EIROPAS DATU AIZSARDZĪBAS UZRAUDZĪTĀJS

Eiropas Datu aizsardzības uzraudzītāja atzinums sakarā ar Komisijas paziņojumu par rīcības plānu Eiropā ieviest inteliģentas transporta sistēmas un tam pievienoto ierosināto Eiropas Parlamenta un Padomes direktīvu, ar ko nosaka pamatu inteliģento transporta sistēmu ieviešanai autotransporta jomā un saskarnēm ar citiem transporta veidiem

(2010/C 47/02)

EIROPAS DATU AIZSARDZĪBAS UZRAUDZĪTĀJS,

ņemot vērā Eiropas Kopienas dibināšanas līgumu un it īpaši tā 286. pantu,

ņemot vērā Eiropas Savienības Pamattiesību hartu un it īpaši tās 8. pantu,

ņemot vērā Eiropas Parlamenta un Padomes Direktīvu 95/46/EK (1995. gada 24. oktobris) par personu aizsardzību attiecībā uz personas datu apstrādi un šo datu brīvu apriti,

ņemot vērā Eiropas Parlamenta un Padomes Direktīvu 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē,

ņemot vērā Eiropas Parlamenta un Padomes Regulu (EK) Nr. 45/2001 (2000. gada 18. decembris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās un par šādu datu brīvu apriti un it īpaši tās 41. pantu,

ņemot vērā no Eiropas Komisijas 2009. gada 11. februārī saņemto lūgumu saskaņā ar Regulas (EK) Nr. 45/2001 28. panta 2. punktu nākt klajā ar atzinumu,

IR PIEŅĒMIS ŠO ATZINUMU.

I. IEVADS

1. Komisija 2008. gada 16. decembrī pieņēma paziņojumu, kurā bija ietverts rīcības plāns Eiropā ieviest inteliģentas transporta sistēmas ("paziņojumu") [1]. Paziņojumam ir pievienots priekšlikums Eiropas Parlamenta un Padomes Direktīvai, ar ko nosaka pamatu inteliģento transporta sistēmu ieviešanai autotransporta jomā un saskarnēm ar citiem transporta veidiem ("priekšlikums") [2]. Komisija saskaņā ar Regulas (EK) Nr. 45/2001 28. panta 2. punktu paziņojumu un pievienoto priekšlikumu nosūtīja EDAU, lai saņemtu atzinumu [3].

2. EDAU pauž gandarījumu par to, ka viņam lūdz padomu, un iesaka uz to atsaukties ierosinātā tiesību akta apsvērumos, kā ir darīts vairākos citos tiesību aktos, par ko saskaņā ar Regulu (EK) Nr. 45/2001 ir lūgts EDAU atzinums.

I.1. Komisijas paziņojums par rīcības plānu Eiropā ieviest inteliģentas transporta sistēmas

3. "Inteliģentas transporta sistēmas" ("*Intelligent Transport Systems – ITS*") ir progresīvas lietojumprogrammas, kas izmanto informācijas un saziņas tehnoloģijas (*Information and Communication Technologies – ICT*), kas ir iestrādātas dažādos transporta veidos, lai tie varētu savstarpēji mijdarboties. Autotransporta jomā ITS dažādiem lietotājiem, piemēram, ceļotājiem, autotransporta infrastruktūru lietotājiem un apsaimniekotājiem, autoparku un glābšanas dienestu vadītājiem dos novatoriskus dažādu transporta veidu un satiksmes vadības pakalpojumus.

4. Ņemot vērā aizvien plašāku ITS ieviešanu dažādos Eiropas Savienības transporta veidos [4], Komisija ir pieņēmusi rīcības plānu paātrināt ITS lietojumprogrammu un

[1] COM(2008) 886 galīgā redakcija. Padome 2009. gada 30. un 31. martā notikušajā 2935. Transporta, telekomunikāciju un enerģētikas padomes sanāksmē ir pieņēmusi secinājumus par paziņojumu.
[2] COM(2008) 887 galīgā redakcija.
[3] Eiropas Parlamenta un Padomes Regula (EK) Nr. 45/2001 (2000. gada 18. decembris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās un par šādu datu brīvu apriti, OV L 8, 12.1.2001., 1. lpp.
[4] Ir daudzas ES mēroga ierosmes integrēt ITS dažādos transporta veidos, arī aviotransportā (*SESAR*), iekšzemes ūdenstransportā (RIS), dzelzceļu transportā (*ERTMS, TAF-TSI*), kuģu transportā (*VTMIS, AIS, LRIT*), un autotransportā (*eToll, eCall*), skat. COM(2008) 886 galīgās redakcijas 3. lpp..

pakalpojumu ieviešanu un lietojumu autotransporta jomā. Plānā ir paredzēts nodrošināt to mijdarbību ar citiem transporta veidiem, atvieglinot multimodālu pārvadājumu pakalpojumu sniegšanu. Viendabīga ITS ieviešana Eiropā palīdzēs dažādiem Kopienas mērķiem, tostarp transporta efektivitātei, nekaitēs apkārtējai videi, veicinās transporta drošumu un drošību, un palīdzēs ES iekšējam tirgum un konkurētspējai. Ņemot vērā to, cik dažādi ir ITS izvēršanas mērķi, paziņojumā ir ieskicētas sešas prioritāras darbības jomas laikā no 2009. līdz 2014. gadam. Lai plānu īstenotu, Komisija ierosina tiesisko regulējumu ES mērogā noteikt ar direktīvu, kurā būtu definēti vairāki pasākumi izvēlētajās prioritārās jomās.

I.2. **Priekšlikums direktīvai, ar ko nosaka pamatu inteliģento transporta sistēmu ieviešanai autotransporta jomāun saskarnēm ar citiem transporta veidiem**

5. Ierosinātajā tiesību aktā ir ieskicēta ITS lietojumprogrammu pārvalstiskas ieviešanas sistēma, ar ko ir iecerēts atvieglināt saskaņotu pārrobežu pakalpojumu sniegšanu, it īpaši satiksmes un ceļojumu informācijas un satiksmes vadības ziņā. Tajā paredzēts dalībvalstīm veikt vairākus tehniskus pasākumus, lai lietotājiem, valstu iestādēm, attiecīgām ieinteresētām pusēm un ITS pakalpojumu sniedzējiem atvieglinātu savstarpēju datu apmaiņu, un transportlīdzekļos un ceļu infrastruktūrā integrētu ar drošību un drošumu saistītas ITS sistēmas. ITS lietojumprogrammu un sistēmu tehniskās specifikācijas četrās rīcības plānā uzskaitītajās prioritārajās jomās ([5]) definēs, izmantojot komitoloģijas procedūru ([6]), kuru pamatelementi ir precizēti II pielikumā. Konkrēti mērķi, kam minētajās jomās izmantos ITS, tomēr nav skaidri. Turklāt ITS ieviešana var aptvert daudz vairāk jomu par četrām sākotnēji izvēlētajām, kurām izstrādāja tehniskās specifikācijas. Kaut gan priekšlikumā galvenokārt ir runa par iecerēto ITS lietojumprogrammu un pakalpojumu ieviešanu, iespēju robežās tas aptvers minētajā jomā jau esošas vai topošas tehnoloģijas (piemēram, *eCall* (*emergency call* – ārkārtas izsaukumu tehnoloģiju), *eToll* (*electronic toll service* – elektroniskas ceļu nodevu iekasēšanas tehnoloģiju), u. c.).

6. Priekšlikums ir nosūtīts Eiropas Parlamentam, kas 2009. gada 23. aprīlī ir pieņēmis nostāju pirmā lasījumā ([7]). Atbildot uz Padomes 2009. gada 29. janvāra lūgumu sniegt konsultāciju, Eiropas Ekonomikas un sociālo lietu komiteja 2009. gada 13. maijā ir pieņēmusi atzinumu par priekšlikumu ([8]).

