeba zavést další záruky s cílem zabránit diskriminaci uživatelů v případě, že odmítnou některou službu využívat.
19. V případech, kdy jsou některé činnosti zpracování povinné a jiné podléhají souhlasu uživatele, musí být zajištěna

transparentnost, pokud jde o jednotlivé operace zpracování údajů, a to tím, že se uživatelé poskytnou příslušné informace o povinné nebo dobrovolné povaze každé konkrétní operace zpracování a o rozsahu tohoto zpracování. Dále je velmi důležité zajistit zavedení odpovídajících bezpečnostních záruk, aby nedošlo ke shromažďování a zpracování údajů mimo oblast, která byla právně vymezena nebo s níž byl vysloven dobrovolný souhlas.

20. Vzhledem k nadnárodnímu dopadu služeb ITS dále EIOÚ doporučuje vypracování celoevropských standardních smluv s cílem zajistit, že služby poskytované prostřednictvím ITS nabízejí stejné záruky ochrany údajů v celé Evropě, a zejména že informace poskytované uživatelům jsou dostatečně jasné, pokud jde o konkrétní použité funkce, dopad používání konkrétních technologií na ochranu jejich údajů a způsob, jak mohou uplatnit svá práva. Dojde-li k doplnění nových funkcí, měli by poskytovatelé služeb přijmout další opatření s cílem poskytnout uživatelům jasné a konkrétní informace týkající se těchto doplňujících funkcí a získat jejich souhlas s používáním nových funkcí.

### II.2 Je nutné dále vymežit účely a aspekty zpracování údajů

21. EIOÚ poukazuje na to, že v návrhu nejsou jasně vymezeny konkrétní služby a účely, pro něž lze aplikace ITS použít, a že tato otázka tedy zůstává otevřená. V praxi tato skutečnost umožňuje flexibilitu, nese však s sebou možnost, že nevyřešené otázky v souvislosti s ochranou soukromí a údajů, jež Komise určila jako jednu z hlavních překážek podpory ITS (viz bod 10), zůstanou i nadále nevyřešeny a budou bránit vyváženému provádění navrhovaných opatření.
22. EIOÚ zdůrazňuje, že je obzvláště důležité, aby zpracování prováděné s ohledem na poskytování konkrétních služeb ITS probíhalo nejen podle řádného právního základu, ale také pro stanovené, výslovně vyjádřené a legitimní účely a aby zamýšlené zpracování bylo přiměřené a nutné z hlediska těchto účelů (článek 6 směrnice 95/46/ES). Měla by se proto zvážit případná nutnost přijmout na úrovni EU další právní předpisy týkající se konkrétních použití ITS s cílem poskytnout harmonizovaný a vhodný právní základ pro prováděné zpracování a zabránit nesrovnalostem při zavádění služeb ITS mezi členskými státy.
23. Na základě navrhovaného rámce ještě nebylo rozhodnuto o aspektech zpracování údajů a výměny údajů pro účely používání ITS. O velkém množství technických parametrů bude rozhodnuto až v pozdější fázi prostřednictvím postupu projednávání ve výborech, přičemž volba těchto parametrů bude mít různé dopady na ochranu soukromí a údajů. S ohledem na zvláštní ochranu, která je přiznána ochraně soukromí a údajů jakožto základním právům podle článku 8 Evropské úmluvy o lidských právech

<sup>(14)</sup> Viz dokument WP 125 o iniciativě eCall, s. 4, uvedený v poznámce pod čarou 10.

a základních svobodách a článků 7 a 8 Listiny základních práv Evropské unie, vyvstává otázka, zda a do jaké míry by vymezení operací zpracování údajů mělo být rozhodnuto prostřednictvím postupu projednávání ve výborech.

24. V demokratické společnosti by rozhodnutí o základních zásadách a aspektech, jež mají dopad na základní práva, měla být přijímána řádným legislativním postupem, který zahrnuje odpovídající kontrolu a vyváženost. V tomto případě to znamená, že o rozhodnutích, která mají důležitý dopad na ochranu soukromí a údajů osob, jako jsou účely a aspekty povinného zpracování údajů a vymezení postupů pro zavádění ITS v nových oblastech, by se mělo rozhodovat v rámci Evropského parlamentu a Rady, nikoli v rámci postupu projednávání ve výborech.

25. EIOÚ v této souvislosti důrazně doporučuje, aby byl společně s pracovní skupinou zřízenou podle článku 29 zapojen v případě potřeby do práce výboru zřízeného podle článku 8 návrhu i do budoucích činností týkajících se zavádění ITS, a to prostřednictvím konzultací a v dostatečném předstihu před zavedením příslušných opatření.

