

# EURÓPSKY DOZORNÝ ÚRADNÍK PRE OCHRANU ÚDAJOV

**Stanovisko európskeho dozorného úradníka pre ochranu údajov k oznámeniu Komisie o akčnom pláne zavádzania inteligentných dopravných systémov v Európe a k sprievodnému návrhu smernice Európskeho parlamentu a Rady, ktorou sa ustanovuje rámec na zavedenie inteligentných dopravných systémov v oblasti cestnej dopravy a na rozhrania s inými druhmi dopravy**

(2010/C 47/02)

EURÓPSKY DOZORNÝ ÚRADNÍK PRE OCHRANU ÚDAJOV,

so zreteľom na Zmluvu o založení Európskeho spoločenstva, a najmä na jej článok 286,

so zreteľom na Chartu základných práv Európskej únie, a najmä na jej článok 8,

so zreteľom na smernicu Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov,

so zreteľom na smernicu Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 týkajúcu sa spracovávaní osobných údajov a ochrany súkromia v sektore elektronických komunikácií,

so zreteľom na nariadenie Európskeho parlamentu a Rady (ES) č. 45/2001 z 18. decembra 2000 o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi Spoločenstva a o voľnom pohybe takýchto údajov, a najmä na jeho článok 41,

so zreteľom na žiadosť Európskej komisie o stanovisko podľa článku 28 ods. 2 nariadenia (ES) č. 45/2001, ktorá bola doručená 11. februára 2009,

ZAUJAL TOTO STANOVISKO:

## I. ÚVOD

1. Komisia prijala 16. decembra 2008 oznámenie, ktorým vymedzuje akčný plán zavádzania inteligentných doprav-

ných systémov v Európe (ďalej len „oznámenie“) <sup>(1)</sup>. Oznámenie sprevádza návrh smernice Európskeho parlamentu a Rady, ktorou sa ustanovuje rámec na zavedenie inteligentných dopravných systémov v oblasti cestnej dopravy a na rozhrania s inými druhmi dopravy (ďalej len „návrh“) <sup>(2)</sup>. Komisia poslala oznámenie a sprievodný návrh EDPS na konzultáciu podľa článku 28 ods. 2 nariadenia (ES) č. 45/2001 <sup>(3)</sup>.

2. EDPS víta skutočnosť, že sa s ním konzultuje a odporúča, aby sa v odôvodneniach návrhu uviedol odkaz na túto konzultáciu podobne ako vo viacerých iných legislatívnych textoch, pri ktorých sa s ním konzultovalo podľa nariadenia (ES) č. 45/2001.

### I.1. Oznámenie Komisie o akčnom pláne zavádzania IDS v Európe

3. „Inteligentné dopravné systémy“ („IDS“) sú moderné aplikácie, ktoré využívajú informačné a komunikačné technológie (IKT), ktoré sú zabudované v rôznych druhoch dopravy na účely vzájomnej interakcie. V oblasti cestnej dopravy budú IDS poskytovať inovatívne služby pre jednotlivé druhy dopravy a riadenie premávky rozličným užívateľom, ako sú cestujúci, užívatelia a prevádzkovatelia infraštruktúry cestnej dopravy, správcovia vozových parkov a prevádzkovatelia pohotovostných služieb.

4. Komisia zhodnotila rastúce zavádzanie IDS v rôznych druhoch dopravy <sup>(4)</sup> v Európskej únii a prijala akčný plán na urýchlenie zavádzania a používania aplikácií a služieb IDS v oblasti cestnej dopravy. Plán si tiež kladie za cieľ

<sup>(1)</sup> KOM(2008) 886 v konečnom znení. Rada prijala závery o oznámení na 2935. zasadnutí Rady pre dopravu, telekomunikácie a energetiku 30. a 31. marca 2009.

<sup>(2)</sup> KOM(2008) 887 v konečnom znení.

<sup>(3)</sup> Nariadenie Európskeho parlamentu a Rady (ES) č. 45/2001 z 18. decembra 2000 o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi Spoločenstva a o voľnom pohybe takýchto údajov (Ú. v. ES L 8, 12.1.2001, s. 1).

<sup>(4)</sup> Existuje mnoho iniciatív na úrovni EÚ, ktorými sa integrujú IDS do rôznych druhov dopravy vrátane leteckej (SESAR), riečnej (RIS), železničnej (ERTMS TAF-TSI), nákladnej (VTMIS, AIS, LRIT) a cestnej dopravy (eToll, eCall), pozri KOM(2008) 886 v konečnom znení, s. 3.

zabezpečiť ich interakciu s inými druhmi dopravy, čo uľahčí poskytovanie multimodálnych služieb. Koherentné zavedenie IDS v Európe bude slúžiť rôznym cieľom Spoločenstva vrátane efektívnosti, udržateľnosti, bezpečnosti a bezpečnostnej ochrany dopravy, pričom podporí vnútorný trh a konkurencieschopnosť EÚ. Vzhľadom na rozmanitosť cieľov, ktoré sa sledujú pri zavádzaní IDS, sa v oznámení načrtáva šesť prioritných oblastí opatrení v období 2009 – 2014. Komisia na účely realizácie plánu navrhuje, aby sa prostredníctvom smernice vymedzil na úrovni EÚ právny rámec, v ktorom sa zafinuje istý počet opatrení vo vybraných prioritných oblastiach.

### 1.2. Návrh smernice, ktorou sa ustanovuje rámec na zavedenie inteligentných dopravných systémov v oblasti cestnej dopravy a na rozhrania s inými druhmi dopravy

5. Návrhom sa ustanovuje rámec pre nadnárodné zavádzanie aplikácií IDS, ktoré má uľahčiť poskytovanie harmonizovaných cezhraničných služieb, najmä pokiaľ ide o informácie o premávke a cestovné informácie a riadenie premávky. Požaduje sa v ňom, aby členské štáty prijali niekoľko technických opatrení, ktoré uľahčia výmenu údajov medzi užívateľmi, orgánmi verejnej moci, relevantnými zainteresovanými stranami a poskytovateľmi služieb IDS, a ktorými sa do vozidiel a cestnej infraštruktúry integrujú systémy IDS, ktoré sa týkajú bezpečnosti a bezpečnostnej ochrany. Technické špecifikácie pre aplikácie a systémy IDS v štyroch z prioritných oblastí<sup>(5)</sup> uvedených v akčnom pláne budú definované prostredníctvom komitologického postupu<sup>(6)</sup>, ktorého hlavné prvky sú uvedené v prílohe II. Konkrétne účely, na ktoré sa IDS budú v týchto oblastiach používať, však nie sú jasné. Okrem toho sa môže zavádzanie IDS rozšíriť do oveľa viac oblastí, ako sú uvedené štyri oblasti pôvodne vybrané s cieľom vypracovať harmonizované technické špecifikácie. Hoci sa návrh zaoberá najmä zavádzaním budúcich aplikácií a služieb IDS, musí tiež, ak je to možné, zahŕňať technológie, ktoré v tejto oblasti už existujú alebo sa v súčasnosti vyvíjajú (ako je systém eCall, eToll atď.).

6. Návrh bol poslaný Európskemu parlamentu, ktorý svoje stanovisko v prvom čítaní<sup>(7)</sup> prijal 23. apríla 2009. V nadväznosti na žiadosť o konzultáciu zaslanú Radou

<sup>(5)</sup> V článku 4 návrhu sa ustanovuje vymedzenie technických opatrení v týchto oblastiach: i) optimálne využívanie údajov o cestách, premávke a cestovaní; ii) kontinuita riadiacich služieb IDS v oblasti premávky a nákladnej prepravy v európskych dopravných koridoroch a mestských aglomeráciách; iii) bezpečnosť cestnej premávky a iv) integrácia vozidiel do dopravnej infraštruktúry.