I.3. **Atzinuma pamatdoma**

7. EDAU ir gandarīts par konsultāciju saistībā ar Komisijas ierosināto ITS ieviešanas plānu. Nav pirmā reize, kad EDAU sastopas ar sarežģījumiem ITS rīcības plānā. EDAU ir nācis klajā ar atzinumu par Komisijas ierosinājumu satiksmes drošuma jomā ([9]) atvieglināt noteikumu pārrobežu izpildi un ir palīdzējis 29. panta darba grupai strādāt ar darba dokumentu par *eCall* (*emergency call* – ārkārtas izsaukumiem) ([10]).

8. Inteliģentu transporta sistēmu pamatā ir daudzu dažādu, gan no valstu, gan privātiem avotiem iegūtu datu vākšana, apstrāde un apmaiņa – minētajās sistēmās datus izmanto intensīvi. Izvēršot ITS, lielā mērā izmantos ģeolokalizācijas (*geolocalisation*) tehnoloģijas, piemēram, pozicionēšanu, izmantojot satelītus, un bezkontaktu tehnoloģijas, piemēram, *RFID*, kas atvieglinās dažādu brīvi pieejamu un/vai maksas pakalpojumu sniegšanu atkarībā no atrašanās vietas (piem., sniegs reāllaika satiksmes informāciju, eKravas transporta informāciju (*eFreight*), *eCall*, *eToll*, rezervēs stāvvietu, utt.). Daļa informācijas, ko apstrādās ar ITS, būs apkopota – piemēram, par satiksmi, nelaimes gadījumiem un dažādām iespējām – un neattieksies uz kādu konkrētu personu, bet cita informācija būs saistīta ar konkrētiem, identificētiem vai identificējamiem cilvēkiem, un tālab ir atzīstama par personas datiem Direktīvas 95/46/EK 2.a panta nozīmē.

9. EDAU uzskata, ka ir būtiski, lai iecerētās ITS ieviešanas darbības saskanētu ar esošo tiesisko regulējumu, kas ir citēts priekšlikumā, it īpaši Direktīvā 95/46/EK par datu aizsardzību ([11]) un Direktīvā 2002/58/EK par e-privātumu ([12]).

([5]) Priekšlikuma 4. pantā ir paredzēts definēt tehniskus pasākumus šādās jomās – i) optimāli izmantot datus par ceļiem, satiksmi un maršrutiem, ii) konsekventiem ITS pakalpojumiem, Eiropas transporta koridoros un konurbācijās regulējot satiksmi un kravu pārvadājumus, iii) satiksmes drošumu un drošību, un iv) transportlīdzekļu integrāciju transporta infrastruktūrās.

([6]) Priekšlikumā saskaņā ar Lēmuma 1999/468/EK 5.a panta 1. līdz 4. punktu un 7. pantu ir paredzēta regulatīva kontroles procedūra.

([7]) Eiropas Parlamenta 2009. gada 23. aprīļa normatīvā rezolūcija par ierosināto Eiropas Parlamenta un Padomes direktīvu, ar ko nosaka pamatu inteliģento transporta sistēmu ieviešanai autotransporta jomā un saskarnēm ar citiem transporta veidiem, T6-0283/2009.

([8]) Eiropas Ekonomikas un sociālo lietu komitejas atzinums par ierosināto Eiropas Parlamenta un Padomes direktīvu, ar ko nosaka pamatu inteliģento transporta sistēmu ieviešanai autotransporta jomā un saskarnēm ar citiem transporta veidiem, TEN/382, (2009. gada 13. maijs).

([9]) Eiropas Datu aizsardzības uzraudzītāja atzinums par ierosināto Eiropas Parlamenta un Padomes Direktīvu, ar ko veicina ceļu satiksmes drošības noteikumu pārrobežu izpildi, 2008/C 310/02, OV C 310, 5.12.2008., 9. lpp.

([10]) 29. panta darba grupas darba dokuments par *eCall* ierosmes sekām datu aizsardzības un privātuma jomā, WP 125 (2006. gada 26. septembris). http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp125_en.pdf

([11]) Eiropas Parlamenta un Padomes Direktīva 95/46/EK (1995. gada 24. oktobris) par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti OV L 281, 23.11.1995., 31. lpp.

([12]) Eiropas Parlamenta un Padomes Direktīva 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju) OV L 201, 31.7.2002., 37. lpp.

10. Komisija ir apzinājusi neatrisinātas privātuma un datu aizsardzības problēmas kā vienu no galveniem šķēršļiem ITS veicināšanā. Atzinumā šie jautājumi būs aplūkoti šādi:

— II nodaļā Komisijas ierosinātais tiesiskais regulējums, kā ieviest ITS, būs analizēts no datu aizsardzības perspektīvas,

— III nodaļā būs izgaismotas datu aizsardzības problēmas, kam turpmāk būtu jāpievēršas, lai pareizi ieviestu ITS

— pirmajā punktā būs uzsvērta vajadzība pēc "integrētas privātās dzīves aizsardzības ("*privacy by design*")", izstrādājot ITS, un turpināts ieskicēt svarīgas problēmas, kam jābūt atrisinātām, izstrādājot ITS lietojumprogrammas un datu apstrādes sistēmas,

— otrajā punktā uzmanība būs pievērsta dažiem privātuma apsvērumiem, ar ko būs jādarbojas arī turpmāk, lai varētu sniegt ITS pakalpojumus.

II. **ITS IZVĒRŠANAI IEROSINĀTĀ TIESISKĀ REGULĒJUMA ANALĪZE**

11. Komisijas direktīvas priekšlikumā ir divi noteikumi (9. apsvērums un 6. pants), kuros ir runa par privātumu, drošību un atkārtotu informācijas lietojumu. Komisijas priekšlikuma 6. panta 1. punktā ir prasīts, lai ITS darbības notiktu, ievērojot datu aizsardzības noteikumus, kas, *inter alia*, ir ietverti Direktīvā 95/46/EK un 2002/58/EK. Komisijas priekšlikuma 6. panta 2. punktā ir paredzēti konkrēti datu aizsardzības pasākumi, galvenokārt no drošības viedokļa – priekšlikuma 6. panta 2. punktā ir teikts, ka "dalībvalstis nodrošina ITS datu un ierakstu aizsardzību pret ļaunprātīgu izmantojumu, arī pret nelikumīgu piekļuvi, sagrozīšanu vai nozaudēšanu". Visbeidzot, Komisijas priekšlikuma 6. panta 3. punktā ir paredzēts piemērot Direktīvu 2003/98/EK.

12. Eiropas Parlaments pirmā lasījumā ir ierosinājis 6. panta grozījumus. Konkrēti, 6. panta 1. punktā ir iekļauti trīs jauni punkti, kas attiecas uz vajadzības gadījumā lietotiem anonīmiem datiem, uz diskrētu datu apstrādi, ko veic tikai tad, kad datu subjekts ir saņēmis informāciju par datu apstrādi un piekritis, ka to veic, un uz garantijām, ka personas datus apstrādā tikai tiktāl, "ciktāl datu apstrāde ir vajadzīga ITS lietojumprogrammām un/vai pakalpojumiem". Turklāt 6. panta 2. punktā ir izdarīti grozījumi, piebilstot, ka ITS datus un ierakstus "nedrīkst izmantot citiem kā vien direktīvā minētajiem mērķiem".

13. EDAU ir gandarīts, ka datu aizsardzība ir ņemta vērā, izstrādājot tiesību akta priekšlikumu – un ka tā ir izvirzīta par vispārēju priekšnosacījumu, lai Eiropā pareizi ieviestu ITS. EDAU apzinās, ka ES mērogā ir vajadzīga viendabīga, saskaņota datu apstrāde, lai visā Eiropā nodrošinātu ITS lietojumprogrammu un pakalpojumu spēju darboties.

