

# DEN EUROPÆISKE TILSYNSFØRENDE FOR DATABESKYTTELSE

## Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse (EDPS) om Kommissionens meddelelse om en handlingsplan for udbygning af intelligente transportsystemer i Europa og det ledsagende forslag til Europa-Parlamentets og Rådets direktiv om fastlæggelse af rammerne for ibrugtagning af intelligente transportsystemer på vejtransportområdet og for grænsefladerne til andre transportmåder

(2010/C 47/02)

DEN EUROPÆISKE TILSYNSFØRENDE FOR DATABESKYTTELSE,

som henviser til traktaten om oprettelse af Det Europæiske Fællesskab, særlig artikel 286,

som henviser til Den Europæiske Unions charter om grundlæggende rettigheder, særlig artikel 8,

som henviser til Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger,

som henviser til Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor,

som henviser til Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger, særlig artikel 41, og

som henviser til Kommissionens anmodning om en udtalelse i overensstemmelse med artikel 28, stk. 2, i forordning (EF) nr. 45/2001, der blev modtaget den 11. februar 2009,

HAR VEDTAGET FØLGENDE UDTALELSE:

### I. INDLEDNING

1. Kommissionen vedtog den 16. december 2008 en meddelelse med en handlingsplan for udbygning af intelligente

transportsystemer i Europa (i det følgende benævnt »meddelelsen«) <sup>(1)</sup>. Meddelelsen ledsages af et forslag til Europa-Parlamentets og Rådets direktiv om fastlæggelse af rammerne for ibrugtagning af intelligente transportsystemer på vejtransportområdet og for grænsefladerne til andre transportmåder (i det følgende benævnt »forslaget«) <sup>(2)</sup>. Kommissionen har sendt EDPS meddelelsen og det ledsagende forslag med henblik på en udtalelse i overensstemmelse med artikel 28, stk. 2, i forordning (EF) nr. 45/2001 <sup>(3)</sup>.

2. EDPS hilser det velkommen, at han høres, og anbefaler, at der henvises til denne høring i forslagens betragtninger på samme måde som i en række andre retsakter, hvor EDPS er blevet hørt i overensstemmelse med forordning (EF) nr. 45/2001.

### I.1. Meddelelse fra Kommissionen om en handlingsplan for udbygning af intelligente transportsystemer i Europa

3. Intelligente transportsystemer (ITS) er avancerede anvendelser, der gør brug af informations- og kommunikationsteknologi (ikt), som er indbygget i forskellige transportmåder med henblik på samspil mellem dem. Inden for vejtransport vil ITS levere innovative tjenester for så vidt angår transportmåder og trafikstyring til forskellige brugere som f.eks. rejsende, vejtransportinfrastrukturbrugere og -operatører, vognparkadministratorer og operatører af beredskabstjenester.

4. På baggrund af den stadig større udbygning af ITS inden for forskellige transportmåder <sup>(4)</sup> i Den Europæiske Union har Kommissionen vedtaget en handlingsplan for at fremskynde indførelsen og brugen af ITS-applikationer og

<sup>(1)</sup> KOM(2008) 886 endelig. Rådet vedtog konklusioner vedrørende meddelelsen på 2935. samling i Rådet (transport, telekommunikation og energi) den 30.-31. marts 2009.

<sup>(2)</sup> KOM(2008) 887 endelig.

<sup>(3)</sup> Europa-Parlamentets og Rådets forordning (EF) nr. 45/2001 af 18. december 2000 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i fællesskabsinstitutionerne og -organerne og om fri udveksling af sådanne oplysninger (EFT L 8 af 12.1.2001, s. 1).

<sup>(4)</sup> Der er mange initiativer på EU-plan, der integrerer ITS i forskellige transportmåder, herunder lufttransport (SESAR), vandveje (RIS), jernbaner (ERTMS, TAF-TSI), søfart (VTMIS, AIS, LRIT) og vejtransport (eToll, eCall), se KOM(2008) 886 endelig, s. 3.

-tjenester inden for vejtransport. Planen tager sigte på at sikre samspillet mellem disse og andre transportmåder, hvilket vil lette leveringen af multimodale tjenester. En sammenhængende udbygning af ITS i Europa vil bidrage til forskellige fællesskabsmål, herunder transportens effektivitet, bæredygtighed og sikkerhed, og samtidig fremme EU's indre marked og konkurrenceevne. I betragtning af de forskelligartede mål, der søges nået med udbygningen af ITS, skitserer meddelelsen seks hovedindsatsområder i perioden 2009-2014. Med henblik på gennemførelse af planen foreslår Kommissionen, at der fastlægges et EU-retsgrundlag i form af et direktiv, i henhold til hvilket der vil blive fastsat en række foranstaltninger på udvalgte hovedindsatsområder.

### 1.2. Forslag til direktiv om fastlæggelse af rammerne for ibrugtagning af ITS på vejtransportområdet og for grænsefladerne til andre transportmåder

- Forslaget fastlægger rammer for tværnational ibrugtagning af ITS-applikationer, der skal lette leveringen af harmoniserede tjenester på tværs af landegrænser, især for trafik- og rejseinformation samt trafikstyring. Det kræver, at medlemsstaterne træffer en række tekniske foranstaltninger for at lette dataudvekslingen mellem brugere, offentlige myndigheder, relevante interessenter og ITS-tjenesteudbydere og for at integrere sikkerheds- og sikringsrelaterede ITS-systemer i køretøjer og vejinfrastruktur. Der vil blive defineret tekniske specifikationer for ITS-applikationer og -systemer inden for fire af de prioriterede områder<sup>(5)</sup>, der er anført i handlingsplanen, efter en udvalgsprocedure<sup>(6)</sup>; specifikationernes centrale elementer er præciseret i bilag II til forslaget. Det er imidlertid ikke klart, hvilke specifikke formål ITS vil blive brugt til på disse områder. Ibrugtagningen af ITS kan endvidere udvides til mange flere områder end de fire, der i første omgang er udvalgt til udvikling af harmoniserede tekniske specifikationer. Mens forslaget hovedsagelig vedrører ibrugtagningen af fremtidige ITS-applikationer og -tjenester, skal det også, hvor det er muligt, omfatte teknologier, der allerede findes eller er under udvikling på området (som f.eks. eCall og eToll).