26. EIOÚ bere dále na vědomí změny přijaté Evropským parlamentem v souvislosti s článkem 6 návrhu. EIOÚ v první řadě uvádí, že změna týkající se podpory případného využívání anonymních údajů je v zásadě velmi vítaná, nevyřeší však všechny obavy spojené se shromažďováním údajů, neboť mnoho údajů, jejichž shromažďování a výměna probíhá prostřednictvím ITS, lze označit za údaje osobní. Aby bylo zpracování osobních údajů prováděno na anonymním základě, je nutné, aby žádná osoba nemohla v žádné fázi zpracování, a to s ohledem na všechny prostředky, jež může správce údajů či jiná osoba s přiměřenou pravděpodobností použít, uvést dané údaje do souvislosti s údaji týkajícími se identifikované osoby; v opačném případě jsou tyto údaje osobními údaji ve smyslu čl. 2 písm. a) směrnice 95/46/ES<sup>(15)</sup>. EIOÚ dále na základě změn navržených Evropským parlamentem doporučuje, aby byl článek 6 návrhu pozměněn takto:

— Je třeba posoudit nutnost zpracování osobních údajů prostřednictvím ITS s ohledem na legitimní a konkrétní účely, pro něž jsou údaje zpracovávány (v souladu

s články 6 a 7 směrnice 95/46/ES). Provoz aplikace ITS<sup>(16)</sup> nemůže být sám o sobě legitimním účelem odůvodňujícím zpracování údajů, neboť aplikace je pouze prostředkem shromažďování a výměny údajů, jejichž využití by mělo být nutně zaměřeno na konkrétní účely.

— Změna<sup>(17)</sup> týkající se zákazu použití údajů a záznamů ITS „pro jiné účely, než které jsou uvedeny v této směrnici,“ nestanoví dostatečné záruky, a to zejména proto, že konkrétní účely a služby, pro něž budou ITS používány, nejsou ve směrnici jasně a vyčerpávajícím způsobem vyjmenovány. Vzhledem k tomu, že prostřednictvím ITS budou zpracovávány různé údaje pro velmi odlišné účely, je třeba zajistit, aby údaje získané v průběhu zpracování za konkrétním účelem nebyly použity pro jiné účely neslučitelné s daným účelem, jak je stanoveno v čl. 6 odst. 1 písm. b) směrnice 95/46/ES. EIOÚ proto doporučuje, aby byl čl. 6 odst. 2 dále změněn tak, aby bylo zajištěno, že údaje a záznamy ITS nebudou použity „pro jiné účely, než pro které byly získány, a způsobem neslučitelným s těmito účely“.

### III. OCHRANA ÚDAJŮ V RÁMCI INTELIGENTNÍCH DOPRAVNÍCH SYSTÉMŮ

27. S cílem určit, kdo ponese odpovědnost za zajištění toho, že systémy budou řádně fungovat z hlediska ochrany údajů, je zejména nutné, aby byly vyjasněny úlohy jednotlivých aktérů zapojených do ITS. Je proto třeba dále vyjasnit, kdo by měl odpovídat za provádění aplikací a systémů, jejichž podoba bude stanovena prostřednictvím postupu projednávání ve výborech, a kdo bude v řetězci zúčastněných subjektů odpovídat za to, že zpracování údajů probíhá v souladu s právními předpisy na ochranu údajů (tedy správci údajů). EIOÚ níže zdůrazní, kterým záležitostem v oblasti ochrany soukromí a údajů by při navrhování aplikací a architektury systémů měla být věnována pozornost v rámci postupu projednávání ve výborech a ze strany správců údajů. Dále uvede některé otázky v oblasti ochrany údajů, kterými se v souvislosti s poskytováním služeb ITS musí zabývat legislativní orgán a správci údajů.