14. Tomēr EDAU norāda, ka ierosinātais tiesiskais regulējums ir pārāk plašs un vispārīgs, lai pienācīgi risinātu privātuma un datu aizsardzības problēmas, ko rada ITS ieviešana dalībvalstīs. Nav skaidrs, kad ITS pakalpojumi liks vākt un apstrādāt personas datus, kādām konkrētām vajadzībām tos apstrādās, kā arī – kāds juridisks pamats attaisnos datu apstrādi. Turklāt, ieviešot ITS, atrašanās vietas noteikšanas tehnoloģiju lietojums palielina iespējamību, ka izstrādātie pakalpojumi iejauksies privātā dzīvē, ja tie liks vākt personas datus un apmainīties ar tiem. Vēl vairāk, priekšlikumā nav skaidri izklāstīti dažādo ITS ieviešanas ķēdē iesaistīto operatoru uzdevumi un pienākumi, un ir grūti saprast, kādi operatori būs datu kontrolieri, un tātad atbildēs ([13]) par datu aizsardzības pienākumu ievērošanu. Ja visus šos jautājumus skaidri nenoteiks tiesību aktā, ITS operatori sastapsies ar ievērojamiem sarežģījumiem, jo galu galā viņi atbildēs par ierosinātajā direktīvā izklāstīto pasākumu piemērošanu.

15. Tālab pastāv iespējamība, ka nepietiekami skaidrs ierosinātais tiesiskais regulējums liks Eiropā dažādi īstenot ITS, un tas nevis mazinās dalībvalstu atšķirības, bet, gluži otrādi, tas izraisīs nopietnas neskaidrības, fragmentāciju un nekonsekvences, jo Eiropā pastāvēs dažādu līmeņu datu aizsardzība. Tas var izraisīt arī būtiskāko datu aizsardzības drošības elementu neievērošanu. EDAU uzsver vajadzību turpmāk ES mērogā saskaņot minētos jautājumus. EDAU še ierosinās grozīt ierosināto tiesisko regulējumu no datu

([13]) Saskaņā ar 11. zemsvītras piezīmē minēto Direktīvas 95/46/EK 2.d pantu, 6. panta 2. punktu un 23. pantu.

aizsardzības viedokļa. Viņš stingri iesaka Eiropas Parlamentam un Padomei priekšlikumā iekļaut ierosinātos grozījumus, kā arī, kur tas iespējams, papildu noteikumus, lai padarītu skaidrākas neatrisinātās problēmas (piemēram, definētu, kas ir ITS darbību veicēji, un kādi ir viņu pienākumi, kā ieviest saskaņotus ITS pakalpojumu sniegšanas līgumus, utt.). Viņš arī uzsver, ka dalībvalstis būs atbildīgas arī par direktīvas pareizu īstenošanu, lai operatori varētu izstrādāt sistēmas un pakalpojumus, kas visā Eiropā datiem nodrošina attiecīga līmeņa aizsardzību.

II.1. **Datu apstrādei ir jābalstās uz attiecīgu juridisku pamatu**

16. Pēc tam, kad ITS iekārtas būs integrētas transportlīdzekļos, nav skaidrs, kad sāksies personas datu apstrāde un ar kādu juridisku pamatojumu tā notiks. Operatori datu apstrādei var izmantot dažādus juridiskus pamatojumus, *inter alia*, lietotāju skaidru piekrišanu, līgumu vai juridisku pienākumu, ko datu kontrolieri ievēros. Ir jāskaņo datu apstrādes juridiskais pamats, uz kā ar ITS starpniecību notiks datu apstrāde, lai nodrošinātu sistēmu darbību visā Eiropā, un lai lietotāji neciestu no datu apstrādes atšķirībām katrā ES valstī.

17. Vairākos gadījumos ITS sistēmas transportlīdzekļos jau automātiski būs integrētas. Tas īpaši attiecas uz ITS sistēmām, kas ir saistītas ar drošību un drošumu, un kam saskaņā ar priekšlikumu ir jābūt iestrādātām transportlīdzekļos. Priekšlikumā tomēr nav definēts, kas ir "ar drošību un drošumu saistītas ITS sistēmas", un tajā vajadzētu labāk paskaidrot, kas ir konkrētās ITS lietojumprogrammas un sistēmas, kam jābūt iestrādātām transportlīdzekļos. Turklāt būtu skaidri jānosaka, vai lietotāji brīvprātīgi vai obligāti iedarbinās un lietos ierīces. Iespēja izvēlēties obligātu datu apstrādi būtu jāparedz tikai konkrētiem mērķiem, neaizmirstot nenoraidāmus likumīgus iemeslus (piem., preču izsekošanu kravas transporta satiksmes regulācijā) un attiecīgus ar konkrētiem cilvēkiem saistītu datu apstrādes drošības elementus. Ja ITS lietojumu izvēlas brīvprātīgi, būtu jāīsteno attiecīgi drošības elementi, lai novērstu stāvokli, ka vien tāpēc, ka sistēmas transportlīdzekļos būtu uzstādītas, uzskatītu, ka lietotāji ir automātiski piekrituši tās lietot.

18. EDAU dod priekšroku tam, ka ITS pakalpojumus sniedz pēc brīvprātīgas izvēles. Tas nozīmē, ka lietotājiem ir jāvar brīvi piekrist sistēmu lietojumam un konkrētiem mērķiem, kam to lietos. Ja sniegtie pakalpojumi izmanto atrašanās vietas datus, lietotājiem ir jāsaņem attiecīga informācija (konkrēti saskaņā ar Direktīvas 2002/58/EK 9. pantu), un viņiem ir jāvar piekrišanu atsaukt. Praksē tas prasa, lai būtu ieviesta iespēja viegli izslēgt ierīci un/vai funkciju, neradot lietotājiem tehniskus vai finanšu sarežģījumus ([14]), ja kāds lietotājs vairs negribētu lietot sistēmu un/vai konkrētu funkciju. Būtu jāīsteno papildu drošības elementi, lai lietotājus nediskriminētu, ja viņi atteiktos lietot kādus pakalpojumus.

([14]) Skat. WP 125 par *eCall*, 4. lpp., kas minēts 10. zemsvītras piezīmē.

19. Gadījumos, ja dažas datu apstrādes darbības būtu obligātas, bet citas notiktu ar lietotāju piekrišanu, jānodrošina pārskatāmība par dažādām veiktām datu apstrādes operācijām, attiecīgi informējot lietotājus par to, vai katra konkrētā datu apstrāde ir obligāta un/vai brīvprātīga, un par konkrētās datu apstrādes mērogiem. Turklāt būs svarīgi īstenot attiecīgus drošības aizsargelementus, lai datus nevāktu un neapstrādātu, pārsniedzot likumīgi nospraustas robežas un/vai tādas, kam lietotāji ir brīvprātīgi piekrituši.

20. Neaizmirstot ITS pakalpojumu pārvalstiskumu, EDAU iesaka arī izstrādāt Eiropas mēroga standartlīgumus, lai nodrošinātu, ka ar ITS starpniecību sniegtie pakalpojumi visā Eiropā dotu vienādu datu aizsardzības drošību, un it īpaši – lai pietiekami skaidra būtu lietotājiem sniegtā informācija par konkrētām izmantotām funkcijām, konkrētu tehnoloģiju lietojuma sekām datu aizsardzībā, un to, kā viņi var īstenot tiesības. Pievienojot jaunas funkcijas, pakalpojumu sniedzējiem būtu jāveic turpmāki pasākumi, lai lietotājiem dotu skaidru un konkrētu informāciju par attiecīgām papildu funkcijām un attiecīgi saņemtu viņu piekrišanu lietot jaunās funkcijas.