- Forslaget er blevet tilsendt Europa-Parlamentet, som vedtog sin holdning i forbindelse med førstebehandlingen<sup>(7)</sup> den

<sup>(5)</sup> Ifølge artikel 4 i forslaget skal der defineres tekniske foranstaltninger på følgende områder: i) optimal udnyttelse af vej-, trafik- og rejse-data, ii) kontinuitet i ITS-tjenester til trafik- og godsstyring i europæiske transportkorridorer og i byområder, iii) færdselssikkerhed og -sikring og iv) integration af køretøjet i transportinfrastrukturen.

<sup>(6)</sup> Forslaget indeholder en forskriftsprocedure med kontrol, jf. artikel 5a, stk. 1-4, og artikel 7 i afgørelse 1999/468/EF.

<sup>(7)</sup> Europa-Parlamentets lovgivningsmæssige beslutning af 23. april 2009 om forslaget til Europa-Parlamentets og Rådets direktiv om fastlæggelse af rammer for udbygning af intelligente transportsystemer på vejtransportområdet samt etablering af kontaktholder med andre transportformer (T6-0283/2009).

23. april 2009. Det Europæiske Økonomiske og Sociale Udvalg vedtog en udtalelse om forslaget den 13. maj 2009<sup>(8)</sup>, efter at Rådet den 29. januar 2009 havde anmodet det om at udtale sig.

### 1.3. Fokus for denne udtalelse

- EDPS hilser høringen om den af Kommissionen foreslåede plan for ibrugtagningen af ITS velkommen. Det er ikke første gang, EDPS beskæftiger sig med de spørgsmål, der rejses i ITS-handlingsplanen. EDPS har afgivet udtalelse om Kommissionens forslag om fremme af grænseoverskridende retshåndhævelse på trafikikkerhedsområdet<sup>(9)</sup> og bidraget til arbejdet i Artikel 29-Gruppen vedrørende et arbejdsdokument om eCall<sup>(10)</sup>.
- Intelligente transportsystemer er baseret på indsamling, behandling og udveksling af et bredt spektrum af data fra offentlige og private kilder; der er altså tale om et dataintensivt område. Ibrugtagningen af ITS vil i vid udstrækning være baseret på geolokaliseringsteknologi som f.eks. satellitbaseret stedsbestemmelse og trådløs teknologi som RFID, der vil lette leveringen af forskellige offentlige og/eller kommercielle positionsbaserede tjenester (f.eks. tidstro trafikmeldinger, e-fragt, eCall, eToll og parkeringsreservation). Nogle af de oplysninger, der vil blive behandlet via ITS, er aggregerede — som f.eks. oplysninger om trafik, ulykker og muligheder — og vedrører ikke nogen fysisk person, mens andre oplysninger vedrører identificerede eller identificerbare fysiske personer og derfor skal betragtes som personoplysninger som defineret i artikel 2, litra a), i direktiv 95/46/EF.
- EDPS finder det væsentligt, at de foranstaltninger, som der er planer om i forbindelse med ibrugtagningen af ITS, er i overensstemmelse med det eksisterende regelsæt som nævnt i forslaget, især direktiv 95/46/EF om databeskyttelse<sup>(11)</sup> og direktiv 2002/58/EF om databeskyttelse inden for elektronisk kommunikation<sup>(12)</sup>.

<sup>(8)</sup> Det Europæiske Økonomiske og Sociale Udvalgs udtalelse om forslaget til Europa-Parlamentets og Rådets direktiv om fastlæggelse af rammerne for ibrugtagning af intelligente transportsystemer på vejtransportområdet og for grænsefladerne til andre transportmåder (TEN/382 af 13 maj 2009).

<sup>(9)</sup> Udtalelse fra Den Europæiske Tilsynsførende for Databeskyttelse om forslaget til Europa-Parlamentets og Rådets direktiv om fremme af grænseoverskridende retshåndhævelse på trafikikkerhedsområdet (2008/C 310/02, EUT C 310 af 5.12.2008, s. 9).

<sup>(10)</sup> Artikel 29-Gruppens arbejdsdokument om databeskyttelse og beskyttelse af privatlivets fred i forbindelse med eCall-initiativet (WP 125 af 26. september 2006) [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2006/wp125\\_da.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp125_da.pdf)

<sup>(11)</sup> Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (EFT L 281 af 23.11.1995, s. 31).

<sup>(12)</sup> Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktivet om databeskyttelse inden for elektronisk kommunikation) (EFT L 201 af 31.7.2002, s. 37).

10. Kommissionen har peget på uløste spørgsmål i forbindelse med beskyttelse af privatlivets fred og databeskyttelse som en af de største hindringer for fremme af ITS. Disse spørgsmål vil blive behandlet som følger i denne udtalelse:

— I kapitel II gennemgås Kommissionens forslag til bestemmelser for ibrugtagningen af ITS set ud fra et databeskyttelsesperspektiv.

— Kapitel III fremhæver de nødvendige databeskyttelses-hensyn, der yderligere skal tages i forbindelse med den egentlige ibrugtagning af ITS:

— I første punkt understreges behovet for »privacy by design« (indbygget databeskyttelse) i forbindelse med udviklingen af ITS, og det skitseres endvidere, hvilke vigtige spørgsmål der skal tackles under udformningen af ITS-applikationer og databeskyttelsessystemer.

— Andet punkt fokuserer på nogle af de privatlivs-hensyn, som man yderligere skal holde sig for øje i forbindelse med leveringen af ITS-tjenester.

## II. GENNEMGANG AF DE BESTEMMELSER, DER FORESLÅS FOR IBRUGTAGNINGEN AF ITS

11. Kommissionens forslag til direktiv indeholder to bestemmelser (betragtning 9 og artikel 6), der beskæftiger sig med privatlivets fred, sikkerhed og videreanvendelse af oplysninger. Ifølge artikel 6, stk. 1, i Kommissionens forslag skal brugen af ITS foregå i overensstemmelse med databeskyttelsesreglerne, som de bl.a. er fastsat i direktiv 95/46/EF og 2002/58/EF. Artikel 6, stk. 2, i Kommissionens forslag omhandler konkrete databeskyttelsesforanstaltninger, hovedsagelig set ud fra et sikkerhedssynspunkt: artikel 6, stk. 2, i forslaget lyder således: »Medlemsstaterne skal navnlig sikre, at ITS-data og -registre beskyttes mod misbrug, herunder ulovlig adgang, ændring eller tab.«. Endelig hedder det i artikel 6, stk. 3, i Kommissionens forslag, at »direktiv 2003/98/EF finder anvendelse«.