#### III.1 „Soukromí coby aspekt návrhu“

28. Správné uplatňování zásad ochrany údajů stanovených ve směrnici 95/46/ES je základní podmínkou úspěšného zavedení ITS ve Společenství. Tyto zásady mají vliv na návrh architektury systémů a na aplikace. EIOÚ doporučuje, aby byl přístup založený na zásadě „soukromí coby aspekt

<sup>(15)</sup> Jak uvádí 26. bod odůvodnění směrnice 95/46/ES, „... že pro určení, zda je osoba identifikovatelná, je třeba přihlídnout ke všem prostředkům, které mohou být rozumně použity jak správcem, tak jakoukoli jinou osobou pro identifikaci dané osoby.“

<sup>(16)</sup> Změna 34, kterou se vkládá nový čl. 6 odst. 1 písm. b), stanoví: „Osobní údaje budou zpracovávány, pouze pokud je to nezbytné pro provoz aplikací nebo služeb ITS.“

<sup>(17)</sup> Změna 36 doplňuje do čl. 6 odst. 2 toto znění: „a aby nesměly být použity pro jiné účely, než které jsou uvedeny v této směrnici.“

návrhu“ přijat v rané fázi návrhu ITS s cílem definovat architekturu, provoz a správu aplikací a systémů. Tento přístup je zdůrazněn zejména ve směrnici 1999/5/ES<sup>(18)</sup> týkající se návrhu rádiových zařízení a telekomunikačních koncových zařízení.

29. Návrhy aplikací a systémů budou probíhat v několika fázích a budou je provádět různé subjekty, jež by všechny měly zohlednit ochranu soukromí a údajů. Komise a výbor pro ITS ponese zvláštní počáteční odpovědnost za definování opatření, iniciativ v oblasti normalizace a postupů, včetně osvědčených postupů, na podporu zásady „soukromí coby aspekt návrhu“; toto definování bude probíhat v rámci postupu projednávání ve výborech.

30. Zásadu „soukromí coby aspekt návrhu“ je třeba prosazovat ve všech fázích a všech podobách procesů:

— na organizační úrovni by soukromí mělo být zvažováno při definování postupů nutných pro výměnu údajů mezi všemi příslušnými místy v rámci výměny – to může mít přímý dopad na druh výměny a na to, jaké údaje jsou vyměňovány,

— požadavky týkající se soukromí a bezpečnosti by měly být začleněny do norem, osvědčených postupů, technických specifikací a systémů,

— pokud jde o technickou úroveň, EIOÚ doporučuje vypracovat, například prostřednictvím postupu projednávání ve výborech, nejlepší dostupné techniky<sup>(19)</sup> pro soukromí, ochranu údajů a bezpečnost v konkrétních oblastech nebo pro konkrétní účely, v nichž by byly definovány jednotlivé bezpečnostní parametry, které je třeba v průběhu životního cyklu systému provést za účelem zajištění souladu s předpisovým rámcem EU.

31. EIOÚ níže uvádí některé z otázek, kterými je třeba se při návrhu aplikací a architektury systémů zabývat. Týkají se shromážděných údajů, interoperability systému a bezpečnosti údajů.

### III.1.a) Minimalizace údajů a anonymita

32. V souladu s čl. 6 odst. 1 písm. c) směrnice 95/46/ES lze shromažďovat a zpracovávat pouze údaje, jež jsou nezbytné a podstatné pro konkrétní účely.

33. EIOÚ zdůrazňuje, že za účelem zabránění hromadnému a nevhodnému shromažďování osobních údajů je důležité, aby byla před navržením aplikací a systémů ITS provedena

odpovídající klasifikace informací a údajů, jež mají být prostřednictvím ITS zpracovány. V této souvislosti je třeba zohlednit:

— zdroj údajů (zda se jedná o veřejný zdroj, poskytovatele telekomunikačních služeb, poskytovatele služeb ITS, jiné provozovatele, vozidlo, uživatele vozidla nebo jiné subjekty údajů),

— povahu údajů (například souhrnné informace, anonymní údaje, osobní údaje, citlivé údaje),

— účel nebo účely, pro něž mají být údaje použity, a

— z hlediska systémů spolupráce je třeba objasnit, které údaje jsou z vozidla získávány na základě strategie tlaku a tahu, vyměňovány s jinými vozidly nebo infrastrukturou a mezi infrastrukturami navzájem a za jakými účely.

34. Jednotlivé funkce je třeba pečlivě analyzovat s ohledem na sledované cíle za účelem posouzení nutnosti shromažďování osobních údajů. EIOÚ zdůrazňuje, že je důležité dosáhnout řádné rovnováhy mezi základními právy subjektů údajů a zájmy jednotlivých zapojených subjektů, což znamená zpracování co nejmenšího možného množství osobních údajů. Architektura aplikací a systémů by měla být v co největší míře navržena tak, aby byly získávány pouze osobní údaje, jež jsou nezbytné nutné ke splnění plánovaných cílů.