II.2. **Datu apstrādes mērķi un mehānismi ir jādefinē precīzāk**

21. EDAU norāda, ka priekšlikumā nav precīzi definēti konkrēti pakalpojumi un mērķi, kam varētu lietot ITS lietojumprogrammas, un tādējādi paveras iespēja spekulācijām. Tas ļauj praksē būt patiesi elastīgiem, bet nozīmē, ka neatrisinātās privātuma un datu aizsardzības problēmas – ko Komisija ir apzinājusi kā vienu no galveniem ITS veicināšanas šķēršļiem (skat. 10. punktu) – var arī palikt neatrisinātas un traucēt līdzsvaroti īstenot ierosinātos pasākumus.

22. EDAU uzsver, ka ir īpaši svarīgi, lai datu apstrādes darbības, ko veic, sniedzot konkrētus ITS pakalpojumus, neveiktu tikai saskaņā ar attiecīgu juridisku pamatu, bet arī konkrētu, skaidri saprotamu un likumīgu mērķu dēļ, un lai paredzētā datu apstrāde būtu samērīga un vajadzīga minētajiem mērķiem (Direktīvas 95/46/EK 6. pants). Tālab būtu jāapsver iespējama vajadzība arī turpmāk ES mērogos pieņemt tiesību aktus par konkrētiem ITS lietojumiem, lai veicamai datu apstrādei nodrošinātu saskaņotu un pareizu juridisku pamatu un izvairītos no atšķirībām, dažādās dalībvalstīs ieviešot ITS pakalpojumus.

23. Ierosinātajā sistēmā vēl nav pieņemts lēmums par ITS vajadzībām veiktas datu apstrādes un datu apmaiņas mehānismiem. Daudzus tehniskus parametrus, kuru izvēlei būs dažādas sekas no privātuma un datu aizsardzības viedokļa, izlems vēlākā stadijā, izmantojot komitoloģiju. Ņemot vērā

konkrēto privātumam un datu aizsardzībai kā Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencijas 8. pantā un Eiropas Savienības Pamattiesību hartas 7. un 8. pantā dotu pamattiesību aizsardzību, var apšaubīt, vai un ciktāl datu apstrādes darbību definīcija būtu jānosaka ar komitoloģijas procedūru.

24. Demokrātiskās sabiedrībās lēmumus par būtiskiem principiem un mehānismiem, kas ietekmē pamattiesības, būtu jāpieņem saskaņā ar pilnvērtīgām likumdošanas procedūrām, pie kā pieder attiecīgas pārbaudes un līdzsvara nodrošinājums. Šajā gadījumā tas nozīmē, ka lēmumi, kas nopietni ietekmēs konkrētu cilvēku privātumu un datu aizsardzību, piemēram, obligātu datu apstrādes darbību mērķus un mehānismus, kā arī nosakot ITS ieviešanas mehānismus jaunās jomās, būtu jāpieņem Eiropas Parlamentā un Padomē, un nevis ar komitoloģijas procedūru.

25. Tādā perspektīvā EDAU stingri iesaka saskaņā ar priekšlikuma 8. pantu izveidotās komitejas darbā, kā arī nākotnes darbībās saistībā ar ITS ieviešanu vajadzības gadījumā iesaistīt 29. panta darba grupu un EDAU, lai konsultācijas notiktu pietiekami agrā stadijā, pirms izstrādāt attiecīgus pasākumus.

26. Turklāt EDAU ņem vērā grozījumus, ko Eiropas Parlaments ir pieņēmis saistībā ar priekšlikuma 6. pantu. EDAU vispirms norāda, ka grozījums, kas paredz vajadzības gadījumā atbalstīt anonīmu datu lietojumu, pēc būtības būtu ļoti apsveicams, tomēr neatrisinās visas datu aizsardzības problēmas, jo daudzi ar ITS starpniecību vāktie dati, kuros jādalās, var būt kvalificējami kā personas dati. Lai personas datu apstrāde notiktu anonīmi, būtu jāpanāk, lai neviena persona nevienā datu apstrādes stadijā – ņemot vērā visus iespējamos līdzekļus, ko loģiski varētu izmantot kāds datu kontrolieris vai cita persona – nevarētu datus saistīt ar tādiem datiem, kas attiektos uz kādu identificētu cilvēku, citādi tādi dati ir personas dati Direktīvas 95/46/EK 2.a panta nozīmē ([15]). Un, pamatojoties uz Eiropas Parlamenta ierosinātiem grozījumiem, EDAU iesaka ierosinātā tiesību akta 6. pantu pārveidot šādi:

— izvērtēt personas datu apstrādes vajadzīgumu ITS sistēmā vajadzētu, ņemot vērā likumīgus un konkrētus mērķus, kāpēc datus apstrādā (saskaņā ar Direktīvas 95/46/EK 6. un 7. pantu). Pašu ITS lietojumprogrammu ([16]) darbība nevar būt likumīgs mērķis, ar ko attaisnot datu apstrādi, jo lietojumprogramma ir tikai līdzeklis, ar ko vākt datus un apmainīties ar tiem, un to lietojumam būtu obligāti jābūt vērstam uz konkrētām vajadzībām,

— Grozījums ([17]) par ITS datu un ierakstu lietojuma aizliegumu "citiem mērķiem nekā tiem, kas ir minēti šajā direktīvā" neparedz pietiekamas garantijas, it īpaši jautājumā par konkrētiem mērķiem un pakalpojumiem, kam lietos ITS, direktīvā nav skaidri un pilnībā izklāstīti. Ņemot vērā to, ka ar ITS starpniecību veiks dažādas datu apstrādes darbības ļoti dažādiem mērķiem, būtu jānodrošina, lai datu apstrādes gaitā kādam konkrētam mērķim vāktus datus neizmantotu citiem mērķiem, kas ar to nav saderīgi – tas ir paredzēts Direktīvas 95/46/EK 6. panta 1. punkta b) apakšpunktā. EDAU tālab ierosina 6. panta 2. punktā izdarīt arī tādus grozījumus, kas nodrošinātu ITS datu un ierakstu neizmatošanu "citiem mērķiem nekā tiem, kam tie ir vākti, un kas nav saderīgi ar minētajiem mērķiem".

III. DATU AIZSARDZĪBA INTELIĢENTĀS TRANSPORTA SISTĒMĀS

27. Ir īpaši svarīgi, lai dažādu ITS jomā iesaistītu darbību veicēju uzdevumi būtu skaidri formulēti, apzinot, kas būs atbildīgs par nodrošinājumu, ka no datu aizsardzības perspektīvas sistēmas darbojas pareizi. Tālab vajadzētu vēl skaidrāk formulēt, kam būtu jāatbild par to lietojumprogrammu īstenošanu un sistēmu ieviešanu, kuru struktūru konkretizēs ar komitoloģijas starpniecību, un kas darbību veicēju ķēdē atbildēs par datu aizsardzības tiesību ievērošanu datu apstrādē (t. i., datu kontrolieri). EDAU še turpmāk uzsvērs dažus privātuma un datu aizsardzības aspektus, kam būtu jāpievēršas komitoloģijā un datu kontrolieriem, izstrādājot lietojumprogrammu un sistēmu arhitektūru. Turpinājumā viņš ieskicēs dažas datu aizsardzības problēmas, kam likumdevējiem un datu kontrolieriem ir jāpievēršas saistībā ar ITS pakalpojumu sniegšanu.

III.1. Integrēta privātās dzīves aizsardzība ("privacy by design")

28. Pareizs Direktīvā 95/46/EK izklāstīto datu aizsardzības principu piemērojums ir pamatnosacījums sekmīgai ITS ieviešanai Kopienā. Minētie principi rada sekas sistēmas arhitektūras un lietojumprogrammu izstrādē. EDAU

([15]) Kā teikts Direktīvas 95/46/EK 26. apsvērumā, "tā kā, lai noteiktu, vai persona ir identificējama, būtu jāņem vērā visi līdzekļi, kurus, iespējams, pamatoti izmantotu vai nu personas datu apstrādātājs, vai jebkura cita persona, lai identificētu minēto personu".