12. Europa-Parlamentet har foreslået førstebehandlings-ændringer vedrørende artikel 6. Navnlig tilføjes der tre nye stykker i artikel 6, der vedrører anvendelse af anonyme oplysninger, hvor dette er muligt, behandling af

følsomme oplysninger alene når den registrerede har givet sit samtykke på et kvalificeret grundlag, og sikkerhed for, at personoplysninger kun behandles, »hvis behandlingen er nødvendig til afvikling af ITS-applikationen og/eller -tjenesten«. Desuden ændres artikel 6, stk. 2, idet det tilføjes, at ITS-data og -registre ikke må »anvendes til andre formål end dem, der er nævnt i dette direktiv«.

13. EDPS hilser det velkommen, at der er taget hensyn til databeskyttelse i forbindelse med udarbejdelsen af forslaget, og at databeskyttelse gøres til en generel betingelse for selve ibrugtagningen af ITS i Europa. EDPS erkender, at der er et behov for en konsekvent harmonisering af data-processer på EU-plan for at sikre, at ITS-applikationerne og -tjenesterne fungerer overalt i Europa.

14. EDPS bemærker imidlertid, at de foreslåede bestemmelser er for brede og generelle til, at der kan tages tilstrækkeligt hensyn til de privatlivs- og databeskyttelsesspørgsmål, som ibrugtagningen af ITS i medlemsstaterne rejser. Det er ikke klart, hvornår afviklingen af ITS-tjenester fører til indsamling og behandling af personoplysninger, til hvilke specifikke formål der foregår databehandling, eller hvilket retsgrundlag der berettiger en sådan behandling. Endvidere giver anvendelsen af lokaliseringsteknologier med henblik på ibrugtagningen af ITS risiko for, at der udvikles tjenester, der er privatlivskrænkende, hvis de medfører indsamling og udveksling af personoplysninger. Desuden fremgår det ikke klart af forslaget, hvilke roller og hvilket ansvar de forskellige operatører i ITS-ibrugtagningskæden har, og det er derfor vanskeligt at vide, hvilke operatører der bliver registeransvarlige og derfor får ansvaret for, at databeskyttelseskravene opfyldes<sup>(13)</sup>. ITS-operatører vil komme til at stå over for store problemer, hvis alle disse spørgsmål ikke præciseres i lovgivningen, eftersom de i sidste ende vil skulle stå for anvendelsen af de foranstaltninger, der fastsættes i det foreslåede direktiv.

15. Der er derfor en risiko for, at manglen på klarhed i det foreslåede regelsæt vil føre til uensartet gennemførelse af ITS i Europa, og at dette — i stedet for at mindske forskellene mellem medlemsstaterne — derimod vil skabe betydelig usikkerhed og fragmentering og betydelige uoverensstemmelser på grund af forskellige databeskyttelsesniveauer i Europa. Dette kan også føre til manglende overensstemmelse med de væsentlige databeskyttelsesregler. EDPS understreger behovet for yderligere EU-harmonisering på disse områder. EDPS vil her foreslå ændringer i det foreslåede regelsæt ud fra et databeskyttelsessynspunkt. Han

<sup>(13)</sup> Ifølge artikel 2, litra d), artikel 6, stk. 2, og artikel 23 i direktiv 95/46/EF som nævnt i fodnote 11.

anbefaler kraftigt, at Parlamentet og Rådet indsætter de foreslåede ændringer i forslaget og om muligt indsætter yderligere bestemmelser, der præciserer udestående spørgsmål (som f.eks. definition af ITS-aktører og deres ansvar og udvikling af harmoniserede kontrakter om levering af ITS-tjenester). Han understreger endvidere, at medlemsstaterne også vil have ansvaret for at gennemføre direktivet korrekt, således at operatørerne kan udvikle systemer og tjenester, der giver et passende databeskyttelsesniveau i hele Europa.

## II.1. Databehandlingsaktiviteter skal være baseret på et passende retsgrundlag

16. Det er ikke klart, hvornår behandlingen af personoplysninger går i gang, når først ITS-udstyret er integreret i et køretøj, og hvilket retsgrundlag der vil ligge til grund for behandlingen. Operatører kan basere sig på forskellige retsgrundlag, når det gælder databehandling, bl.a. et utvetydigt samtykke fra brugerne, en kontrakt eller en retlig forpligtelse, som den registeransvarlige skal efterleve. Det er nødvendigt at harmonisere retsgrundlaget for behandlingen af data via ITS for at sikre, at systemerne fungerer i hele Europa, og at brugerne ikke lider under forskelle mellem databehandlingsmetoderne i de enkelte EU-lande.
17. I en række tilfælde vil ITS-systemer automatisk blive integreret i køretøjer. Dette gælder især sikkerheds- og sikringsrelaterede ITS-systemer, der skal indbygges i køretøjer i henhold til forslaget. Forslaget definerer imidlertid ikke, hvad »sikkerheds- og sikringsrelaterede ITS-systemer« er, og det bør derfor præciseres yderligere, hvilke specifikke ITS-applikationer og -systemer der skal indbygges i køretøjer. Det bør endvidere gøres klart, om aktiveringen og brugen af udstyret vil være frivillig eller obligatorisk for brugerne. Hvis det vælges at foretage databehandling på obligatorisk grundlag, bør den kun foretages til specifikke formål af tvingende grunde (f.eks. sporing af varer med henblik på godsstyring) og med passende garantier for så vidt angår behandlingen af personoplysninger. Hvis brugen af ITS foregår på frivilligt grundlag, bør der indføres passende garantier for at hindre, at blot fordi systemet findes i et køretøj, anses brugeren for at implicit have givet samtykke til, at det bruges.
18. EDPS går ind for den valgmulighed, at ITS-tjenester leveres på frivilligt grundlag. Dette betyder, at brugere frit skal kunne give deres samtykke til brugen af systemet og til de specielle formål, som det vil blive brugt til. Når den leverede tjeneste er baseret på lokaliseringsdata, skal brugeren underrettes på passende måde (navnlig i overensstemmelse med artikel 9 i direktiv 2002/58/EF) og skal kunne trække sit samtykke tilbage. Rent praktisk kræver dette, at der indføres en let metode til at deaktivere dette system og/eller denne mekanisme uden tekniske eller finansielle hindringer for brugeren<sup>(14)</sup>, når denne ikke længere samtykker til brugen af systemet og/eller af en bestemt mekanisme. Der bør indføres yderligere garantier, således at brugerne ikke diskrimineres, når de afslår at bruge en tjeneste.