<sup>(6)</sup> V návrhu sa ustanovuje použitie regulačného postupu s kontrolou podľa článku 5a ods. 1) až 4) a článku 7 rozhodnutia 1999/468/ES.

<sup>(7)</sup> Legislatívne uznesenie Európskeho parlamentu z 23. apríla 2009 o návrhu smernice Európskeho parlamentu a Rady, ktorou sa ustanovuje rámec na zavedenie inteligentných dopravných systémov v oblasti cestnej dopravy a na rozhrania s inými druhmi dopravy, T6-0283/2009.

29. januára 2009 prijal Európsky hospodársky a sociálny výbor svoje stanovisko k návrhu 13. mája 2009<sup>(8)</sup>.

### 1.3. Zameranie stanoviska

7. EDPS víta konzultácie o navrhovanom pláne zavádzania IDS, ktorý predložila Komisia. EDPS sa nezaobrá otázkami vznesenými v akčnom pláne pre IDS prvýkrát. EDPS vydal stanovisko k návrhu Komisie o zjednodušení cezhraničného presadzovania pravidiel v oblasti bezpečnosti cestnej premávky<sup>(9)</sup> a prispel k práci pracovnej skupiny zriadenej podľa článku 29 na pracovnom dokumente o systéme eCall<sup>(10)</sup>.
8. Inteligentné dopravné systémy sú založené na zhromažďovaní, spracúvaní a výmene najrôznejších údajov z verejných a súkromných zdrojov, predstavujú teda oblasť s intenzívnym využívaním údajov. Zavádzanie IDS bude do značnej miery založené na technológiách určovania zemepisnej polohy, napríklad satelitných, a bezkontaktných technológiách, ako napríklad RFID, ktoré umožnia poskytovanie rozličných verejných a/alebo komerčných služieb založených na znalosti polohy (napr. dopravné informácie poskytované v reálnom čase, eFreight, eCall, eToll, rezervácie parkovania atď.). Niektoré z informácií, ktoré budú spracúvané prostredníctvom IDS, budú agregované – napríklad informácie o premávke, nehodách a príležitostiach – a nesúvisia so žiadnym konkrétnym jednotlivcom, zatiaľ čo iné informácie sa budú týkať identifikovaných alebo identifikovateľných jednotlivcov, a preto sa považujú za osobné údaje v zmysle článku 2 písm. a) smernice 95/46/ES.
9. EDPS považuje za zásadné, aby opatrenia plánované v rámci zavádzania IDS boli v súlade s existujúcim právnym rámcem uvedeným v návrhu, najmä smernicou 95/46/ES o ochrane údajov<sup>(11)</sup> a smernicou 2002/58/ES o elektronickom súkromí<sup>(12)</sup>.

<sup>(8)</sup> Stanovisko Európskeho hospodárskeho a sociálneho výboru k návrhu smernice Európskeho parlamentu a Rady, ktorou sa ustanovuje rámec na zavedenie inteligentných dopravných systémov v oblasti cestnej dopravy a na rozhrania s inými druhmi dopravy, TEN/382, 13. mája 2009.

<sup>(9)</sup> Stanovisko európskeho dozorného úradníka pre ochranu údajov k návrhu smernice Európskeho parlamentu a Rady, ktorou sa zjednodušuje cezhraničné presadzovanie pravidiel v oblasti bezpečnosti cestnej premávky, 2008/C 310/02, Ú. v. EÚ C 310, 5.12.2008, s. 9.

<sup>(10)</sup> Pracovný dokument pracovnej skupiny zriadenej podľa článku 29 o ochrane údajov a dôsledkoch systému eCall na ochranu súkromia, WP 125, 26. septembra 2006. [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2006/wp125\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp125_en.pdf)

<sup>(11)</sup> Smernica Európskeho parlamentu a Rady 95/46/ES z 24. októbra 1995 o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov, Ú. v. ES L 281, 23.11.1995, s. 31.

<sup>(12)</sup> Smernica Európskeho parlamentu a Rady 2002/58/ES z 12. júla 2002 týkajúca sa spracovávaní osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách), Ú. v. ES L 201, 31.7.2002, s. 37.

10. Komisia ako jednu z hlavných prekážok presadzovania IDS identifikovala nevyriešené otázky týkajúce sa súkromia a ochrany údajov. Tieto otázky budú v tomto stanovisku rozpracované takto:

— v kapitole II sa analyzuje právny rámec predložený Komisiou na účely zavádzania IDS z hľadiska ochrany údajov,

— kapitola III je zameraná na obavy spojené s ochranou údajov, ktoré sa musia ďalej riešiť s cieľom správneho zavádzania IDS:

— v prvom bode stanoviska sa zdôrazňuje potreba, aby sa pri vývoji IDS dodržiavala zásada „ochrany súkromia už v štádiu návrhu“, a načrtávajú sa ďalšie dôležité otázky, ktoré treba riešiť pri vývoji aplikácií a systémov spracovania údajov v rámci IDS,

— druhý bod sa zameriava na niektoré úvahy týkajúce sa súkromia, ktorými je potrebné ďalej sa zaoberať v oblasti poskytovania služieb IDS.

## II. ANALÝZA PRÁVNEHO RÁMCA NAVRHOVANÉHO PRE ZAVÁDZANIE IDS

11. Návrh smernice predložený Komisiou obsahuje dve ustanovenia (odôvodnenie 9 a článok 6), ktoré sa zaoberajú ochranou súkromia, bezpečnosťou a opätovným používaním informácií. V článku 6 ods. 1 návrhu Komisie sa vyžaduje, aby sa prevádzka IDS uskutočňovala v súlade s pravidlami na ochranu údajov ustanovenými okrem iného v smernici 95/46/ES a smernici 2002/58/ES. V návrhu Komisie sa v článku 6 ods. 2 ustanovujú konkrétne opatrenia na ochranu údajov najmä z bezpečnostného hľadiska: uvádza sa v ňom, že „členské štáty predovšetkým zabezpečia, aby boli údaje a záznamy IDS chránené pred zneužitím vrátane nezákonného prístupu, zmeny alebo straty“. Nakoniec, v článku 6 ods. 3 návrhu Komisie sa ustanovuje: „Uplatňuje sa smernica 2003/98/ES.“

12. Európsky parlament navrhol v prvom čítaní pozmeňujúce a doplnujúce návrhy týkajúce sa článku 6. Ide najmä o tri nové odseky doplnené k článku 6 ods. 1, ktoré sa týkajú používania prípadných anonymných údajov, spracovania

citlivých údajov až po udelení informovaného súhlasu dotknutej osoby a zabezpečenia toho, aby sa osobné údaje spracúvali, iba „ak je toto spracúvanie nevyhnutné na fungovanie aplikácií a/alebo služieb IDS“. Okrem toho sa mení článok 6 ods. 2, do ktorého sa dopĺňa, že údaje a záznamy IDS „nesmú byť použité na iné účely, než tie, ktoré sú uvedené v tejto smernici“.

13. EDPS víta skutočnosť, že ochrana údajov sa pri príprave návrhu zohľadnila a že je v návrhu prezentovaná ako všeobecná podmienka pre správne zavedenie IDS v Európe. EDPS uznáva, že na účely zabezpečenia funkčnosti aplikácií a služieb IDS v celej Európe je potrebné dosiahnuť ucelenú harmonizáciu dátových procesov na úrovni EÚ.