([16]) 34. grozījumā, ar ko ir ievadīts jauns 6. panta 1. punkta b) apakšpunkts, ir paredzēts: "Personas datus apstrādā tikai tiktāl, ciktāl to apstrāde ir vajadzīga ITS lietojumprogrammu darbības nodrošināšanai un/vai pakalpojumu sniegšanai."

([17]) Ar 36. grozījumu 6. panta 2. punkts ir papildināts šādi: "un nevar lietot citām vajadzībām kā vien šajā direktīvā minētās".

ierosina, izstrādājot ITS, jau agrā stadijā izmantot "integrētas privātās dzīves aizsardzības" pieeju, definējot lietojumprogrammu un sistēmu arhitektūru, darbību un apsaimniekošanu. Tāda pieeja ir īpaši uzsvērta Direktīvā 1999/5/EK ([18]), kas attiecas uz radio un telekomunikāciju termināliekārtu izstrādi.

29. ITS lietojumprogrammas un sistēmas izstrādās vairākās stadijās, to darīs dažādi darbību veicēji, un viņiem visiem vajadzētu ievērot privātuma un datu aizsardzības prasības. Pirmām kārtām Komisija un ITS komiteja būs konkrēti atbildīga par to, lai, izmantojot komitoloģijas procedūru, definētu pasākumus, standartizācijas ierosmes, procedūras un paraugpraksi, kam būtu jāveicina integrēta privātās dzīves aizsardzība ("*privacy by design*").

30. Integrēta privātās dzīves aizsardzība ("*privacy by design*") būtu jāveicina visās apstrādes stadijās, turklāt jebkādā apstrādē:

— privātums būtu jāņem vērā organizatoriskā līmenī, definējot visos attiecīgos datu apmaiņas punktos vajadzīgās datu apmaiņas procedūras – un tas var tieši ietekmēt to, kāda ir datu apmaiņa un ar kādiem datiem tā notiek,

— privātuma un drošības prasības būtu jāiestrādā standartos, paraugpraksē, tehniskās specifikācijās un sistēmās,

— EDAU iesaka tehniskā līmenī, piemēram, ar komitoloģijas starpniecību izstrādāt labākos pieejamos paņēmienus ([19]) (*Best Available Technique – BAT*) konkrētos privātuma, datu aizsardzības un drošības jomas sektoros un/vai konkrētiem mērķiem, un dažādie drošības parametri, kas būtu jāīsteno sistēmas kalpošanas laikā, būtu jādefinē tā, lai garantētu atbilsmi ES normatīvu sistēmai.

31. EDAU še turpmāk ieskicēs dažus jautājumus, kam konkrēti jāpievēršas, izstrādājot lietojumprogrammas un sistēmu arhitektūru. Tie attiecas uz savāktiem datiem, sistēmu sadarbspēju un datu drošumu.

III.1.a) *Datu apjoma samazinājums un anonimitāte*

32. Saskaņā ar Direktīvas 95/46/EK 6. panta 1. punkta c) apakšpunktu vākt un apstrādāt var tikai tādus personas datus, kas ir vajadzīgi un svarīgi konkrētiem mērķiem.

33. EDAU uzsver to, cik svarīgi ir pareizi klasificēt ar ITS starpniecību apstrādājamo informāciju un datus, pirms izstrādāt lietojumprogrammas un sistēmas, lai izvairītos no plašas un nepareizas personas datu vākšanas. Tādā sakarā būtu jāņem vērā:

— datu avots (neatkarīgi no tā, vai datus saņem no atklātībā pieejama avota, telekomunikāciju pakalpojumu sniedzēja, ITS pakalpojumu sniedzēja, kāda cita operatora, kāda transportlīdzekļa, kāda transportlīdzekļa lietotāja vai cita datu subjekta),

— datu būtība (piem., vai tā ir apkopota informācija, anonīmi dati, personas dati, diskrēti dati),

— kādiem mērķiem ir paredzēts datus lietot, un

— runājot par sadarbīgām sistēmām, būtu precīzi jānosaka, kādus datus automātiski vai piespiedu kārtā (*push/pull*) iegūst no transportlīdzekļiem, kādi ir dati, ar ko notiek apmaiņa ar citiem transportlīdzekļiem un/vai infrastruktūrām, un ar ko infrastruktūra apmainās ar citu infrastruktūru, un kādām vajadzībām tas notiek.

34. Atsevišķās funkcijas būtu rūpīgi jāanalizē saskaņā ar apzinātām vajadzībām, lai izvērtētu vajadzību vākt personas datus. EDAU uzsver to, cik svarīgi ir pareizi līdzsvarot datu subjektu pamattiesības ar dažādu iesaistīto darbību veicēju interesēm, un tas nozīmē, ka ir jāapstrādā tik maz personas datu, cik vien iespējams. Lietojumprogrammu un sistēmu arhitektūra pēc iespējas būtu jāizstrādā, lai vāktu tikai mērķu īstenošanai noteikti vajadzīgus personas datus.

35. Ja personas dati nav obligāti vai ir obligāti tikai agrā datu apstrādes stadijā, tos nevajadzētu vākt – vai tie jāpadara anonīmi cik drīz vien iespējams. Tādējādi ir īpaši svarīgi ne tikai izvērtēt to, cik ļoti ir jāvāc dati, bet arī to, cik svarīgi ir vāktos datus glabāt dažādās sistēmās. Visiem dažādajiem darbību veicējiem pakalpojumu ķēdē būtu jānosaka konkrēti personas datu glabāšanas termiņi, un tie būtu jādažādo atkarībā no datu tipa un mērķiem, kam tie ir vākti ([20]). Tālab, kad personas dati vairs nav jāglabā, lai sasniegtu mērķi, kam tie ir vākti vai apstrādāti, tie būtu jādara anonīmi, t. i., tiem vairs nevajadzētu būt atvedināmiem uz identificētiem vai identificējamiem indivīdiem.

36. Sistēmu arhitektūra un datu apmaiņa procedūras būtu jāizstrādā tā, lai vajadzētu apstrādāt tik maz personas datu cik vien iespējams. Tādā sakarā būtu jāņem vērā visas datu apstrādes stadijas un visi ITS pakalpojumu ķēdes darbību veicēji. Ja arī ar dažiem datiem var dalīties un tos apstrādāt anonīmi, citus datus – pat, ja ar tiem apmainās, nevienu neidentificējot – var saistīt ar konkrētu cilvēku datiem, un tālab tie būs personas dati Direktīvas 95/46/EK 2. panta

([18]) Galvenokārt 3.3. panta c) punkts Eiropas Parlamenta un Padomes Direktīvā 1999/5/EK (1999. gada 9. marts) par radioiekārtām un telekomunikāciju termināla iekārtām un to atbilstības savstarpējo atzīšanu.

([19]) Labākie pieejamie paņēmieni (*Best Available Techniques*) ir darbību visefektīvākā un modernākā izstrādes stadija, un to īstenošanas metodes, kas apliecina konkrēto paņēmienu praktisku piemērotību, lai pamatotu ITS drošības lietojumprogrammu un sistēmu atbilstību ES tiesiskā regulējumā noteiktām privātuma, datu aizsardzības un drošības prasībām.