35. Pokud osobní údaje nejsou nutné nebo pokud jsou nutné jen v počáteční fázi zpracování, nemělo by docházet k jejich shromažďování nebo by měly být co nejdříve anonymizovány. Je proto zvláště důležité posoudit nutnost shromažďování údajů, ale i nutnost jejich uchovávání v jednotlivých systémech. Je třeba stanovit konkrétní časové lhůty pro uchovávání osobních údajů pro všechny jednotlivé subjekty v řetězci služeb; tyto lhůty by měly být odlišeny podle druhu údajů a účelu, pro něž byly získány<sup>(20)</sup>. Není-li proto nadále nutné uchovávat osobní údaje za účelem dosažení cílů, pro něž byly získány nebo dále zpracovány, mělo by dojít k jejich anonymizaci, tj. neměly by se již vztahovat k žádným identifikovaným nebo identifikovatelným osobám.

36. Podoba architektury systémů a postupů výměny údajů by měla podpořit zpracování co nejmenšího množství osobních údajů. V této souvislosti je třeba zohlednit všechny fáze zpracování a všechny subjekty zapojené do řetězce poskytování služeb ITS. Některé údaje lze vyměňovat

<sup>(18)</sup> Zejména čl. 3 odst. 3 písm. c) 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.

<sup>(19)</sup> Nejlepší dostupné techniky chápeme jako neúčinnější a nejpokročilejší fázi vývoje činností a jejich způsobů fungování, což znamená, že určité techniky jsou z praktického hlediska vhodné pro to, aby byly v zásadě základem aplikací a systémů ITS, které musí být v souladu s požadavky předpisového rámce EU v oblasti soukromí, ochrany údajů a bezpečnosti.

<sup>(20)</sup> Například uchovávání provozních a lokalizačních údajů zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací ve veřejných komunikačních sítích je upraveno směrnicí Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES.

a zpracovávat na anonymním základě, jiné údaje, i když jejich výměna neprobíhá na základě identifikace, však mohou být uvedeny do souvislosti s údaji o identifikovaných osobách, a budou tedy představovat osobní údaje ve smyslu čl. 2 písm. a) směrnice 95/46/ES<sup>(21)</sup>. S ohledem na účely, pro něž budou ITS používány, bude problematické zajistit, aby velké množství údajů získávaných prostřednictvím ITS bylo zpracováno na anonymním základě, neboť totožnost dané osoby bude v určitém okamžiku nutná pro konkrétní účely, jako je fakturace. Proto by bylo potřeba alespoň přijmout zvláštní – technická, organizační a právní – opatření s cílem zajistit anonymitu v některých oblastech.

### III.1.b) Interoperabilita, kvalita údajů a omezení účelu

37. Ústředním prvkem úspěšného zavedení ITS je interoperabilita aplikací a systémů. Bude probíhat harmonizační činnost, jejímž prostřednictvím budou určeny technické specifikace rozhraní, která je třeba do aplikací a systémů integrovat, aby byla zajištěna jejich interoperabilita s jinými aplikacemi používanými v dalších druzích dopravy nebo dopravních systémech. Interoperabilita systémů napomůže snazšímu poskytování škály služeb a přispěje k zajištění jejich kontinuity v celé Evropě, avšak zároveň s sebou nese určité množství rizik z hlediska ochrany údajů, například riziko jejich nesprávného použití nebo jejich zneužití. Veškerá propojení databází by měla probíhat s řádným ohledem na zásady ochrany údajů<sup>(22)</sup> a na praktické záruky bezpečnosti (viz rovněž oddíl III.1.c).
38. V kontextu interoperability aplikací a systémů má obzvláště klíčový význam zásada kvality údajů, jež je upravena v čl. 6 odst. 1 písm. d) směrnice 95/46/ES. Technické specifikace stanovené pro tvorbu rozhraní by měly zajišťovat přesnost údajů, jež budou v důsledku propojení aplikací a systémů získávány.
39. Vzhledem k tomu, že interoperabilita systémů usnadní propojení databází a přiřazování údajů pro další účely, EIOÚ zdůrazňuje, že veškerá propojení by měla být uskutečňována po pečlivém zvážení zásady omezení účelu stanovené v čl. 6 odst. 1 písm. b) směrnice 95/46/ES. Zejména je důležité, aby byla architektura systémů ITS vybudována způsobem, jenž zamezí jakémukoli dalšímu použití údajů pro jiné účely, než pro které byly tyto údaje shromážděny. Systém musí obsahovat vhodné prvky bezpečnostní ochrany pro předcházení zneužití, neoprávněnému zveřejnění nebo přístupu a vedlejším účinkům příslušného zařízení. Měla by být například zavedena bezpečnostní ochrana dostatečně zajišťující, že k pohyblivým zařízením nebudou mít přístup třetí strany bez oprávnění a že tato zařízení nebudou použita k identifikaci a sledování osob nad rámec účelů daného systému.