19. I tilfælde, hvor visse behandlingsaktiviteter er obligatoriske, og andre kræver brugerens samtykke, skal der sikres åbenhed omkring de forskellige databehandlingsoperationer, der udføres, ved at brugeren modtager passende underretning om den obligatoriske og/eller frivillige karakter af hver enkelt behandling og dens rækkevidde. Det vil endvidere være afgørende, at der indføres passende sikkerhedsgarantier, således at der ikke indsamles og behandles data ud over, hvad der er fastsat i lovgivningen og/eller aftalt på frivilligt grundlag.
20. I betragtning af den tværnationale virkning af ITS-tjenester anbefaler EDPS endvidere, at der udvikles paneuropæiske standardkontrakter for at sikre, at tjenester leveret via ITS giver den samme databeskyttelsessikkerhed i hele Europa, og især at brugerne underrettes tilstrækkeligt klart om de specifikke mekanismer, der bruges, om den virkning, som brugen af specifik teknologi har for beskyttelsen af deres data, og om, hvordan de kan udøve deres rettigheder. Når der tilføjes nye mekanismer, bør tjenesteudbydere tage yderligere skridt til at underrette brugerne klart og specifikt om disse ekstra mekanismer og til at indhente deres samtykke til brugen heraf.

## II.2. Formålet med og de nærmere regler for databehandlingen skal præciseres yderligere

21. EDPS noterer sig, at forslaget ikke præcist definerer de specifikke tjenester og formål, som ITS-applikationer kan bruges til, og dette står derfor åbent. Dette giver fleksibilitet i praksis, men betyder også, at uløste spørgsmål angående beskyttelse af privatlivets fred og databeskyttelse — som Kommissionen har identificeret som en af de største hindringer for fremme af ITS (se punkt 10) — måske forbliver uløst og kan hindre en afbalanceret gennemførelse af de foreslåede foranstaltninger.
22. EDPS understreger, at det er specielt vigtigt, at databehandling med henblik på levering af specifikke ITS-tjenester ikke kun foregår på basis af et passende retsgrundlag, men også til udtrykkeligt angivne og legitime formål, og at den pågældende behandling står i forhold til og er nødvendig til disse formål (artikel 6 i direktiv 95/46/EF). Det bør derfor overvejes, om det eventuelt er nødvendigt at fastsætte yderligere EU-bestemmelser for specifik brug af ITS for at sørge for et harmoniseret og tilstrækkeligt retsgrundlag for den databehandling, der skal foregå, og for at undgå uoverensstemmelser mellem medlemsstaterne i forbindelse med ibrugtagningen af ITS-tjenester.
23. Inden for de foreslåede rammer er der foreløbig ikke truffet nogen beslutning om de nærmere regler for databehandling og dataudveksling med henblik på brug af ITS. Valget af mange tekniske parametre, som vil få forskellige konsekvenser for beskyttelsen af privatlivets fred og databeskyttelsen, vil først blive truffet på et senere tidspunkt efter udvalgsproceduren. I betragtning af den specielle beskyttelse, som privatliv og personoplysninger i deres egenskab af grundlæggende rettigheder er omfattet af i henhold til

<sup>(14)</sup> Se WP 125 om eCall, s. 4, som nævnt i fodnote 10.

artikel 8 i den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder og artikel 7 og 8 i Den Europæiske Unions charter om grundlæggende rettigheder, kan der sættes spørgsmålstegn ved, om og i hvilken udstrækning definitionen af databehandlingsoperationer bør besluttes efter udvalgsproceduren.

24. I et demokratisk samfund bør beslutninger om væsentlige principper og regler, der berører de grundlæggende rettigheder, træffes inden for rammerne af en fuld lovgivningsprocedure, der omfatter de rette kontrolmekanismer. Dette betyder derfor, at beslutninger, der har større indvirkning på fysiske personers ret til beskyttelse af privatlivets fred og databeskyttelse — f.eks. vedrørende formålene med og reglerne for obligatorisk databehandlingsaktiviteter og fastlæggelsen af regler for ibrugtagning af ITS på nye områder — bør træffes af Europa-Parlamentet og Rådet og ikke efter udvalgsproceduren.
25. På den baggrund råder EDPS kraftigt til, at Artikel 29-Gruppen og EDPS, hvor det er relevant, inddrages i arbejdet i det udvalg, der nedsættes ved artikel 8 i forslaget, og i fremtidige foranstaltninger, der træffes angående ibrugtagningen af ITS, ved at de høres på et tilstrækkeligt tidligt stadium inden udviklingen af de relevante foranstaltninger.
26. EDPS noterer sig endvidere de ændringer, Europa-Parlamentet har vedtaget til artikel 6 i forslaget. EDPS bemærker først og fremmest, at den ændring, der tager sigte på at opfordre til at anvende anonyme oplysninger, hvor dette er muligt, ganske vist er meget velkommen i princippet, men at den ikke løser alle databeskyttelsesspørgsmålene, da mange af de oplysninger, der vil blive indsamlet og udvekslet gennem ITS, vil kunne betegnes som personoplysninger. For at der kan være tale om behandling af personoplysninger på anonymt grundlag, må det ikke være muligt for nogen person på noget stadium af behandlingen — i betragtning af alle de hjælpemidler, der med rimelighed kan tænkes bragt i anvendelse af den registeransvarlige eller af enhver anden person — at kæde oplysningerne sammen med oplysninger om en identificeret fysisk person, da sådanne oplysninger ellers betragtes som personoplysninger som defineret i artikel 2, litra a), i direktiv 95/46/EF<sup>(15)</sup>. På baggrund af de af Europa-Parlamentet foreslåede ændringer anbefaler EDPS, at artikel 6 i forslaget ændres således:

— Vurderingen af, om behandlingen af personoplysninger via ITS er nødvendig, bør foretages ud fra de legitime og specifikke formål, som behandlingen af oplysningerne tjener (i overensstemmelse med artikel 6 og 7 i

direktiv 95/46/EF). Afviklingen af ITS-applikationen<sup>(16)</sup> kan ikke i sig selv betragtes som et legitimt formål, der berettiger databehandling, da applikationen kun er et middel til at indsamle og udveksle oplysninger, hvis brug nødvendigvis skal have bestemte formål.