14. EDPS však konštatuje, že navrhovaný právny rámec je príliš široký a všeobecný na to, aby sa ním mohlo primerane reagovať na obavy o ochranu súkromia a údajov, ktoré vyvoláva zavádzanie IDS v členských štátoch. Nie je jasné, v akej situácii výkon služieb IDS povedie k zhromažďovaniu a spracúvaniu osobných údajov, aké sú konkrétne účely, na ktoré sa spracúvanie údajov vykonáva, ani aký právny základ opodstatňuje takéto spracúvanie. Okrem toho používanie technológií na určovanie polohy v rámci zavádzania IDS zvyšuje riziko vývoja služieb, ktoré narušujú ochranu súkromia, ak je ich súčasťou zhromažďovanie a výmena osobných údajov. V návrhu sa navyše jasne neustanovujú úlohy a povinnosti rozličných subjektov zasahujúcich do reťazca zavádzania IDS, a preto je ťažké zistiť, ktoré subjekty budú kontrolórmí údajov a budú preto zodpovedné<sup>(13)</sup> za dodržiavanie povinností v oblasti ochrany údajov. Prevádzkovatelia IDS budú čeliť značným problémom, ak všetky tieto otázky nebudú právne objasnené, pretože v konečnom dôsledku budú za uplatňovanie opatrení ustanovených v navrhovanej smernici zodpovední oni.

15. Existuje teda riziko, že nejasnosť navrhovaného právneho rámca spôsobí rôznorodosť prístupov pri zavádzaní IDS v Európe, a že namiesto znižovania rozdielov medzi členskými štátmi bude vzhľadom na odlišné úrovne ochrany osobných údajov v Európe naopak viesť k značnej neistote, roztrieštenosti a nekonzistentnosti. To môže viesť aj k nedodržiavaniu základných záruk v oblasti ochrany údajov. EDPS zdôrazňuje potrebu ďalšej harmonizácie v týchto otázkach na úrovni EÚ. EDPS týmto navrhuje úpravy navrhovaného právneho rámca z hľadiska ochrany údajov. Dôrazne odporúča, aby Parlament a Rada vložili do návrhu navrhované zmeny, ako aj, kde je to možné, ďalšie ustanovenia na objasnenie nevyriešených otázok (napr. vymedzenia a povinnosti aktérov v oblasti IDS, vypracovanie harmonizovaných zmlúv na poskytovanie služieb

<sup>(13)</sup> Podľa článku 2 písm. d), 6 ods. 2 a článku 23 smernice 95/46/ES uvedenej v poznámke pod čiarou č. 11.

IDS atď.). Ďalej zdôrazňuje, že členské štáty budú tiež niesť zodpovednosť za riadne vykonávanie smernice tak, aby operátori mohli vyvinúť systémy a služby, ktoré poskytujú primeranú úroveň ochrany údajov v celej Európe.

### II.1. Činnosti spracúvania údajov musia spočívať na vhodnom právnom základe

16. Nie je jasné, kedy po integrovaní zariadenia IDS do vozidla sa spracúvanie osobných údajov začne, ani na akom právnom základe sa bude spracúvanie vykonávať. Subjekty sa môžu spoliehať na rôzne právne základy spracúvania údajov, okrem iného jednoznačný súhlas užívateľov, zmluvu alebo právny záväzok, ktorý musí kontrolór dodržiavať. Je potrebné harmonizovať právny základ, na ktorom sa bude spracúvanie údajov prostredníctvom IDS vykonávať, aby bolo zabezpečené, že systémy budú fungovať v celej Európe a že užívatelia nebudú trpieť rozdielmi v spôsobe spracúvania v jednotlivých krajinách EÚ.
17. V mnohých prípadoch budú systémy IDS integrované do vozidiel štandardne. To platí najmä pre systémy IDS súvisiace s bezpečnosťou a bezpečnostnou ochranou, ktoré musia byť podľa návrhu zabudovanou súčasťou vozidla. Návrh však „systémy IDS súvisiace s bezpečnosťou a bezpečnostnou ochranou“ nevymedzuje, a preto by sa malo lepšie objasniť, ktoré konkrétne aplikácie a systémy IDS musia byť zabudovanou súčasťou vozidla. Okrem toho by sa malo objasniť, či aktivácia a používanie zariadení budú pre užívateľov dobrovoľné alebo povinné. Voľba povinného spracúvania údajov by sa mala prijať len na špecifické účely, po zväžení presvedčivých dôvodov (napr. kvalitné sledovanie nákladnej dopravy) a spolu so zodpovedajúcimi zárukami, pokiaľ ide o spracúvanie údajov týkajúcich sa jednotlivcov. Ak by sa IDS používali na základe dobrovoľnosti, mali by sa prijať vhodné záruky, aby sa zabránilo tomu, že len z dôvodu samotnej prítomnosti systému vo vozidle sa budú jeho užívatelia považovať za subjekty, ktoré implicitne súhlasia s jeho použitím.
18. EDPS uprednostňuje, aby sa služby IDS poskytovali na základe dobrovoľnosti. To znamená, že užívatelia musia mať možnosť slobodne súhlasiť s použitím systému a s konkrétnymi účely, na ktoré sa bude používať. Ak poskytovaná služba vychádza z údajov o polohe, musia sa užívateľom poskytnúť primerané informácie (najmä v súlade s článkom 9 smernice 2002/58/ES), pričom užívatelia musia mať možnosť, aby takýto súhlas vzali späť. V praxi si to vyžaduje zavedenie jednoduchého spôsobu deaktivácie zariadenia a/alebo príslušnej funkcie v prípade, že užívateľ prestane súhlasiť s používaním systému a/alebo konkrétnej funkcie, bez toho, aby to pre neho predstavovalo technické alebo finančné obmedzenie<sup>(14)</sup>. Mali by sa zaviesť ďalšie záruky, aby užívatelia neboli diskriminovaní, keď odmietnu používať nejakú službu.
19. V prípade, že niektoré činnosti spracúvania sú povinné a iné podliehajú súhlasu užívateľa, sa musí zabezpečiť

transparentnosť v otázke rôznych vykonávaných operácií spracúvania tým, že sa užívateľom poskytnú primerané informácie o povinnej alebo dobrovoľnej povahe každého konkrétneho spracovania, ako aj rozsah takéhoto spracovania. Okrem toho bude veľmi dôležité zaviesť primerané bezpečnostné záruky, aby sa žiadne údaje nezhrádzovali ani nespracúvali nad právne vymedzený a/alebo dobrovoľne odsúhlasený rámec.

20. Vzhľadom na nadnárodný vplyv služieb IDS EDPS okrem toho odporúča vypracovanie celoeurópskych štandardných zmlúv s cieľom zabezpečiť, aby služby poskytované prostredníctvom IDS ponúkali rovnaké záruky ochrany osobných údajov v celej Európe, a najmä zabezpečiť, aby informácie poskytované užívateľom o konkrétnych používaných funkciách, vplyve používania konkrétnych technológií na ochranu ich údajov a spôsobe, akým si môžu uplatniť svoje práva, boli dostatočne zrozumiteľné. Keď sa pridávajú nové funkcie, poskytovatelia služieb by mali prijať ďalšie kroky s cieľom poskytnúť užívateľom jasné a konkrétne informácie o takýchto nových funkciách a získať ich príslušný súhlas s ich používaním.