([20]) Piemēram, satiksmes un atrašanās vietas datu apstrādi saistībā ar atklātībā pieejamiem elektroniskiem saziņas pakalpojumiem atklātībā pieejamos komunikāciju tīklos regulē ar Eiropas Parlamenta un Padomes Direktīvu 2006/24/EK (2006. gada 15. marts) par tādu datu saglabāšanu, kurus iegūst vai apstrādā saistībā ar publiski pieejamu elektronisko komunikāciju pakalpojumu sniegšanu vai publiski pieejamu komunikāciju tīklu nodrošināšanu, un par grozījumiem Direktīvā 2002/58/EK.

a) punkta nozīmē ([21]). Ņemot vērā mērķus, kam ITS lietos, šķiet grūti nodrošināt, lai lielu datu daudzumu, kas būs savākti ar ITS starpniecību, apstrādātu anonīmi, jo kādā konkrētā punktā, piemēram, sagatavojot rēķinus, būs jāuzrāda konkrētu cilvēku identitāte. Tālab būs vajadzīgi vismaz daži īpaši – tehniski, organizatoriski un juridiski – pasākumi, lai vairākās jomās nodrošinātu anonimitāti.

III.1.b) *Sadarbspēja, datu kvalitāte un to lietojuma ierobežojumi*

37. Lietojumprogrammu un sistēmu sadarbspēja ir sekmīgas ITS attīstības pamatelements. Notiks saskaņošana, lai lietojumprogrammās un sistēmās integrējamo saskarņu tehniskās specifikācijas definētu tā, ka tās varētu mijdarboties ar citām transporta veidosos un/vai sistēmās iestrādātām lietojumprogrammām. Kaut gan sistēmu sadarbspēja atvieglinās dažādu pakalpojumu sniegšanu un palīdzēs nodrošināt to konsekvenci visā Eiropā, tā rada vairākus apdraudējumus no datu aizsardzības viedokļa, piemēram, iespējamību, ka datus lietos nepareizi vai ļaunprātīgi. Visiem savstarpējiem datu bāzu savienojumiem būtu jānotiek, pienācīgi ievērojot datu aizsardzības principus ([22]) un reālus aizsardzības pasākumus (skat. arī III.1.c, iedaļu).

38. Direktīvas 95/46/EK 6. panta d) punktā pasludinātais datu kvalitātes princips lietojumprogrammu un sistēmu sadarbspējas kontekstā ir īpaši svarīgs. Saskarņu izstrādes vajadzībām definējamām tehniskām specifikācijām lietojumprogrammu un sistēmu savstarpējos savienojumos būtu jānodrošina iegūstamo datu precizitāte.

39. Tā kā sistēmu mijdarbība atvieglinās savstarpējus datu bāzu savienojumus un datu salāgošanu vēl citiem mērķiem, EDAU uzsver, ka visi savstarpējie savienojumi būtu jāveic uzmanīgi, ņemot vērā Direktīvas 95/46/EK 6. panta 1. punkta b) apakšpunktā formulēto lietojuma ierobežojuma principu. Īpaši svarīgi ir, lai izstrādātā ITS sistēmu arhitektūra liegtu jebkādu turpmāku datu lietojumu citiem mērķiem nekā tiem, kam tie ir vākti. Sistēmā ir jābūt iestrādātiem attiecīgiem aizsargelementiem, lai novērstu ierīču nepareizu lietojumu, datu neatļautu atklāšanu vai piekļuvi tiem, kā arī neparedzētas ierīču darbības sekas. Piemēram, būtu jāizvērš pietiekama aizsardzība, lai pārvietojamām iekārtām nepiekļūtu trešās puses, kam uz to nav tiesību, un tās neizmantotu iekārtas cilvēku identifikācijai un izsekošanai – mērķiem, kam sistēma nebūtu domāta.

40. Runājot par pašu savstarpējo savienojumu likumīgumu, to vajadzēs izvērtēt katrā konkrētā gadījumā, ņemot vērā tādu datu būtību, kurus, izmantojot sistēmas, dara pieejamus un ar ko apmainās, kā arī mērķus, kam tas ir paredzēts.

III.1.c) *Datu drošība*

41. Personas datu drošums ir ITS izvēršanas pamatelements. EDAU ir gandarīts par to, ka rīcības plānā un ierosinātajā direktīvā drošība ir skaidri piesaukta. Būtu jāparedz drošība ne tikai ITS ierīces darbības laikā (transportlīdzekļos iebūvētās sistēmās un paziņojumu pārsūtīšanas protokolos), bet arī neatkarīgi no ierīces darbības – datu bāzēs, kur datus apstrādā un/vai glabā. Attiecīgas tehniskas, administratīvas un organizatoriskas prasības būtu jādefinē visām datu apstrādes stadijām, nodrošinot pienācīga līmeņa drošību saskaņā ar Direktīvas 95/46/EK 16. un 17. pantu (kā arī, vajadzības gadījumā, Direktīvas 2002/58/EK 4. un 5. pantu).

42. Attiecīgi aizsargpasākumi būtu jānosaka pēc rūpīga, konkrēta izvērtējuma – kādām vajadzībām izmantos ITS, un kādi būs izmantotie datu apstrādes mehānismi. Tādā sakarā EDAU ierosina veikt privātuma un datu aizsardzības efektivitātes ekspertīzes konkrētās lietojuma jomās un/vai saistībā ar konkrētiem mērķiem (piem., ar drošību saistītās ITS sistēmās, kravas transporta satiksmes regulācijas sistēmās, utt.). Privātuma un datu aizsardzības efektivitātes ekspertīzes, kā arī labāko pieejamo privātuma un datu aizsardzības paņēmienu lietojums palīdzēs noteikt labākos aizsargpasākumus konkrētai datu apstrādei.

III.2. **Turpmāki datu aizsardzības un privātuma apsvērumi ITS pakalpojumu sniegšanā**

43. Lai novērstu neatbilstības ieviestajos ITS pakalpojumos, ES mērogā ir jāveic turpmāka ITS pakalpojumu ieviešanas mehānismu saskaņošana. Tādā sakarā EDAU vēlas izcelt divas problēmas, kas noteikti prasīs rūpīgāku aplūkojumu no privātuma un datu aizsardzības viedokļa, proti:

— atrašanās vietas noteikšanas instrumentu lietojums, sniedzot atklātībā pieejamus un maksas pakalpojumus, prasa, lai būtu īstenoti papildu drošības elementi. Tādā sakarā īpaša uzmanība būtu jāpievērš tam, vai un kad ITS atrašanās vietas noteikšanas pakalpojumus izmanto privātām vajadzībām, vai profesionālām vajadzībām, un kā konkrētus cilvēkus, kas transportlīdzekļus izmanto darbam, var ietekmēt tādu sistēmu lietojums,

— integrētās sistēmās īpaši svarīgi ir panākt, lai skaidri būtu formulēti dažādu ITS ieviešanā iesaistīto pušu uzdevumi un pienākumi.

([21]) Skat. 15. zemsvītras piezīmi.

([22]) Skat. arī EDAU piebildes saistībā ar Komisijas paziņojumu par Eiropas datu bāzu mijdarbību, 2006. gada 10. marts. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2006/06-03-10_Interoperability_EN.pdf

III.2.a) *Atrašanās vietas noteikšanas instrumentu lietojuma drošības elementi, sniedzot ITS atrašanās vietas noteikšanas pakalpojumus*

44. ITS ieviešana sekmēs tādu lietojumprogrammu izstrādi, ar ko izsekot un atrast preces, un dos iespēju ieviest brīvi pieejamus un/vai maksas pakalpojumus atkarībā no atrašanās vietas. Tādos pakalpojumos izmantos tehnoloģijas piemēram, atrašanās vietas noteikšanu, izmantojot satelītus, un radiofrekvenču identifikācijas (*RFID tags*) marķierus ([23]). Ir iecerēts navigācijas, atrašanās vietas konstatācijas un izsekošanas sistēmas lietot daudzām un dažādām vajadzībām, piemēram, transportlīdzekļu un kravu pārraudzībai no attāluma (*remote in-route monitoring*) (piem., pārvadājot bīstamas preces vai dzīvus lopus), transportlīdzekļu pavadzīmes formējot pēc daudziem un dažādiem parametriem, arī nobrauktā attāluma un diennakts stundas (piem., ceļu lietojuma maksa datorizētās ceļu lietojuma maksas iekasēšanas sistēmās), un šoferu pārraudzībai, lai pārbaudītu, kā viņi ievēro noteikumus, piemēram, pārbaudot braukšanas ilgumu (izmantojot digitālus tahografus) un lai uzliktu sankcijas (izmantojot transportlīdzekļu elektronisku identifikāciju).