<sup>(21)</sup> Viz poznámka pod čarou 15.

<sup>(22)</sup> Viz též připomínky EIOÚ ke sdělení Komise o interoperabilitě evropských databází, 10. března 2006. [http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2006/06-03-10\\_Interoperability\\_EN.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2006/06-03-10_Interoperability_EN.pdf)

40. Pokud jde o zákonnost propojení jako takového, bude při jejím hodnocení třeba postupovat případ od případu, s přihlédnutím k povaze údajů, jež jsou prostřednictvím systémů zpřístupněny a vyměňovány, a k původním účelům jejich zamýšleného využití.

### III.1.c) Zabezpečení údajů

41. Zabezpečení osobních údajů je v rámci zavádění ITS klíčovým prvkem. EIOÚ vítá, že v akčním plánu i v návrhu směrnice je zabezpečení údajů výslovně uvedeno. Se zabezpečením by se mělo počítat nejen v průběhu fungování zařízení ITS (v palubním systému a v komunikačním protokolu), nýbrž i nad rámec provozu tohoto zařízení – v databázích, kde jsou údaje zpracovávány nebo uchovávány. Pro všechny fáze zpracování by měly být stanoveny vhodné technické, administrativní a organizační požadavky zajišťující příslušnou úroveň zabezpečení v souladu s články 16 a 17 směrnice 95/46/ES (a v relevantních případech i s články 4 a 5 směrnice 2002/58/ES).
42. Vhodná bezpečnostní opatření by měla být definována teprve po pečlivém vyhodnocení konkrétních účelů používání ITS a aspektů týkajících se zpracování. V této souvislosti EIOÚ doporučuje, aby byla prováděna hodnocení dopadu z hlediska ochrany soukromí a údajů ve vztahu k jednotlivým oblastem nebo účelům využití (např. pro systémy ITS související s bezpečností, pro systémy řízení nákladní dopravy atd.). Provádění hodnocení dopadu z hlediska ochrany soukromí a údajů a využití nejlepších dostupných technik pro tuto ochranu přispěje k určení nejvhodnějších bezpečnostních opatření, jež budou relevantní pro konkrétně prováděné zpracování.

### III.2 Další aspekty ochrany údajů a soukromí z hlediska poskytování služeb ITS

43. Na úrovni EU je nezbytná další harmonizace aspektů zavádění služeb ITS, aby se předešlo tomu, že v tomto zavádění bude docházet k nesrovnalostem. V této souvislosti by EIOÚ rád poukázal na následující dvě otázky, jež si zejména vyžádají dalšího uvážení z hlediska ochrany soukromí a údajů:
- používání lokalizačních nástrojů pro účely poskytování veřejných i komerčních služeb založených na lokalizaci vyžaduje zavedení dalších záruk. V tomto kontextu by měla být věnována zvláštní pozornost otázce, zda a kdy jsou služby ITS založené na lokalizaci používány pro soukromé nebo profesionální účely, a jak by použitím takového systému mohly být zasaženy osoby využívající vozidla pro pracovní účely,

- u integrovaných systémů je zejména důležité, aby byly vyjasněny role a povinnosti jednotlivých stran účastnících se zavádění ITS.

III.2.a) Závazky týkající se používání lokalizačních nástrojů pro účely poskytování služeb ITS založených na lokalizaci

44. Zaváděním ITS bude podpořen vývoj aplikací pro „sledování a vyhledávání“ zboží a bude umožněno zahájení komerčních i veřejných služeb založených na lokalizaci. Takové služby budou vycházet z technologií jako družicové určování polohy a štítky RFID<sup>(23)</sup>. Systémy navigace, sledování a vyhledávání mají být používány za mnoha účely, jako je například dálkové sledování vozidel a nákladu v průběhu jízdy (např. při přepravě nebezpečného zboží nebo živých zvířat), fakturace vozidel z hlediska řady parametrů včetně ujeté vzdálenosti a denní doby (např. zpoplatnění cest, elektronické systémy pro výběr mýtného) a sledování řidičů pro účely vynuocování práva, např. pokud jde o kontrolu doby jízdy (pomocí digitálních tachografů) a ukládání sankcí (prostřednictvím elektronického určení totožnosti vozidla).