### II.2. Účely a spôsoby spracúvania údajov sa musia presnejšie vymedziť

21. EDPS konštatuje, že v návrhu nie je presné vymedzenie konkrétnych služieb a účelov, na ktoré by sa mohli aplikácie IDS používať, tieto sa teda ponechali otvorené. To umožňuje flexibilitu v praxi, ale znamená to, že nevyriešené otázky ochrany súkromia a osobných údajov – ktoré Komisia identifikovala ako jednu z hlavných prekážok presadzovania IDS (pozri bod 10) – môžu zostať nevyriešené a mohli by brániť vyváženému vykonávaniu navrhovaných opatrení.
22. EDPS zdôrazňuje, že je obzvlášť dôležité, aby sa operácie spracúvania vykonávané na účely poskytovania špecifických služieb IDS nevykonávali len v súlade so zodpovedajúcim právnym základom, ale aj na konkrétne, explicitné a zákonné účely, a aby plánované spracúvanie bolo z hľadiska týchto účelov primerané a nevyhnutné (článok 6 smernice 95/46/ES). Mala by sa preto zväziť možná potreba ďalších právnych predpisov na úrovni EÚ, pokiaľ ide o špecifické využitia IDS, s cieľom ustanoviť harmonizovaný a zodpovedajúci právny základ pre činnosti spracúvania, ktoré sa majú vykonávať, a aby sa predišlo nezrovnalostiam pri zavádzaní služieb IDS medzi členskými štátmi.
23. V navrhovanom rámci zatiaľ neexistuje žiadne rozhodnutie o spôsoboch spracúvania a výmene údajov na účely používania IDS. O množstve technických parametrov, ktorých voľba bude mať rôzne účinky na ochranu súkromia a údajov, sa rozhodne neskôr prostredníctvom komitologického postupu. Vzhľadom na skutočnosť, že ochrana súkromia a údajov je osobitne hájená ako základné právo v článku 8 Európskeho dohovoru o ochrane ľudských práv

<sup>(14)</sup> Pozri stanovisko pracovnej skupiny zriadenej podľa článku 125 k systému eCall, pozn. pod čiarou č. 10.

a základných slobôd a v článkoch 7 a 8 Charty základných práv Európskej únie, možno spochybníť, či a do akej miery by sa o vymedzení operácií spracúvania údajov malo rozhodovať prostredníctvom komitologického postupu.

24. V demokratickej spoločnosti by sa rozhodnutia o základných princípoch a podmienkach, ktoré ovplyvňujú základné práva, malo rozhodovať v rámci úplného legislatívneho postupu, ktorý zahŕňa príslušné kontroly a protiváhy. V tomto prípade to znamená, že rozhodnutia, ktoré majú zásadný vplyv na ochranu súkromia a údajov, ako sú rozhodnutia o účele a spôsoboch povinného spracúvania údajov a vymedzenie spôsobov zavádzania IDS v nových oblastiach, by mal prijímať Európsky parlament a Rada, a nie výbory prostredníctvom komitologického postupu.
25. EDPS preto dôrazne odporúča, aby sa pracovná skupina zriadená podľa článku 29 a EDPS v relevantných prípadoch podieľali na práci výboru zriadeného podľa článku 8 návrhu a na budúcich krokoch prijatých v oblasti zavádzania IDS prostredníctvom konzultácií v dostatočne skoréj fáze pred vypracovaním príslušných opatrení.
26. EDPS okrem toho berie na vedomie pozmeňujúce a doplnujúce návrhy, ktoré Európsky parlament prijal vo vzťahu k článku 6 návrhu. EDPS pre začiatok konštatuje, že aj keď je pozmeňujúci a doplnujúci návrh týkajúci sa podpory používania anonymných údajov v prípadoch, keď je to vhodné, v zásade veľmi vítaný, nevyrieši všetky obavy o ochranu údajov, pretože mnohé údaje zhromažďované a vymieňané prostredníctvom IDS možno považovať za osobné údaje. Ak sa má spracúvanie osobných údajov vykonávať na anonymnom základe, žiadna osoba nemôže mať v žiadnej fáze spracovania – berúc do úvahy všetky prostriedky, ktoré môže s primeranou pravdepodobnosťou použiť kontrolór alebo akákoľvek iná osoba – možnosť prepojiť spracúvané údaje s údajmi týkajúcimi sa nejakého identifikovaného jednotlivca, inak tieto údaje predstavujú osobné údaje v zmysle článku 2 písm. a) smernice 95/46/ES<sup>(15)</sup>. EDPS ďalej na základe pozmeňujúcich a doplnujúcich návrhov Európskeho parlamentu odporúča, aby sa článok 6 návrhu zmenil a doplnil takto:

— Malo by sa vykonať posúdenie potreby spracúvania osobných údajov prostredníctvom IDS z hľadiska zákonných a konkrétnych účelov, na ktoré sa údaje spracúvajú (v súlade s článkami 6 a 7 smernice

95/46/ES). Výkonnosť aplikácie IDS<sup>(16)</sup> nemôže byť sama o sebe zákonným účelom odôvodňujúcim spracúvanie údajov, keďže aplikácia je iba prostriedkom zhromažďovania a výmeny údajov, ktorého použitie by malo byť nevyhnutne zamerané na konkrétne účely.

— Pozmeňujúci a doplnujúci návrh<sup>(17)</sup> týkajúci sa zákazu používania údajov a záznamov IDS „na iné účely, než tie, ktoré sú uvedené v tejto smernici“ neposkytuje dostatočné záruky, najmä pretože špecifické účely a služby, pre ktoré sa bude IDS používať, nie sú v smernici jasne a vyčerpávajúco vymedzené. Vzhľadom na to, že prostredníctvom IDS sa budú vykonávať rôzne činnosti spracúvania údajov na veľmi odlišné účely, by sa malo zabezpečiť, aby sa údaje zhromaždené v priebehu spracúvania na jeden konkrétny účel nepoužívali na iné, nezlučiteľné účely, ako sa ustanovuje v článku 6 ods. 1 písm. b) smernice 95/46/ES. EDPS preto odporúča, aby sa článok 6 ods. 2 ďalej upravil tak, aby sa zabezpečilo, aby sa údaje a záznamy IDS nepoužívali „na iné účely, ako tie, na ktoré boli zhromaždené, spôsobom nezlučiteľným s takýmito účelmi“.

### III. OCHRANA ÚDAJOV V INTELIGENTNÝCH DOPRAVNÝCH SYSTÉMOCH

27. Je obzvlášť dôležité, aby sa objasnili úlohy jednotlivých aktérov zapojených do IDS, aby sa určilo, kto ponese zodpovednosť za zabezpečenie toho, aby systémy fungovali správne z hľadiska ochrany údajov. Preto by sa malo lepšie objasniť, kto by mal byť zodpovedný za implementáciu aplikácií a systémov, ktorých technický návrh bude upresnený prostredníctvom komitológie, a kto v reťazci aktérov bude zodpovedný za súlad spracúvania údajov s právnymi predpismi o ochrane údajov (t. j. kto budú kontrolóri údajov). EDPS nižšie zdôrazní určité obavy o ochranu súkromia a údajov, ktoré by sa mali riešiť v rámci komitológie a zo strany kontrolórov údajov pri navrhovaní aplikácií a systémov architektúry. Ďalej načrtne niektoré z otázok ochrany údajov, ktoré musia riešiť zákonodarcovia a kontrolóri údajov vo vzťahu k poskytovaniu služieb IDS.