— Ændringen<sup>(17)</sup> om forbud mod brug af ITS-data og -registre »til andre formål end dem, der er nævnt i dette direktiv«, giver ikke tilstrækkelige garantier, navnlig fordi de specifikke formål og tjenester, som ITS vil blive brugt til, ikke er klart og udtømmende fastsat i direktivet. Da der vil blive udført forskellige databehandlingsaktiviteter via ITS til meget forskellige formål, bør det sikres, at de data, der indsamles i forbindelse med behandling til et bestemt formål, ikke bruges til andre formål, der er uforenelige, jf. artikel 6, stk. 1, litra b), i direktiv 95/46/EF. EDPS anbefaler derfor, at artikel 6, stk. 2, ændres yderligere for at sikre, at ITS-data og -registre ikke anvendes »til andre formål end dem, hvortil de blev indsamlet, på en måde, som er uforenelig med disse formål«.

### III. DATABESKYTTELSE I FORBINDELSE MED INTEL-LIGENTE TRANSPORTSYSTEMER

27. Det er særligt afgørende at præcisere de roller, der spilles af de forskellige ITS-aktører, så det fastsættes, hvem der får ansvaret for at sikre, at systemerne fungerer korrekt set ud fra et databeskyttelsessynspunkt. Det bør derfor afklares nærmere, hvem der bør være ansvarlig for at implementere de applikationer og systemer, som vil blive udformet efter udvalgsproceduren, og hvem i kæden af aktører der vil være ansvarlig for, at databehandlingen er i overensstemmelse med databeskyttelseslovgivningen (dvs. de registeransvarlige). EDPS vil i det følgende fremhæve nogle af de spørgsmål vedrørende beskyttelse af privatlivets fred og databeskyttelse, som udvalgsproceduren og de registeransvarlige bør tage hensyn til i forbindelse med udformningen af applikationerne og systemarkitekturen. Han vil endvidere pege på nogle af de databeskyttelsesspørgsmål i forbindelse med leveringen af ITS-tjenester, som lovgiveren og de registeransvarlige skal finde en løsning på.

#### III.1. »Privacy by design« (indbygget databeskyttelse)

28. Korrekt anvendelse af databeskyttelsesprincipperne i direktiv 95/46/EF er en central betingelse for en vellykket ibrugtagning af ITS i Fællesskabet. Disse principper har betydning for udformningen af systemarkitekturen og

<sup>(15)</sup> Det hedder således i betragtning 26 i direktiv 95/46/EF, at »for at afgøre, om en person er identificerbar, tages alle de hjælpemidler i betragtning, der med rimelighed kan tænkes bragt i anvendelse for at identificere den pågældende enten af den registeransvarlige eller af enhver anden person«.

<sup>(16)</sup> Ændring 34, der indfører et nyt stk. 1b i artikel 6, lyder således: »Personoplysninger behandles kun, hvis behandlingen er nødvendig til afvikling af ITS-applikationen og/eller -tjenesten.«

<sup>(17)</sup> Ændring 36 tilføjer følgende tekst i artikel 6, stk. 2: »og ikke anvendes til andre formål end dem, der er nævnt i dette direktiv«.

- applikationer. EDPS anbefaler, at »privacy by design«-tilgangen vedtages på et tidligt stadium af udformningen af ITS med det formål af definere arkitekturen, driften og styringen af applikationer og systemerne. Denne tilgang fremhæves navnlig i direktiv 1999/5/EF<sup>(18)</sup> for så vidt angår udformningen af radio- og teleterminaludstyr.
29. Udformningen af ITS-applikationer og -systemer vil komme til at foregå i flere etaper og vil blive udført af forskellige aktører, som alle bør tage hensyn til beskyttelse af privatlivets fred og databeskyttelse. Kommissionen og ITS-udvalget vil have det specifikke indledende ansvar for fastlæggelsen — efter udvalgsproceduren — af foranstaltninger, standardiseringsinitiativer, procedurer og bedste praksis, der bør fremme »privacy by design«.
30. Der bør tilskyndes til »privacy by design« på alle stadier af processerne og under alle former:
- På organisatorisk niveau bør der tages hensyn hertil i forbindelse med fastlæggelsen af de nødvendige procedurer for dataudveksling mellem alle relevante udvekslingspunkter — dette kan have direkte indvirkning på udvekslingstypen og på, hvilke data der udveksles.
  - Privatlivs- og sikkerhedskrav bør integreres i standarder, bedste praksis, tekniske specifikationer og systemer.
  - På teknisk niveau anbefaler EDPS, at der f.eks. efter udvalgsproceduren udvikles en bedste tilgængelig teknik<sup>(19)</sup> (BAT) for så vidt angår privatlivets fred, databeskyttelse og sikkerhed i bestemte sektorer og/eller til bestemte formål, med henblik på at definere de forskellige sikkerhedsparametre, der skal implementeres i hele systemets levetid, så der sikres overensstemmelse med EU's lovramme.
31. EDPS skitserer i det følgende nogle af de spørgsmål, som der specifikt skal findes en løsning på i forbindelse med udformningen af applikationer og systemarkitekturen. De vedrører de indsamlede data, systemernes interoperabilitet og datasikkerhed.
- III.1.a) *Dataminimering og anonymitet*
32. I overensstemmelse med artikel 6, stk. 1, litra c), i direktiv 95/46/EF må kun personoplysninger, der er nødvendige og relevante for specifikke formål, indsamles og behandles.
33. EDPS fremhæver betydningen af at foretage en passende klassificering af de oplysninger og data, der skal behandles inden for rammerne af ITS, før applikationer og systemerne udformes, således at man undgår en massiv og uhensigtsmæssig indsamling af personoplysninger. Der bør i den forbindelse tages hensyn til:
- datakilden (offentlig kilde, teleudbyder, ITS-tjenesteudbydere, andre operatører, køretøj, køretøjsbruger eller andre registrerede)
  - dataenes art (f.eks. aggregerede data, anonyme data, personoplysninger eller følsomme oplysninger)
  - det eller de formål, som dataene skal anvendes til, og
  - hvad angår samarbejdende systemer bør det gøres klart, hvilke data der hentes fra køretøjet ved push- eller pullteknologi og udveksles med andre køretøjer og/eller infrastrukturer og fra infrastruktur til infrastruktur og til hvilke formål.
34. De enkelte mekanismer bør analyseres nøje i forhold til de formål, der søges opfyldt, for at vurdere nødvendigheden af at indsamle personoplysninger. EDPS fremhæver betydningen af at finde den rette balance mellem de registreredes grundlæggende rettigheder og de forskellige involverede aktørers interesser, hvilket indebærer, at så få personoplysninger som muligt behandles. Applikationernes og systemernes arkitektur bør så vidt muligt udformes på en sådan måde, at det kun er de personoplysninger, der er strengt nødvendige til opfyldelse af formålene, der indsamles.
35. Hvis personoplysninger ikke er nødvendige eller kun er nødvendige på et tidligt tidspunkt af behandlingen, bør de ikke indsamles, eller de bør hurtigst muligt gøres anonyme. Det er derfor specielt vigtigt ikke kun at vurdere nødvendigheden af at indsamle data, men også nødvendigheden af at opbevare dem i de forskellige systemer. Der bør fastsættes specifikke frister for lagring af personoplysninger for alle de forskellige aktører i tjenstekæden, og disse bør variere alt efter, hvilken type data der er tale om, og til hvilket formål de blev indsamlet<sup>(20)</sup>. Når det ikke længere er nødvendigt at opbevare personoplysninger for at opfylde de formål, til hvilke de blev indsamlet eller viderebehandlet, bør de derfor gøres anonyme, dvs. ikke længere være relateret til en identificeret eller identificerbar fysisk person.
36. Udformningen af systemarkitekturen og dataudvekslingsprocedurerne bør understøtte behandlingen af så få personoplysninger som muligt. Der bør i den forbindelse tages hensyn til alle behandlingsstadierne og til alle aktørerne i ITS-tjenesteleveringskæden. Mens nogle oplysninger kan udveksles og behandles anonymt, kan andre oplysninger — også selv om de udveksles uidentificeret — kædes sammen med oplysninger om identificerede fysiske personer, hvorfor de betragtes som personoplysninger som