45. Z hlediska ochrany soukromí je využívání lokalizačních technologií zvláště rušivé, neboť umožňuje sledovat řidiče a shromažďovat nejrůznější údaje o jejich jízdních návycích. Jak zdůraznila pracovní skupina zřízená podle článku 29<sup>(24)</sup>, zpracování lokalizačních údajů představuje zvláště citlivé téma zahrnující klíčovou otázku svobody anonymního pohybu a vyžadující zavedení zvláštních záruk, jimiž se předejde sledování osob a zneužití dotyčných údajů.

46. EIOÚ zdůrazňuje, že použití lokalizačních nástrojů musí být zákonné, tedy vycházející z řádného právního základu, musí sledovat explicitní a legitimní účely a musí být přiměřené cílům, jichž má být dosaženo. Zákonnost prováděného zpracování údajů bude do značné míry záviset na způsobu a účelech použití lokalizačních nástrojů. Jak pracovní skupina zřízená podle článku 29 zdůraznila ve stanovisku k iniciativě eCall, „z hlediska ochrany údajů by nebylo přijatelné, aby byla příslušná zařízení trvale připojena na síť a vozidla tím trvale sledovatelná kvůli možné aktivaci přístroje eCall“<sup>(25)</sup>. Je tudíž důležité dále ujasnit konkrétní okolnosti, za nichž bude vozidlo sledováno, a dopad sledování na uživatele. Použití lokalizačních zaří-

zení by v každém případě mělo být odůvodněno legitimní potřebou (např. sledování přepravy zboží) a důsledně omezeno pouze na aspekty, jež jsou pro dosažení tohoto účelu nezbytné. Proto je důležité přesně stanovit, které lokalizační údaje se shromažďují, kde a jak dlouho se uchovávají, kdo se účastní jejich výměny a za jakým účelem taková výměna probíhá; dále je důležité podniknout veškeré nezbytné kroky, aby nedošlo k nesprávnému použití údajů nebo k jejich zneužití.

47. Zpracování lokalizačních údajů týkajících se uživatelů veřejných komunikačních sítí nebo veřejně dostupných elektronických komunikačních služeb je navíc striktně upraveno v článku 9 směrnice 2002/58/ES. Zde se zejména vyžaduje, aby zpracování lokalizačních údajů probíhalo anonymně nebo případně za informovaného souhlasu dotyčného uživatele. To znamená, že před použitím lokalizačního nástroje musí být uživatelům poskytnuty příslušné informace zahrnující typ lokalizačních údajů, které budou zpracovávány, účel a délku doby zpracování a informaci o tom, zda budou údaje předány třetí osobě za účelem poskytování služeb s přidanou hodnotou. Zdarma musí být k dispozici jednoduché prostředky, které uživatelům umožní dočasně odmítnout zpracování lokalizačních údajů při každém připojení k síti nebo při každém přenosu sdělení. Zpracování lokalizačních údajů by mělo být přísně omezeno na osoby, které jednájí z pověření provozovatele veřejných komunikačních sítí nebo poskytovatele veřejně dostupných služeb elektronických komunikací nebo třetích osob, které poskytují služby s přidanou hodnotou.

48. Musí být přijaty další záruky, pokud dochází ke shromažďování lokalizačních údajů z vozidel využívaných v rámci zaměstnání, aby se předešlo tomu, že lokalizační technologie bude využita k neoprávněnému sledování zaměstnanců. Zpracování by se v každém případě mělo omezovat na lokalizační údaje shromážděné v pracovní době – zaměstnanci tím pádem musí mít možnost vypnout lokalizační funkci mimo pracovní dobu nebo v době, kdy vozidlo využívají pro soukromé účely.

49. Existuje riziko, že třetí strany (jako pojišťovny, zaměstnavatelé a donucovací orgány) budou vyžadovat přístup k údajům, jež byly shromážděny prostřednictvím navigačních a sledovacích systémů pro legitimní a konkrétní účely (jako sledování zboží, elektronická platba mýtného atd.), aby je využily pro sekundární účely, jako je kontrola doby jízdy a odpočinku nebo dodržování dopravních předpisů a ukládání sankcí. Přístup k údajům pro sekundární účely není v zásadě povolen, slouží-li tento přístup účelům, jež nejsou slučitelné s účely, pro něž byly údaje shromážděny. Odchylně od této zásady lze přístup povolit pouze v případech, že podmínky takového přístupu odpovídají