#### III.1. „Ochrana súkromia už v štádiu návrhu“

28. Správne uplatňovanie zásad ochrany údajov ustanovených v smernici 95/46/ES je kľúčovou podmienkou úspešného zavedenia IDS v Spoločenstve. Tieto zásady vplyvajú na návrhy architektúry a aplikácií systémov. EDPS odporúča, aby sa v ranom štádiu navrhovania IDS zaujal prístup „ochrana súkromia už v štádiu návrhu“, ktorým by sa

<sup>(15)</sup> Ako sa uvádza v odôvodnení 26 smernice 95/46/ES: „keďže k určeniu, či je osoba identifikovateľná, by sa mali vziať do úvahy všetky prostriedky, u ktorých je primeraná pravdepodobnosť, že ich využije kontrolór alebo ľubovoľná iná osoba na identifikáciu príslušnej osoby“.

<sup>(16)</sup> V pozmeňujúcom a doplnujúcom návrhu 34 sa zavádza nový článok 6 ods. 1b: „Osobné údaje sa môžu spracúvať iba to tej miery, do akej je toto spracúvanie nevyhnutné na fungovanie aplikácií a/alebo služieb IDS.“

<sup>(17)</sup> Pozmeňujúcim a doplnujúcim návrhom 36 sa v článku 6 ods. 2 dopĺňa tento text: „a aby sa nesmeli použiť na iné účely než tie, ktoré sú uvedené v tejto smernici“.

- definovala štruktúra, prevádzka a riadenie príslušných aplikácií a systémov. Tento prístup je zdôraznený najmä v smernici 1999/5/ES<sup>(18)</sup>, pokiaľ ide o návrhy rádiových a koncových telekomunikačných zariadení.
29. Navrhovanie aplikácií a systémov IDS bude prebiehať v niekoľkých fázach, pričom ho budú realizovať rôzni aktéri, a každý z nich by mal brať do úvahy ochranu súkromia a údajov. Komisia a výbor pre IDS budú mať prostredníctvom komitologického postupu osobitnú počiatočnú zodpovednosť za vymedzenie opatrení, iniciatív v oblasti normalizácie, procedúr a najlepších postupov, ktoré by mali podporovať prístup „ochrana súkromia už v štádiu návrhu“.
30. Prístup „ochrana súkromia už v štádiu návrhu“ by sa mal podporovať vo všetkých fázach a vo všetkých podobách procesov:
- Na organizačnej úrovni by sa malo prihliadať na ochranu súkromia pri definícii postupov potrebných na výmenu údajov medzi všetkými relevantnými bodmi výmeny – to môže mať priamy vplyv na druh výmeny a údajov, ktoré sa budú vymieňať.
  - Požiadavky na ochranu súkromia a bezpečnostné požiadavky by mali byť začlenené do noriem, najlepších postupov, technických špecifikácií a systémov.
  - Na technickej úrovni EDPS odporúča vypracovanie, napríklad prostredníctvom komitologického postupu, najlepších dostupných postupov<sup>(19)</sup> v oblasti ochrany súkromia a údajov a bezpečnosti v konkrétnych sektoroch a/alebo na konkrétne účely, v ktorých by boli definované rôzne bezpečnostné parametre, ktoré sa musia implementovať počas celého životného cyklu systému s cieľom zaručiť súlad s regulačným rámcom EÚ.
31. EDPS nižšie načrtáva niektoré z otázok, ktoré sa musia pri navrhovaní aplikácií a architektúry systémov osobitne riešiť. Týkajú sa zhromaždených údajov, interoperability systémov a bezpečnosti údajov.
- III.1.a) *Minimalizácia údajov a anonymita*
32. Podľa článku 6 ods. 1 písm. c) smernice 95/46/ES možno zhromažďovať a spracúvať iba osobné údaje, ktoré sú nevyhnutné a relevantné pre konkrétne účely.
33. EDPS zdôrazňuje, že ešte pred navrhnutím aplikácií a systémov je dôležité vykonať zodpovedajúcu klasifikáciu informácií a údajov, ktoré majú byť spracúvané prostredníctvom IDS, aby sa predišlo rozsiahlemu a neprimeranému zhromažďovaniu osobných údajov. V tejto súvislosti by sa malo prihliadať na:
- zdroj údajov (či už pochádzajú z verejných zdrojov, od poskytovateľov telekomunikačných služieb, poskytovateľov služieb IDS, iných subjektov, z vozidiel, od užívateľov vozidiel alebo iných dotknutých osôb),
  - povahu údajov (napr. agregované informácie, anonymné údaje, osobné údaje, citlivé údaje),
  - účel(y), na ktoré sa údaje zamýšľajú použiť, a
  - pokiaľ ide o spolupracujúce systémy, malo by sa objasniť, aké údaje systémy vysielajú do vozidla a odosielajú z vozidla, aké údaje sa vymieňajú s iným vozidlom a/alebo infraštruktúrou a medzi jednotlivými infraštruktúrami a na aké účely sa vymieňajú.
34. S cieľom posúdiť potrebu zhromažďovania osobných údajov by sa jednotlivé funkcie mali starostlivo zanalyzovať z hľadiska účelov, ktoré majú spĺňať. EDPS zdôrazňuje, že je dôležité nájsť správnu rovnováhu medzi základnými právami dotknutých osôb a záujmami rôznych aktérov zapojených do IDS, čo implikuje, že by sa mal spracúvať najmenší možný objem osobných údajov. Je potrebné, aby bola architektúra aplikácií a systémov v čo najväčšej miere navrhnutá tak, aby sa zhromažďovali iba osobné údaje, ktoré sú nevyhnutne potrebné na účely, ktoré sa majú splniť.
35. Ak osobné údaje nie sú potrebné alebo sú potrebné len v počiatočnom štádiu spracúvania, nemali by sa zhromažďovať alebo by sa mali čo najskôr anonymizovať. Preto je mimoriadne dôležité nielen posudzovať potrebu zhromažďovania údajov, ale aj ich uchovávanie v rôznych systémoch. Pre všetkých rôznych aktérov v rámci reťazca služieb by sa mali vymedziť osobitné lehoty na uchovávanie osobných údajov, ktoré by sa mali líšiť v závislosti od typu údajov a účelu, na ktorý boli zhromaždené<sup>(20)</sup>. Ak teda zanikne potreba uchovávať osobné údaje na dosiahnutie účelov, na ktoré boli zhromaždené alebo ďalej spracované, mali byť anonymizované, t. j. nesmú sa viac vzťahovať na identifikovaného alebo identifikovateľného jednotlivca.
36. Návrh architektúry systémov a postupov výmeny údajov by mal podporovať spracúvanie najmenšieho možného objemu osobných údajov. V tejto súvislosti by sa mali brať do úvahy všetky fázy spracúvania a všetci aktéri v reťazci poskytovania služieb IDS. Zatiaľ čo niektoré údaje je možné vymieňať a spracúvať na anonymnom základe, iné údaje, i keď sa vymieňajú na neidentifikovanom základe, možno prepojiť s údajmi vzťahujúcimi sa na identifikovaných jednotlivcov, a preto predstavujú osobné údaje v zmysle článku 2 písm. a) smernice

<sup>(18)</sup> Ide najmä o článok 3 ods. 3 písm. c) smernice Európskeho parlamentu a Rady 1999/5/ES z 9. marca 1999 o rádiovom zariadení a koncových telekomunikačných zariadeniach a o vzájomnom uznávaní ich zhody.

<sup>(19)</sup> Pod pojmom najlepšie dostupné postupy sa rozumie najúčinnejšia a najpokročilejšia fáza vývoja činností a metód ich vykonávania, ktoré poukazujú na praktickú vhodnosť konkrétnych postupov ako základu pre aplikácie a systémy IDS z hľadiska zabezpečenia ich súladu s požiadavkami regulačného rámca EÚ v oblasti ochrany súkromia, údajov a bezpečnosti.