45. Atrašanās vietas noteikšanas tehnoloģiju lietojums ir īpaši uzbāzīgs no privātuma viedokļa, jo ļauj izsekot šoferus un vākt daudzus dažādus datus par viņu braukšanas ieradumiem. 29. panta darba grupa ir uzsvērusi ([24]), ka atrašanās vietas datu apstrāde ir īpaši diskrēts jautājums, kurā svarīgākā problēma skar brīvību pārvietoties anonīmi, un kas prasa īstenot konkrētus drošības elementus, lai novērstu konkrētu cilvēku novērošanu un datu nepareizu lietojumu.

46. EDAU uzsver, ka atrašanās vietas noteikšanas instrumentu lietojumam ir jānotiek likumīgi, t. i., ar pareiziem juridiskiem pamatiem, skaidru un likumīgu vajadzību vārdā, un samērīgi ar iecerētajiem mērķiem. Veiktās datu apstrādes likumīgums būs ļoti atkarīgs no tā, kā izmantos atrašanās vietas noteikšanas instrumentus, un kādiem mērķiem tos izmantos. 29. panta darba grupa atzinumā par ārkārtas izsaukumiem (*eCall – emergency call*) ir uzsvērusi, ka "no datu aizsardzības viedokļa nebūs pieļaujams, ka tādas ierīces būtu pastāvīgi pievienotas, un transportlīdzekļi tālab būtu visu laiku izsekojami, jo varētu iedarbināt eCall ierīces" ([25]). Tālab ir svarīgi padarīt vēl skaidrākus konkrētus nosacījumus, kādos transportlīdzekļus izsekos, un kā izsekošana ietekmēs transportlīdzekļu lietotājus. Katrā ziņā atrašanās vietas konstatācijas ierīču lietojums būtu pamatojams ar likumīgām vajadzībām (piem., preču pārvadāšanas pārraudzībai) un tam būtu stingri jāaprobežojas ar to, kas ir vajadzīgs minētajām vajadzībām. Tādējādi ir svarīgi precīzi definēt, kādus atrašanās vietas datus vāc, kur tos glabā, un cik ilgi glabā, kas ir tie, ar ko tajos dalās un kādiem mērķiem tas notiek, un veikt visus vajadzīgos pasākumus, lai izvairītos no jebkāda nepareiza vai ļaunprātīga datu lietojuma.

47. Turklāt Direktīvas 2002/58/EK 9. pantā ir stingri normēta atklātībā pieejamu komunikāciju tīklu vai atklātībā pieejamu elektronisku komunikācijas pakalpojumu lietotāju atrašanās vietas datu apstrāde. Tajā ir skaidri prasīts, lai atrašanās vietas datu apstrāde notiktu anonīmi vai arī – ar informēta iekārtu lietotāja piekrišanu. Tas nozīmē, ka lietotājiem, pirms piekrist kāda atrašanās vietas noteikšanas instrumenta lietojumam, būtu jādara zināma attiecīga informācija, tostarp atrašanās vietas datu apstrādes tips, datu apstrādes mērķi un ilgums, un tas, vai datus pārsūtīs kādai trešai pusei – tādām vajadzībām, kas sniegs pakalpojumus ar pievienotu vērtību. Ir jābūt vienkāršam bezmaksas līdzeklim, kā lietotāji varētu uz laiku atteikties no atrašanās vietas datu apstrādes, ik reizi, pievienojoties tīklam vai ik reizi, pārsūtot kādu informāciju. Atrašanās vietas datu apstrādei būtu stingri jāaprobežojas ar personām, kas darbojas saskaņā ar atklātībā pieejamā komunikācijas tīkla vai atklātībā pieejamā komunikācijas pakalpojumu sniedzēja pilnvarām – vai tās trešās puses pilnvarām, kura sniedz pakalpojumus ar pievienotu vērtību.

48. Ir jāparedz papildu drošības elementi, ja atrašanās vietas datus vāc transportlīdzekļos, ko lieto profesionālām darbībām, novēršot to, ka atrašanās vietas tehnoloģijas lietotu, nevajadzīgi uzraugot darbiniekus. Katrā ziņā datu apstrādei būtu jāaprobežojas ar atrašanās vietas datu vākšanu darba laikā – tādējādi darbinieki varēs izslēgt atrašanās vietas noteikšanas funkciju pēc darba laika beigām un/vai lietojot transportlīdzekļus privātām vajadzībām.

49. Pastāv iespējamība, ka trešās puses (piemēram, apdrošināšanas sabiedrības, darba devēji un tiesībaizsardzības iestādes) likumīgām un konkrētām vajadzībām prasīs piekļuvi ar navigācijas un izsekošanas sistēmām vāktiem datiem (piemēram, lai izsekotu preces, elektroniskus ceļa lietošanas nodevas maksājumus, utt.), lai tos lietotu sekundāriem mērķiem, piemēram, pārbaudītu braukšanas un atpūtas laika ilgumu vai pārliecinātos, kā ir ievēroti ceļu lietošanas noteikumi, un lai uzliktu sankcijas. Faktiski, ja piekļuve kalpo vajadzībām, kas nav saderīgas ar mērķiem, kam dati ir vākti, piekļuve tiem sekundāru vajadzību dēļ

([23]) Eiropas datu aizsardzības uzraudzītāja atzinums saistībā ar Komisijas paziņojumu Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai par radiofrekvenču identifikāciju (*Radio Frequency Identification – RFID*) Eiropā – ceļā uz politikas izstrādi COM(2007) 96, OV C 101, 23.4.2008., 1. lpp. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-12-20_RFID_EN.pdf

([24]) 29. panta darba grupa, Atzinums par atrašanās vietas datu izmantojumu, lai sniegtu pakalpojumus ar pievienotu vērtību, WP 115, 2005. gada novembris. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_en.pdf

([25]) Skat. WP 125 par *eCall*, 5. lpp., kā minēts 10. zemsvītras piezīmē.

nav pieļaujama. Piekļuvi, atkāpjoties no minētā principa, var atļaut tikai, ja piekļuves nosacījumi atbilst Direktīvas 95/46/EK 13. panta stingrajām prasībām. Tālab jebkāda trešo pušu piekļuve atrašanās vietas datiem būtu jānodrošina tikai saskaņā ar tiesībām, turklāt pārskatāmi, saskaņā ar kādu juridisku pasākumu, kas nosaka attiecīgas procedūras un mehānismus, kā datiem piekļūst konkrētu vajadzību dēļ, un kas konkrētiem cilvēkiem nodrošinātu pietiekamus drošības elementus saskaņā ar vēl citiem mērķiem, kam varētu izmantot viņu datus.

III.2.b) *ITS darbību veicēju uzdevumi un pienākumi*

50. Nav vēl skaidrs, kas kurā katrā datu apstrādes daļā būs datu kontrolieris. Daudzos gadījumos ITS pakalpojumu sniedzēji droši vien būs datu kontrolieri – vieni paši – un apstrādās personas datus, lai sniegtu ITS pakalpojumus – vai kopā ar kādiem – un apstrādās datus līdz ar citiem datu kontrolieriem. Katrā datu apstrādes daļā būtu skaidri jāformulē dažādi pilnvarotu, ITS darbībās iesaistītu operatoru – datu kontrolieru un datu apstrādātāju – uzdevumi un pienākumi (piem., uzdevumi un pienākumi telekomunikāciju operatoriem, kas sniedz sakaru pakalpojumus, kā arī ITS pakalpojumus).