<sup>(18)</sup> Særlig artikel 3, stk. 3, litra c), i Europa-Parlamentets og Rådets direktiv 1999/5/EF af 9. marts 1999 om radio- og teleterminaludstyr samt gensidig anerkendelse af udstyrets overensstemmelse.

<sup>(19)</sup> Med den bedste tilgængelige teknik menes der det mest effektive og avancerede trin i udviklingen af aktiviteter og driftsmetoder, som er udtryk for en given tekniks principielle praktiske egnethed som grundlag for, at ITS-applikationer og -systemer overholder kravene vedrørende privatlivets fred, databeskyttelse og sikkerhed, der er fastlagt i EU's lovramme.

<sup>(20)</sup> F.eks. reguleres lagringen af trafikdata og lokaliseringsdata, der behandles i forbindelse med tilvejebringelsen af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet, ved Europa-Parlamentets og Rådets direktiv 2006/24/EF af 15. marts 2006 om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF.

defineret i artikel 2, litra a), i direktiv 95/46/EF<sup>(21)</sup>. I betragtning af de formål, som ITS vil blive brugt til, forekommer det vanskeligt at sikre, at et stort antal af de oplysninger, der indsamles via ITS, vil blive behandlet anonymt, idet de fysiske personers identitet vil være nødvendig på et eller andet tidspunkt til specifikke formål som f.eks. fakturering. Der vil derfor i det mindste skulle træffes særlige — tekniske, organisatoriske og lovgivningsmæssige — foranstaltninger til at sikre anonymitet på visse områder.

### III.1.b) Interoperabilitet, datakvalitet og formålsbegrænsning

37. Applikationernes og systemernes interoperabilitet er et centralt element i en vellykket ibrugtagning af ITS. Der vil blive udført harmoniseringsarbejde, hvor de tekniske specifikationer for de grænseflader, der skal integreres i applikationerne og systemerne, vil blive defineret, således at de bliver interoperable med andre applikationer, der er indbygget i andre transportmåder og/eller -systemer. Systemernes interoperabilitet vil ganske vist hjælpe med til at lette leveringen af en række tjenester og bidrage til at sikre deres kontinuitet i hele Europa, men indebærer samtidig en række risici fra et databeskyttelsessynspunkt som f.eks. risikoen for misbrug af data. Enhver sammenkobling af databaser bør foregå under behørig hensyntagen til databeskyttelsesprincipperne<sup>(22)</sup> og praktiske sikkerhedsgarantier (se også del III.1.c)).
38. Princippet om datakvalitet i artikel 6, stk. 1, litra d), i direktiv 95/46/EF er specielt afgørende i forbindelse med applikationernes og systemernes interoperabilitet. De tekniske specifikationer, der skal defineres for udformningen af grænsefladerne, bør sikre, at de data, der fremskaffes som følge af sammenkoblingen af applikationerne og systemerne, er korrekte.
39. Da systemernes interoperabilitet vil lette sammenkoblingen af databaser og matchningen af data til videre formål, understreger EDPS, at enhver sammenkobling bør foregå under nøje iagttagelse af formålsbegrænsningsprincippet i artikel 6, stk. 1, litra b), i direktiv 95/46/EF. Det er særligt vigtigt, at udformningen af ITS-systemarkitekturen hindrer enhver videre anvendelse af oplysningerne til andre formål end dem, hvortil de blev indsamlet. Der skal indbygges en passende sikkerhedsbeskyttelse i systemet for at hindre misbrug, ubeføjet udbredelse eller ikke-autoriseret adgang og sidevirkninger ved udstyret. F.eks. bør der iværksættes tilstrækkelig beskyttelse, således at ikke-autoriserede tredjeparter ikke får adgang til flytbart udstyr, og dette udstyr ikke bruges til at identificere og spore personer til andre formål end de med systemet tiltænkte.

<sup>(21)</sup> Se fodnote 15.