<sup>(23)</sup> Viz otázky ochrany soukromí a údajů uvedené ve spojitosti s použitím RFID ve stanovisku evropského inspektora ochrany údajů 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. [http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-12-20\\_RFID\\_CS.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-12-20_RFID_CS.pdf)

<sup>(24)</sup> Pracovní skupina zřízená podle článku 29, stanovisko k používání lokalizačních údajů v souvislosti s poskytováním služeb s přidanou hodnotou, WP 115, listopad 2005. [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2005/wp115\\_cs.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_cs.pdf)

<sup>(25)</sup> Viz dokument WP 125 o iniciativě eCall, s. 5, uvedený v poznámce pod čarou 10.



přísným požadavkům článku 13 směrnice 95/46/ES. V důsledku toho by veškerý přístup třetích stran k lokalizačním údajům měl být poskytován v souladu s právními předpisy a transparentním způsobem, na základě právního opatření stanovícího příslušné postupy a podmínky přístupu k údajům pro konkrétní účely a stanovícího dotčeným osobám přiměřené záruky s ohledem na další účely, pro něž by jejich údaje mohly být použity.

### III.2.b) Role a povinnosti subjektů účastnících se ITS

50. Dosud není zřejmé, kdo bude správcem údajů ve vztahu k jednotlivým částem zpracování. V mnoha případech budou správci údajů pravděpodobně poskytovatelé služeb ITS, ať již samostatně, pokud jde o osobní údaje zpracovávány za účelem poskytování vlastních služeb ITS, nebo společně v případech, kdy ke zpracování dochází ve spolupráci s dalšími správci údajů. Ve vztahu ke každé části zpracování by měly být jednoznačně stanoveny role a povinnosti provozovatelů zapojených do ITS na různých pozicích jako správci údajů a jako zpracovatelé údajů (např. provozovatelé telekomunikací poskytující komunikační služby i služby ITS).
51. Osoby vystupující jako správci údajů budou odpovědné<sup>(26)</sup> za zajištění toho, aby systémy a služby splňovaly všechny požadavky na ochranu údajů, a zejména za zavedení systémů vycházejících ze zásady „soukromí coby aspekt návrhu“, dodržujících zásady kvality údajů a omezení účelu a zajišťujících odpovídající úroveň bezpečnosti údajů, jak je popsáno v části III.1).
52. Bude třeba, aby správci údajů zajistili zavedení vhodných záruk na všech úrovních řetězce subjektů zapojených do zavádění ITS. To bude zejména vyžadovat, aby se všemi zúčastněnými stranami zapojenými do výměny a zpracování údajů uzavřeli vhodná smluvní ujednání, v nichž by záruky odpovídající ochrany údajů měly být stanoveny (zejména pokud jde o články 16 a 17 směrnice 95/46/ES a články 4 a 5 směrnice 2002/58/ES). Je důležité poukázat na to, že z hlediska ochrany údajů musí správci údajů sice zabezpečit, aby byla ochrana údajů zajištěna ve všech fázích zpracování, avšak zůstávají za zpracování odpovědní a nemohou se z této odpovědnosti smluvně vyvázat.

## IV. ZÁVĚRY

53. EIOÚ vítá navrhovaný plán na zavedení ITS, který předložila Komise a jehož cílem je harmonizace zpracování údajů v evropském měřítku v zájmu snazšího poskytování služeb ITS, přičemž na ochranu údajů je v tomto plánu kladen důraz jakožto na klíčovou podmínku řádného zavedení ITS v Evropě.

54. EIOÚ poukazuje na to, že návrh směrnice stanoví obecný rámec, s nímž vyvstávají mnohé otázky ochrany soukromí a údajů, jimž je třeba se věnovat na úrovni EU i na úrovni jednotlivých států:

- Vzniká riziko, že nejasnosti v souvislosti s navrhovaným právním rámcem povedou k odlišnostem v provádění ITS v Evropě, což povede k odlišným úrovním ochrany údajů v Evropě. EIOÚ zdůrazňuje, že tato témata je třeba dále harmonizovat na úrovni EU, aby mohly být vyjasněny nedorozumění otázky (jako například definice rolí a povinností subjektů v oblasti ITS, které konkrétní aplikace a systémy ITS musí být zabudovány do vozidel, vývoj harmonizovaných smluv pro poskytování služeb ITS, konkrétní účely a podmínky používání ITS atd.). Je zejména nutné stanovit, kdo budou správci údajů, pokud jde o prováděné zpracování údajů, neboť bude v odpovědnosti správců, aby zajistili uplatňování aspektů ochrany soukromí a údajů ve všech fázích řetězce zpracování.
- Rozhodnutí o určitých aspektech zpracování, jež by mohly mít významný dopad na práva osob na ochranu soukromí a údajů, by měla být přijímána v rámci Evropského parlamentu a Rady, nikoli v rámci postupu projednávání ve výborech.
- Je velmi důležité, aby ochrana soukromí a údajů byla zohledňována již od počáteční fáze zpracování údajů a ve všech jeho krocích; při tvorbě aplikací a systémů ITS by mělo být podporováno uplatňování zásady „soukromí coby aspekt návrhu“ a tato zásada by měla být začleněna do norem, osvědčených postupů, technických specifikací a systémů.
- Veškerá propojení aplikací a systémů by měla probíhat s řádným ohledem na zásady ochrany údajů a na praktické záruky bezpečnosti.
- Pokud jde o nejistotu, jež v této fázi v určitých otázkách přetrvává s ohledem na aspekty zavádění ITS, EIOÚ zejména vítá iniciativu předloženou Komisí ve sdělení, podle níž má být do roku 2011 provedeno hodnocení z hlediska soukromí. EIOÚ dále důrazně doporučuje, aby byla prováděna hodnocení dopadu z hlediska ochrany soukromí a údajů ve vztahu k jednotlivým oblastem nebo účelům využití, s cílem stanovit vhodná bezpečnostní opatření, a aby byly vyvíjeny nejlepší dostupné techniky pro otázky soukromí, ochrany údajů a bezpečnosti v ITS.
- Dále EIOÚ zdůrazňuje, že členské státy rovněž ponese odpovědnost za řádné provádění směrnice, aby provozovatelé EIOÚ mohli uplatňovat systémy a služby nabízející odpovídající úroveň ochrany údajů v celé Evropě.

<sup>(26)</sup> Viz poznámka pod čarou 13.

- Ze strany správců údajů poskytujících služby ITS by měly být uplatněny přiměřené záruky, aby použití lokalizačních technologií, jako je družicové určování polohy a štítky RFID, nenarušovalo soukromí osob využívajících vozidel pro zcela soukromé nebo pro pracovní účely. To bude zejména vyžadovat omezení zpracování na údaje naprosto nezbytné pro uvedený účel, zajištění toho, aby v systémech byla zabudována vhodná bezpečnostní opatření zamezující předání lokalizačních údajů neoprávněným příjemcům, a zajištění účinného prostředku, jímž budou uživatelé moci lokalizační zařízení či funkci deaktivovat.
55. EIOÚ doporučuje, aby byl článek 6 návrhu pozměněn v souladu se směrnicí 95/46/ES, a to takto:
- Při zpracování údajů v rámci ITS by měla být podpořována jejich minimalizace. Z tohoto hlediska se doporučuje změnit čl. 6 odst. 1 písm. b) návrhu takto: „Osobní údaje budou zpracovávány, pouze pokud je to nezbytné pro konkrétní účel, za kterým se ITS používá, přičemž se vychází z vhodného právního základu.“
- Je důležité, aby osobní údaje zpracovávané interoperabilními systémy nebyly používány za dalšími účely, jež by nebyly slučitelné s účely vedoucími ke shromáždění těchto údajů. Proto se doporučuje pozměnit čl. 6 odst. 2 takto: „a aby nesměly být použity pro jiné účely, než které vedly k jejich shromáždění, způsobem, jenž je s uvedenými účely neslučitelný.“
- EIOÚ doporučuje, aby byl v článku 6 návrhu učiněn výslovný odkaz na zásadu „soukromí coby aspekt návrhu“ , pokud jde o tvorbu aplikací a systémů ITS. Kromě toho doporučuje, aby pracovní skupina zřízená podle článku 29 a EIOÚ byli informováni a konzultováni v otázce dalších kroků podniknutých k tomuto tématu postupem projednávání ve výborech.
56. EIOÚ dále doporučuje, aby byl v odůvodnění návrhu uveden odkaz na tuto konzultaci.
57. S přihlédnutím k výše uvedenému EIOÚ doporučuje, aby orgány pro ochranu údajů – především prostřednictvím pracovní skupiny zřízené podle článku 29 – i EIOÚ byli úzce zapojeni do iniciativ spojených se zaváděním ITS, a to prostřednictvím konzultací v dostatečně rané fázi před vývojem relevantních opatření.
- V Bruselu dne 22. července 2009.
- Peter HUSTINX  
Evropský inspektor ochrany údajů