51. Personas, kas veiks datu kontrolieru pienākumus, atbildēs ([26]) par sistēmu un pakalpojumu atbilsmi visiem datu aizsardzības pienākumiem, un it īpaši, īstenojot sistēmas, kurās būs iestrādāta "integrēta privātās dzīves aizsardzība", kurās ievēro datu kvalitātes un lietojuma ierobežojuma principus, un datiem garantē attiecīga līmeņa drošumu, kā aprakstīts III. daļas 1. punktā.

52. Datu kontrolieriem būs jānodrošina attiecīgu drošības elementu iestrāde visos ITS ieviešanā iesaistīto darbību veicēju ķēdes posmos. Tas noteikti prasīs viņiem stāties attiecīgās līgumattiecībās ar visām datu apmaiņā un apstrādē iesaistītām ieinteresētām pusēm, un līgumattiecībām būtu jāparedz pietiekami datu aizsardzības drošības elementi (it īpaši saistībā ar Direktīvas 95/46/EK 16. un 17. pantu, un Direktīvas 2002/58/EK 4. un 5. pantu). No datu aizsardzības perspektīvas ir svarīgi ņemt vērā, ka datu kontrolieriem gan ir jānodrošina datu aizsardzības garantijas visās datu apstrādes stadijās, bet viņi ir un paliek atbildīgi par datu apstrādi un nevar līgumā paredzēt izvairīšanos no atbildības.

IV. **SECINĀJUMI**

53. EDAU ir gandarīts par Komisijas ierosināto ITS ieviešanas plānu, kas paredz visā Eiropā saskaņot datu apstrādi, atvieglinot ITS pakalpojumu sniegšanu, un kurā datu aizsardzība ir izvirzīta par pamatnosacījumu, lai Eiropā nopietni ieviestu ITS.

54. EDAU norāda, ka ierosinātajā direktīvā ir ieskicēta vispārēja sistēma, kas rada vairākas privātuma un datu aizsardzības problēmas, kuras vēl jārisina ES un valstu mērogā

— pastāv iespējamība, ka nepietiekama ierosinātā tiesiskā regulējuma skaidrība liks Eiropā dažādi īstenot ITS, un tas Eiropā radīs dažādu līmeņu datu aizsardzību. EDAU uzsver, ka minētie jautājumi ir labāk jāsaskaņo ES mērogā, lai neatrisinātās problēmas padarītu skaidrākas (piemēram, noteiktu ITS darbību veicēju uzdevumus un pienākumus, konkrēti kādām ITS lietojumprogrammām un sistēmām jābūt iestrādātām transportlīdzekļos, izstrādātu saskaņotus ITS pakalpojumu līgumus, konkretizētu ITS lietojuma mērķus un mehānismus, utt.). Ir īpaši svarīgi apzināt, kas būs datu kontrolieri no veicamās datu apstrādes viedokļa, jo viņu atbildībā būs nodrošināt privātuma un datu aizsardzības apsvērumu īstenošanu visos datu apstrādes ķēdes posmos,

— Eiropas Parlamentam un Padomei, nevis ar komitoloģijas procedūru, būtu jāpieņem lēmumi par dažiem datu apstrādes mehānismiem, kas varētu nopietni ietekmēt konkrētu cilvēku privātuma un datu aizsardzības tiesības,

— ir ļoti būtiski no agras datu apstrādes stadijas un visās datu apstrādes stadijās ņemt vērā privātumu un datu aizsardzību; "Integrētas privātās dzīves aizsardzības" īstenošanai būtu jāveicina tādas ITS lietojumprogrammas un sistēmas, un tā būtu jāiestrādā standartos, paraugpraksēs, tehniskās specifikācijās un sistēmās,

— visi savstarpēji lietojumprogrammu un sistēmu savienojumi būtu jāveic, pienācīgi ievērojot datu aizsardzības principus un reālus aizsardzības pasākumus,

— runājot par šajā stadijā atlikušām neskaidrībām saistībā ar ITS ieviešanas mehānismiem, EDAU īpaši sveic Komisijas paziņojumā ietverto ierosmi, ka privātuma ekspertīzei būtu jānotiek līdz 2011. gadam. Turklāt viņš stingri iesaka ITS privātuma un datu aizsardzības efektivitātes ekspertīzes veikt saistībā ar konkrētām lietojuma jomām un/vai mērķiem, nosakot attiecīgus aizsargpasākumus, kā arī attīstīt labākos pieejamos paņēmienus (*Best Available Techniques*) privātuma, datu aizsardzības un drošības jomā,

— EDAU īpaši uzsver, ka dalībvalstis būs atbildīgas par direktīvas pareizu īstenošanu, lai ITS operatori īstenotu sistēmas un pakalpojumus, kas visā Eiropā nodrošinātu attiecīga līmeņa datu aizsardzību,

([26]) Skat. 13. zemsvītras piezīmi.

— datu kontrolieriem, kuri sniedz ITS pakalpojumus, būtu jāīsteno attiecīgi drošības aizsargmehānismi, lai atrašanās vietas noteikšanas tehnoloģijas, piemēram, atrašanās vietas noteikšana, izmantojot satelītus un *RFID* marķierus, transportlīdzekļos netraucētu konkrētu cilvēku privātumu tīri privātā vai darba sakarā. Tas noteikti liks aprobežot datu apstrādi ar tādiem datiem, kas noteikti ir vajadzīgi konkrētiem mērķiem, nodrošinot, lai sistēmās būtu iestrādāti attiecīgi aizsargpasākumi, kas neļautu atklāt atrašanās vietas datus tādiem, kuri nav pilnvaroti tos saņemt, un kas lietotājiem nodrošinātu praktisku iespēju izslēgt atrašanās vietas noteikšanas ierīci/funkciju.

55. EDAU ierosina priekšlikuma 6. pantā saskaņā ar Direktīvu 95/46/EK izdarīt šādus grozījums:

— apstrādājot datus ar ITS starpniecību, būtu jāveicina izmantojamo datu apjoma samazinājums. Tādā sakarā ir ieteikts izdarīt šādus grozījumus priekšlikuma 6. panta 1. punkta b) apakšpunktā – "Personas datus apstrādā tikai tiktāl, ciktāl datu apstrāde ir vajadzīga konkrētiem mērķiem, kam izmanto ITS, un saskaņā ar attiecīgu juridisku pamatu".

— ir svarīgi, lai personas datus, ko apstrādā ar sadarbspējīgām sistēmām, neizmantotu vēl citiem mērķiem, kas nesader ar vajadzībām, kam tie ir vākti. Tālab ir ieteikts izdarīt 6. panta 2. punktā šādus grozījumus – "un nevar izmantot citiem mērķiem kā vien tiem, kam tie ir vākti, un tā, ka tas nesader ar minētajiem mērķiem.",

— viņš aicina pievienot skaidru atsauci uz integrētas privātās dzīves aizsardzības ("*privacy by design*") jēdzienu, lai varētu izstrādāt priekšlikuma 6. pantā paredzētās ITS lietojumprogrammas un sistēmas. Turklāt viņš ierosina 29. panta darba grupai un EDAU sūtīt informāciju un konsultēties ar viņiem par turpmākām darbībām, ko veiks, risinot šo problēmu, izmantojot komitoloģijas procedūru.

56. EDAU iesaka arī priekšlikuma apsvērumos dot atsauci uz šo atzinumu.

57. Neaizmirstot iepriekš minēto, EDAU ierosina datu aizsardzības iestādēm, it īpaši ar 29. panta darba grupas un EDAU starpniecību, cieši iekļauties ar ITS ieviešanu saistītās ierosmēs, izmantojot konsultācijas pietiekami agrā stadijā, pirms izstrādāt attiecīgus pasākumus.

Brisele, 2009. gada 22. jūlijā

Eiropas Datu aizsardzības uzraudzītājs

Peter HUSTINX