<sup>(22)</sup> Jf. også EDPS' bemærkninger til Kommissionens meddelelse om kompatibilitet mellem europæiske databaser, 10. marts 2006 [http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2006/06-03-10\\_Interoperability\\_EN.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2006/06-03-10_Interoperability_EN.pdf)

40. Hvad angår lovligheden af selve sammenkoblingen skal denne vurderes i hvert enkelt tilfælde under hensyn til arten af de oplysninger, der gøres tilgængelige og udveksles gennem systemerne, og de formål, som det oprindeligt var meningen, at de skulle anvendes til.

### III.1.c) Datasikkerhed

41. Personoplysningers sikkerhed er et centralt element i ibrugtagningen af ITS. EDPS hilser det velkommen, at sikkerhed udtrykkeligt nævnes i handlingsplanen og direktivforslaget. Der bør ikke blot sættes fokus på sikkerhed, så længe ITS-udstyret fungerer (i systemet i køretøjerne og i kommunikationstransportprotokollen), men også efterfølgende — i de databaser, hvor dataene behandles og/eller lagres. Der bør fastsættes passende tekniske, administrative og organisatoriske krav for alle stadier af behandlingen, som garanterer et passende sikkerhedsniveau i overensstemmelse med artikel 16 og 17 i direktiv 95/46/EF (samt artikel 4 og 5 i direktiv 2002/58/EF, hvor det er relevant).
42. Der bør først fastsættes passende sikkerhedsforanstaltninger, når der er foretaget en nøje vurdering af de specifikke formål, som ITS vil blive anvendt til, og af de nærmere regler for behandlingen. EDPS anbefaler i den forbindelse, at der foretages konsekvensanalyser for så vidt angår beskyttelse af privatlivets fred og databeskyttelse i relation til bestemte sektorer og/eller anvendelsesformål (f.eks. for sikkerhedsrelaterede ITS-systemer og for godsstyringssystemer). Udførelsen af en konsekvensanalyse for så vidt angår beskyttelse af privatlivets fred og databeskyttelse og brugen af BAT med henblik på denne beskyttelse vil bidrage til fastsættelsen af de mest hensigtsmæssige sikkerhedsforanstaltninger, der er relevante for den pågældende specifikke behandling.

### III.2. Yderligere databeskyttelses- og privatlivshensyn i forbindelse med leveringen af ITS-tjenester

43. Der er brug for yderligere EU-harmonisering af de nærmere regler for ibrugtagningen af ITS-tjenester for at hindre uoverensstemmelser i den forbindelse. EDPS ønsker her at fremhæve to spørgsmål, der især vil kræve nærmere overvejelser i henseende til beskyttelse af privatlivets fred og databeskyttelse:
- Brugen af lokaliseringværktøjer med henblik på levering af lokaliseringbaserede offentlige og kommercielle tjenester kræver, at der implementeres yderligere garantier. I den forbindelse bør der især lægges vægt på, om og hvornår ITS-lokaliseringbaserede tjenester anvendes til private formål eller erhvervsformål, og hvordan fysiske personer, der bruger et køretøj i erhvervsammenhæng, vil kunne blive berørt af anvendelsen af et sådant system.

- Det er særligt vigtigt i integrerede systemer, at det klart fremgår, hvilke roller og ansvarsområder de forskellige parter i ibrugtagningen af ITS har.

III.2.a) *Garantier i forbindelse med brugen af lokalisingsværktøjer med henblik på levering af ITS-lokalisingsbaserede tjenester*

44. Ibrugtagningen af ITS vil understøtte udviklingen af applikationer til »tracking and tracing« af gods og vil muliggøre udvikling af lokalisingsbaserede kommercielle og offentlige tjenester. Sådanne tjenester vil blive baseret på brugen af teknologier som satellitbaseret stedsbestemmelse og RFID-tags<sup>(23)</sup>. Det er meningen, at navigations- og »tracking and tracing«-systemer skal bruges til en lang række formål som f.eks. på afstand at følge køretøjer og laster undervejs (f.eks. ved transport af farligt gods eller levende dyr), fakturering af køretøjer baseret på en række parametre, herunder tilbagelagt afstand og tidspunkt på dagen (f.eks. vejafgifter og elektroniske bompengesystemer), overvågning af førere til håndhævelsesformål (f.eks. kontrol af køretider (ved hjælp af digitale fartskrivere)) og pålæggelse af sanktioner (ved elektronisk køretøjsidentifikation).
45. Brugen af lokaliseringsteknologier er specielt privatlivskrænkende, eftersom der bliver mulighed for at spore førere af køretøjer og for at indsamle en lang række data om deres kørevaner. Som det blev understreget af Artikel 29-Gruppen<sup>(24)</sup>, er behandlingen af lokaliseringsdata et særligt følsomt emne, der vedrører det afgørende spørgsmål om friheden til at bevæge sig anonymt, og som kræver, at der implementeres specifikke garantier for at hindre overvågning af fysiske personer og misbrug af data.
46. EDPS understreger, at brugen af lokalisingsværktøjer skal være lovlige, dvs. baseret på et hensigtsmæssigt retsgrundlag, have udtrykkeligt angivne og legitime formål og stå i forhold til de formål, der skal opfyldes. Lovligheden af databehandlingen vil for en stor dels vedkommende afhænge af, hvordan og til hvilke formål lokalisingsværktøjerne bruges. Som Artikel 29-Gruppen understregede i sin udtalelse om eCall, vil det »ud fra et databeskyttelsessynspunkt ikke [...] være acceptabelt, hvis sådanne apparater til stadighed er tilsluttet nettet, og køretøjet således løbende kan følges med henblik på en eventuel aktivering af eCall-systemet«<sup>(25)</sup>. Det er derfor vigtigt at afklare nærmere, under hvilke specifikke omstændigheder et køretøj vil blive sporet, og hvilken betydning det vil få for brugeren. Under alle omstændigheder bør brugen af

lokaliseringsapparater være begrundet i et legitimt behov (f.eks. overvågning af godstransport) og være strengt begrænset til, hvad der er nødvendigt til dette formål. Det er altså vigtigt at definere præcist, hvilke lokaliseringsdata der indsamles, hvor de lagres, og hvor længe de opbevares, samt med hvem og til hvilke formål de udveksles, og at tage alle nødvendige skridt til at undgå eventuelt misbrug af dataene.