<sup>(20)</sup> Napríklad uchovávanie údajov o premávke a polohe spracovaných v súvislosti s poskytovaním verejne dostupných elektronických komunikačných služieb vo verejných komunikačných sieťach je upravené v smernici Európskeho parlamentu 2006/24/ES a Rady z 15. marca 2006 o uchovávaní údajov vytvorených alebo spracovaných v súvislosti s poskytovaním verejne dostupných elektronických komunikačných služieb alebo verejných komunikačných sietí a o zmene a doplnení smernice 2002/58/ES.

95/46/ES<sup>(21)</sup>. Vzhľadom na účel, na ktorý sa budú IDS využívať, sa zdá byť ťažké zabezpečiť, že veľké množstvo údajov zhromaždených prostredníctvom IDS sa bude spracúvať na anonymnom základe, keďže totožnosť jednotlivca bude v určitom bode potrebná na špecifické účely, napríklad pri fakturácii. Vyžadovalo by si to teda aspoň prijatie zvláštnych technických, organizačných a právnych opatrení na zabezpečenie anonymity v niektorých oblastiach.

### III.1.b) Interoperabilita, kvalita údajov a obmedzenie účelu

37. Interoperabilita aplikácií a systémov je kľúčovým prvkom úspešného zavedenia IDS. Vykoná sa harmonizácia, prostredníctvom ktorej sa vymedzia technické špecifikácie rozhraní, ktoré sa majú integrovať do aplikácií a systémov, aby mohli spolupracovať s ostatnými aplikáciami a/alebo systémami zabudovanými do iných druhov dopravy. Interoperabilita systémov na jednej strane pomôže uľahčiť poskytovanie rôznych služieb a prispeje k zabezpečeniu ich kontinuity v celej Európe, na druhej strane však predstavuje niekoľko rizík z hľadiska ochrany údajov, ako je napr. riziko úmyselného zneužitia údajov alebo ich zneužitia z nedbanlivosti. Všetky prepojenia databáz by sa mali realizovať s náležitým zreteľom na zásady ochrany údajov<sup>(22)</sup> a praktické bezpečnostné záruky [pozri tiež bod III.1.c)].
38. V kontexte interoperability aplikácií a systémov je obzvlášť dôležitá zásada kvality údajov vyjadrená v článku 6 písm. d) smernice 95/46/ES. Technické špecifikácie, ktoré sa vymedzia pre návrh rozhraní, by mali zabezpečiť správnosť údajov, ktoré sa získajú ako výsledok prepojenia aplikácií a systémov.
39. Vzhľadom na skutočnosť, že interoperabilita systémov uľahčí prepojenie databáz a spájanie údajov na ďalšie účely, EDPS zdôrazňuje, že každé prepojenie by sa malo realizovať za starostlivého zváženia zásady obmedzenia účelu ustanovenej v článku 6 ods. 1 písm. b) smernice 95/46/ES. Je obzvlášť dôležité, aby návrh architektúry systémov IDS bránil akémukoľvek ďalšiemu použitiu údajov na iné účely, než na ktoré boli zhromaždené. Do systémov musia byť vbudované primerané bezpečnostné ochrany, aby sa predišlo zneužitiu, neoprávnenému zverejneniu alebo prístupu, ako aj vedľajším účinkom používania zariadení. Napríklad by sa mali implementovať dostatočné ochranné opatrenia, aby neoprávnené tretie strany nemali prístup k prenosným zariadeniam a nepoužívali ich na identifikáciu a sledovanie osôb na účely, ktoré nie sú v rámci systému prípustné.
40. Pokiaľ ide o zákonnosť prepojení samotných, bude ich potrebné posudzovať jednotlivo a s prihliadnutím na

charakter údajov, ktoré sa sprístupňujú a vymieňajú prostredníctvom systémov, a na účely, na ktoré sa majú podľa pôvodného určenia využívať.

### III.1.c) Bezpečnosť údajov

41. Bezpečnosť osobných údajov je kľúčovým prvkom zavádzania IDS. EDPS víta skutočnosť, že v akčnom pláne aj v návrhu smernice sa bezpečnosť výslovne spomína. Bezpečnosť by sa mala zabezpečiť nielen počas fungovania zariadenia IDS (v systéme zabudovanom do vozidla a v komunikačnom dopravnom protokole), ale aj po tom, čo zariadenie prestane fungovať – v databázach, v ktorých sa údaje spracúvajú a/alebo uchovávajú. Pre všetky fázy spracúvania by sa mali vymedziť vhodné technické, administratívne a organizačné požiadavky, ktoré zabezpečia primeranú úroveň bezpečnosti v súlade s článkami 16 a 17 smernice 95/46/ES (v prípade potreby aj s článkami 4 a 5 smernice 2002/58/ES).
42. Vymedzenie vhodných bezpečnostných opatrení by sa malo vykonať až po starostlivom posúdení konkrétnych účelov, na ktoré sa budú IDS používať, ako aj po posúdení spôsobov spracúvania. EDPS v tejto súvislosti odporúča, aby sa pre určité odvetvia a/alebo účely použitia (napr. pre systémy IDS súvisiace s bezpečnostnou ochranou alebo pre systémy riadenia nákladnej dopravy) vypracovali posúdenia vplyvu na ochranu súkromia a údajov. Vypracovanie posúdení vplyvu na ochranu súkromia a údajov a využívanie najlepších dostupných postupov v oblasti ochrany súkromia a údajov prispeje k vymedzeniu najvhodnejších bezpečnostných opatrení týkajúcich sa konkrétnych vykonávaných operácií spracúvania.

### III.2. Ďalšie úvahy o ochrane údajov a súkromia v súvislosti s poskytovaním služieb IDS

43. Aby sa predišlo nezrovnalostiam pri zavádzaní služieb IDS, je na úrovni EÚ potrebná ďalšia harmonizácia spôsobov ich zavádzania. V tejto súvislosti by EDPS chcel poukázať na dva problémy, ktoré budú vyžadovať ďalšie zváženie z hľadiska ochrany súkromia a údajov:
- Použitie nástrojov na určovanie polohy na poskytovanie verejných a komerčných služieb založených na informáciách o polohe si vyžaduje zavedenie dodatočných záruk. V tejto súvislosti je potrebné venovať osobitnú pozornosť skutočnosti, či a kedy sa služby IDS založené na informáciách o polohe používajú na súkromné prípadne profesionálne účely, a aký vplyv môže mať používanie takéhoto systému na jednotlivcov, ktorí používajú vozidlá v profesionálnom kontexte.
  - V prípade integrovaných systémov je obzvlášť dôležité, aby sa objasnili úlohy a povinnosti jednotlivých strán zapojených do zavádzania IDS.

<sup>(21)</sup> Pozri poznámku pod čiarou č. 15.

<sup>(22)</sup> Pozri tiež stanovisko EDPS k oznámeniu Komisie o interoperabilite európskych databáz, 10. marec 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)

III.2.a) Záruky v oblasti používania nástrojov na určovanie polohy pri poskytovaní služieb IDS založených na informáciách o polohe

44. Zavádzaním IDS sa podporí vývoj aplikácií na sledovanie a stopovanie tovaru a umožní zavádzanie komerčných a verejných služieb založených na informáciách o polohe. Tieto služby budú využívať technológie, ako napr. satelitné systémy na určovanie polohy a značky RFID<sup>(23)</sup>. Navigačné systémy a systémy na sledovanie a stopovanie sú určené na použitie na rôzne účely, napríklad diaľkové monitorovanie trasy vozidiel a nákladu (napr. pri preprave nebezpečného tovaru alebo živých zvierat), fakturáciu vozidiel na základe rôznych parametrov vrátane prejazdenej vzdialenosti a dennej doby (napr. spolplatňovanie používania ciest, elektronické systémy na výber mýta), a sledovanie vodičov na účely presadzovania právnych predpisov, ako je kontrola doby vedenia vozidla (prostredníctvom digitálnych tachografov) a ukládanie sankcií (cez elektronickú identifikáciu vozidiel).

45. Použitie technológií určovania polohy je obzvlášť problematické z hľadiska ochrany súkromia, pretože umožňuje sledovanie vodičov a zhromažďovanie najrôznejších údajov týkajúcich sa ich vodičských návykov. Ako zdôraznila pracovná skupina zriadená podľa článku 29<sup>(24)</sup>, spracúvanie údajov o polohe je obzvlášť citlivá záležitosť obsahujúca kľúčovú otázku anonymného voľného pohybu, ktorá si vyžaduje zavedenie osobitných záruk s cieľom zabrániť sledovaniu osôb a zneužívaniu údajov.

46. EDPS zdôrazňuje, že používanie nástrojov na určovanie polohy musí byť zákonné, t. j. musí sa vykonávať na základe riadneho právneho základu, na explicitné a zákonné účely a musí byť primerané účelom, ktoré sa majú dosiahnuť. Zákonnosť vykonávaného spracúvania údajov bude vo veľkej miere závisieť na spôsobe, akým sa budú nástroje na určovanie polohy používať, a účeloch, na ktoré sa budú používať. Ako zdôraznila pracovná skupina zriadená podľa článku 29 vo svojom stanovisku k systému eCall: „z hľadiska ochrany údajov by nebolo prijateľné, aby boli príslušné zariadenia trvalo pripojené na sieť a vozidlá tým pádom trvalo sledovateľné v záujme novej aktivácie zariadení systému eCall“<sup>(25)</sup>. Je preto dôležité, aby sa viac objasnili osobitné okolnosti, za ktorých sa bude vozidlo sledovať, a súvisiaci vplyv na užívateľa. V každom prípade by malo byť používanie zaria-

dení na určovanie polohy odôvodnené zákonnou potrebou (napr. sledovanie prepravy tovaru) a prísne obmedzené na to, čo je na takýto účel nevyhnutné. Preto je dôležité presne definovať, ktoré údaje o polohe sa zhromažďujú, kde sú uložené a na ako dlho sú uchovávané, s kým a na aké účely sa vymieňajú, a prijať všetky kroky potrebné na to, aby sa predchádzalo úmyselnému zneužívaniu údajov alebo ich zneužívaniu z nedbanlivosti.

47. Navyše je spracúvanie údajov o polohe týkajúcich sa užívateľov verejných komunikačných sietí alebo verejne dostupných elektronických komunikačných služieb prísne regulované v článku 9 smernice 2002/58/ES. Vyžaduje sa v ňom najmä, aby sa spracúvanie údajov o polohe vykonávalo na anonymnom základe, alebo na základe informovaného súhlasu užívateľa. To znamená, že užívateľom sa musia pred udelením súhlasu s používaním zariadenia na určovanie polohy poskytnúť primerané informácie vrátane druhu spracúvaných údajov o polohe, účeloch a dĺžke trvania spracúvania a o tom, či sa údaje budú prenášať tretej strane na účely poskytovania služieb s pridanou hodnotou. Pre každé pripojenie k sieti alebo pre každý prenos správy musí byť k dispozícii jednoduchý a bezplatný prostriedok, ktorý užívateľom umožní dočasne odmietnuť spracúvanie údajov o polohe. Spracúvanie údajov o polohe by malo byť prísne obmedzené na osoby, ktoré konajú v rámci právomoci poskytovateľa verejnej komunikačnej siete alebo verejne dostupnej komunikačnej služby alebo tretej osoby, ktorá poskytuje služby s pridanou hodnotou.

48. Keď sa údaje o polohe zhromažďujú z vozidiel, ktoré sa používajú v rámci profesionálnej činnosti, musia sa prijať dodatočné záruky s cieľom zabrániť používaniu technológie na určovanie polohy na neoprávnené monitorovanie zamestnancov. Spracúvanie by malo byť v každom prípade obmedzené na údaje o polohe zhromaždené počas pracovnej doby – zamestnanci teda musia mať možnosť vypnúť funkciu určovania polohy po skončení pracovnej doby a/alebo keď používajú vozidlo na súkromné účely.

49. Existuje riziko, že tretie strany (napr. poisťovne, zamestnávateľia a orgány presadzovania práva) môžu vyžadovať prístup k údajom zhromaždeným prostredníctvom navigačných a sledovacích systémov na zákonné a špecifikované účely (napríklad sledovanie pohybu tovaru, elektronické platby mýta atď.), aby ich mohli použiť na sekundárne účely, ako je kontrola doby vedenia vozidla a doby odpočinku alebo overovanie dodržiavania dopravných predpisov a ukládanie sankcií. Prístup k údajom na sekundárne účely v zásade nie je povolený, ak slúži na účely, ktoré sú nezlučiteľné s účelmi, na ktoré boli dané údaje zhromaždené. Takýto prístup možno povoliť iba ako výnimku z tejto zásady, ak spĺňa prísne požiadavky uvedené v článku 13 smernice 95/46/ES. V dôsledku toho sa tretím stranám môže poskytnúť prístup k údajom o polohe len v súlade s právnymi predpismi a transparentným spôsobom, a to na základe právneho opatrenia, v ktorom sa ustanovia vhodné postupy

<sup>(23)</sup> Pozri stanovisko európskeho dozorného úradníka pre ochranu údajov k oznámeniu Komisie Európskemu parlamentu, Rade, Európskemu hospodárskemu a sociálnemu výboru a Výboru regiónov o rádiových frekvenciách (RFID) v Európe: kroky k politickému rámcu, KOM(2007) 96, Ú. v. EÚ 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\\_EN.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-12-20_RFID_EN.pdf)

<sup>(24)</sup> Pracovná skupina zriadená podľa článku 29, stanovisko k používaniu miestnych údajov s cieľom poskytovať služby s pridanou hodnotou, WP 115, november 2005. [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2005/wp115\\_sk.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_sk.pdf)

<sup>(25)</sup> Pozri dokument WP 125 o systéme eCall, s. 5, uvedený v pozn. pod čiarou č. 10.



a spôsoby upravujúce prístup k takýmto údajom na osobitné účely a ktorý poskytuje jednotlivcom dostatočné záruky vzhľadom na ďalšie účely, na ktoré by ich údaje mohli byť použité.

### III.2.b) Úlohy a povinnosti aktérov v oblasti IDS

50. Zatiaľ nie je jasné, kto bude kontrolárom údajov pre jednotlivé časti spracúvania. V mnohých prípadoch budú kontrolórmi údajov pravdepodobne poskytovatelia služieb IDS, či už samostatne, pokiaľ ide o spracúvanie osobných údajov na účely poskytovania svojich vlastných služieb IDS, alebo spoločne v prípade, že sa spracúvanie vykonáva spoločne s ďalšími kontrolórmi údajov. Pre každú časť spracúvania (napr. v prípade telekomunikačných operátorov poskytujúcich komunikačné služby, ako aj služby IDS) by sa mali jasne vymedziť úlohy a povinnosti subjektov zapojených do IDS v rôznych funkciách, ktoré vyplývajú z ich postavenia kontrolórov a spracovateľov údajov.
51. Osoby, ktoré budú plniť úlohu kontrolórov údajov budú zodpovedné<sup>(26)</sup> za súlad systémov a služieb so všetkými povinnosťami v oblasti ochrany údajov, a najmä za zavádzanie systémov, do ktorých sa ochrana súkromia zabuduje už vo fáze ich návrhu, ktoré dodržiavajú zásadu kvality údajov a zásadu obmedzenia účelu a ktoré zaručujú primeranú úroveň zabezpečenia údajov, ako je popísané v časti III.1).
52. Kontrolóri údajov budú musieť zabezpečiť, aby sa na všetkých úrovniach reťazca subjektov zapojených do zavádzania IDS prijali primerané záruky. To si bude predovšetkým vyžadovať, aby vstúpili do primeraných zmluvných režimov so všetkými zainteresovanými stranami podieľajúcimi sa na výmene a spracúvaní údajov, ktoré by mali zabezpečiť primerané záruky ochrany údajov (najmä pokiaľ ide o články 16 a 17 smernice 95/46/ES a články 4 a 5 smernice 2002/58/ES). Je dôležité si uvedomiť, že z hľadiska ochrany údajov kontrolóri údajov síce musia zaistiť zabezpečenie ochrany údajov vo všetkých fázach spracúvania, sú však za spracúvanie aj naďalej zodpovední a túto zodpovednosť nemôžu zmluvne preniesť na iný subjekt.

## IV. ZÁVERY

53. EDPS víta navrhovaný plán zavádzania IDS predložený Komisiou, ktorý sa zameriava na harmonizáciu dátových procesov v celej Európe s cieľom uľahčiť poskytovanie služieb IDS a v ktorom sa ochrana údajov vyzdvihuje ako základná podmienka správneho zavádzania IDS v Európe.
54. EDPS konštatuje, že navrhovaná smernica ustanovuje všeobecný rámec, ktorý vyvoláva množstvo otázok týkajúcich sa ochrany súkromia a údajov, ktoré je potrebné ďalej riešiť na úrovni EÚ a na vnútroštátnej úrovni:

- Existuje riziko, že nejasnosti v navrhovanom právnom rámci spôsobia rôznorodosť pri zavádzaní IDS v Európe, ktorá bude viesť k odlišným úrovniam ochrany údajov v Európe. EDPS zdôrazňuje potrebu ďalšej harmonizácie v týchto otázkach na úrovni EÚ s cieľom objasniť nevyriešené otázky (napr. vymedzenie úloh a povinností aktérov IDS, určenie konkrétnych aplikácií a systémov IDS, ktoré musia byť zabudované vo vozidlách, vypracovanie harmonizovaných zmlúv o poskytovaní služieb IDS, určenie osobitných účelov a spôsobov používania IDS, atď.). Je mimoriadne dôležité identifikovať, kto bude kontrolárom údajov, pokiaľ ide o vykonávané spracúvanie údajov, pretože tento ponese zodpovednosť za zabezpečenie toho, aby sa riešenia otázok ochrany súkromia a údajov zaviedli na všetkých úrovniach reťazca spracúvania.
- Rozhodnutia o určitých spôsoboch spracúvania, ktoré by mohli vážne ovplyvniť práva jednotlivcov na ochranu súkromia a údajov by mal prijímať Európsky parlament a Rada, a nie výbory prostredníctvom komitológie.
- Je zásadné, aby sa na ochranu súkromia a údajov prihliadalo už od skorých fáz spracúvania a vo všetkých fázach spracúvania; pri navrhovaní aplikácií a systémov by sa malo podporovať zavádzanie zásady „ochrana súkromia už v štádiu návrhu“, ktorá by sa mala zapracovať do noriem, najlepších postupov, technických špecifikácií a systémov.
- Akékoľvek prepájanie aplikácií a systémov by malo sprevádzať náležité zohľadnenie zásad ochrany údajov a praktických bezpečnostných záruk.
- Vzhľadom na nejasnosti, ktoré zostávajú v tejto fáze, pokiaľ ide o spôsoby zavádzania IDS, EDPS osobitne víta iniciatívu predloženú Komisiou v jej oznámení, aby sa do roku 2011 uskutočnilo posúdenie vplyvu na ochranu súkromia. Navyše dôrazne odporúča, aby sa posúdenia vplyvu na ochranu súkromia a údajov vykonávali pre konkrétne odvetvia a/alebo účely použitia s cieľom vymedziť vhodné bezpečnostné opatrenia a aby sa vypracovali najlepšie dostupné postupy na ochranu súkromia a údajov a zaistenie bezpečnosti v rámci IDS.
- EDPS ďalej zdôrazňuje, že členské štáty ponесú zodpovednosť za správne vykonávanie smernice tak, aby subjekty zavádzali systémy a služby, ktoré poskytujú primeranú úroveň ochrany údajov v celej Európe.

<sup>(26)</sup> Pozri poznámku pod čiarou č. 13.

- Kontrolóri údajov poskytujúci služby IDS by mali zavádzať primerané záruky tak, aby používanie technológií určovania polohy, ako sú napríklad satelitné systémy na určovanie polohy a značky RFID, nenarúšalo súkromie jednotlivcov, ktorí používajú vozidlá na čisto súkromné alebo profesionálne účely. To si bude vyžadovať najmä obmedzenie spracúvania na údaje nevyhnutné na daný účel, zaistenie toho, aby sa do systémov zabudovali primerané bezpečnostné opatrenia tak, aby sa údaje o polohe nespřístupňovali neoprávneným príjemcom, a aby sa užívateľom poskytl účinné prostriedky na deaktiváciu zariadenia/funkcie na určovanie polohy.
55. EDPS odporúča, aby sa článok 6 návrhu zmenil a doplnil podľa smernice 95/46/ES takto:
- Pri spracúvaní údajov prostredníctvom IDS by sa mala podporovať minimalizácia údajov. Preto je vhodné zmeniť a doplniť článok 6 ods. 1b) návrhu takto: „Osobné údaje sa môžu spracúvať, iba pokiaľ je toto spracúvanie nevyhnutné na konkrétny účel, na ktorý sa IDS používa, a len v súlade s príslušným právnym základom“.
- Je dôležité, aby sa osobné údaje spracúvané prostredníctvom interoperabilných systémov nepoužívali na ďalšie účely, ktoré sú nezlučiteľné s tými, na ktoré boli zhromaždené. Preto EDPS odporúča upraviť
- článok 6 ods. 2 takto: „a aby sa nesmeli použiť na iné účely, ako tie, na ktoré boli zhromaždené, spôsobom nezlučiteľným s takýmito účelmi“.
- EDPS odporúča, aby sa v súvislosti s navrhovaním aplikácií a systémov IDS v článku 6 návrhu doplnil výslovný odkaz na pojem „ochrana súkromia už v štádiu návrhu“. Navyše odporúča, aby pracovná skupina zriadená podľa článku 29 a EDPS boli informovaní o ďalších opatreniach, ktoré sa v rámci tejto otázky prijímú prostredníctvom komitologického postupu, a aby sa s nimi o týchto opatreniach konzultovalo.
56. EDPS ďalej odporúča, aby sa v odôvodneniach návrhu uviedol odkaz na túto konzultáciu.
57. Vzhľadom na vyššie uvedené skutočnosti EDPS odporúča, aby mali orgány ochrany údajov možnosť úzko sa zapájať do iniciatív týkajúcich sa zavádzania IDS, najmä prostredníctvom pracovnej skupiny zriadenej podľa článku 29 a EDPS, pričom by sa s nimi malo konzultovať v dostatočne skorom štádiu pred vypracovaním príslušných opatrení.

V Bruseli 22. júla 2009

Peter HUSTINX

európsky dozorný úradník pre ochranu údajov