47. Endvidere er behandlingen af lokaliseringsdata vedrørende brugere af offentlige kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester nøje reguleret i artikel 9 i direktiv 2002/58/EF. Det kræves navnlig, at lokaliseringsdata kun behandles, når de er gjort anonyme, eller når brugeren har givet sit informerede samtykke hertil. Dette betyder, at brugere, inden de giver deres samtykke til brugen af et lokalisingsværktøj, skal underrettes behørigt, bl.a. om, hvilken type lokaliseringsdata der behandles, og hvorfor og hvor længe de behandles, og om de videregives til en tredjemand med henblik på levering af tillægstjenesten. Brugeren skal have mulighed for ved hjælp af en simpel, gebyrfri anordning midlertidigt at forhindre behandling af lokaliseringsdata ved hvert enkelt opkald til nettet eller ved hver enkelt fremføring af kommunikation. Behandlingen af lokaliseringsdata bør være strengt begrænset til personer, som handler efter bemyndigelse fra udbyderen af det offentlige kommunikationsnetværk eller den offentligt tilgængelige kommunikationstjeneste eller fra den tredjemand, som leverer tillægstjenesten.
48. Der skal vedtages yderligere garantier, når lokaliseringsdata indsamles fra køretøjer, der bruges i erhvervsøjemed, for at forhindre, at positionsteknologi bruges til ubehørig overvågning af de ansatte. Under alle omstændigheder bør behandlingen være begrænset til lokaliseringsdata, der indsamles i arbejdstiden — ansatte skal således kunne slå lokaliseringsfunktionen fra uden for arbejdstid, og/eller når køretøjet bruges til private formål.
49. Der er en risiko for, at tredjeparter (såsom forsikringselskaber, arbejdsgivere og retshåndhavende myndigheder) kræver adgang til de data, der er indsamlet ved hjælp af navigations- og sporingssystemer til bestemte legitime formål (som f.eks. sporing af varer og elektronisk betaling af vejafgifter), for at bruge dem til sekundære formål, bl.a. kontrol af køre- og hviletider eller af overholdelsen af færdselsreglerne og pålæggelse af sanktioner. Adgang til data til sekundære formål er i princippet ikke tilladt, hvis denne adgang tjener formål, der er uforenelige med de formål, til hvilke de blev indsamlet. Der kan kun tillades adgang som undtagelse fra dette princip, hvis betingelserne for sådan adgang opfylder de strenge krav, der er fastsat i

<sup>(23)</sup> Se de spørgsmål vedrørende beskyttelse af privatlivets fred og databeskyttelse, som bruges af RFID rejser, i udtalelsen fra den europæiske tilsynsførende for databeskyttelse om meddelelsen fra Kommissionen til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget om radiofrekvensbaseret identifikation (RFID) i Europa: elementer til en politisk ramme KOM(2007) 96 (EUT C 101 af 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> Artikel 29-Gruppen, udtalelse om brug af lokaliseringsdata med henblik på at yde tillægstjenester, WP 115, november 2005. [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/2005/wp115\\_da.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_da.pdf)

<sup>(25)</sup> Se WP 125 om eCall, s. 5, som nævnt i fodnote 10.



artikel 13 i direktiv 95/46/EF. Som følge heraf bør tredje-parter kun gives adgang til lokaliseringsdata i overensstemmelse med loven og på en gennemsigtig måde og på grundlag af en lovgivningsmæssig foranstaltning, der omhandler passende procedurer og regler for adgang til dataene til specifikke formål og indeholder tilstrækkelige garantier for fysiske personer, når det gælder de videre formål, som deres oplysninger måtte blive brugt til.

### III.2.b) ITS-aktørers roller og ansvar

50. Det er endnu ikke klart, hvem den registeransvarlige bliver for hver del af behandlingen. I mange tilfælde vil ITS-tjenestudbyderne sandsynligvis være de registeransvarlige, enten alene, når det drejer sig om personoplysninger, der behandles med henblik på levering af deres egne ITS-tjenester, eller i fællesskab, når behandlingen foregår sammen med andre registeransvarlige. Operatører, der er involveret i ITS i forskellige kapaciteter, bør have deres rolle og ansvar som registeransvarlige og registerførere klart defineret for hver enkelt del af behandlingen (f.eks. teleoperatører, der leverer kommunikationstjenester såvel som ITS-tjenester).
51. De personer, der fungerer som registeransvarlige, vil have ansvaret <sup>(26)</sup> for at sikre, at systemerne og tjenesterne overholder alle databeskyttelseskravene, og især for at implementere »privacy by design«-systemer, der opfylder principperne om datakvalitet og formålsbegrænsning og garanterer et passende datasikkerhedsniveau som beskrevet i punkt III.1.
52. Registeransvarlige vil skulle sikre, at der er passende garantier på plads i alle led af kæden af aktører, der er involveret i ibrugtagningen af ITS. Dette vil navnlig kræve, at de med alle de interessenter, der er involveret i dataudvekslingen og -behandlingen, indgår kontraktordninger, som giver tilstrækkelige databeskyttelsesgarantier (især for så vidt angår artikel 16 og 17 i direktiv 95/46/EF og artikel 4 og 5 i direktiv 2002/58/EF). Det er vigtigt at bemærke, at mens registeransvarlige skal sørge for, at databeskyttelsen sikres på alle stadier af behandlingen, forbliver de ud fra et databeskyttelsessynspunkt ansvarlige for behandlingen og kan ikke fralægge sig deres ansvar ved kontrakt.

## IV. KONKLUSIONER

53. EDPS hilser den af Kommissionen foreslåede plan for udbygning af ITS velkommen, som tager sigte på at harmonisere dataprocesser i hele Europa for at lette leveringen af ITS-tjenester, og som opstiller databeskyttelse som en central betingelse for korrekt ibrugtagning af ITS i Europa.
54. EDPS bemærker, at det foreslåede direktiv fastsætter generelle rammer, som rejser en række spørgsmål i relation til beskyttelse af privatlivets fred og databeskyttelse, som skal behandles nærmere på EU-niveau og på nationalt plan:

- Der er en risiko for, at manglen på klarhed i det foreslåede regelsæt vil føre til uensartet gennemførelse af ITS i Europa og dermed resultere i forskellige databeskyttelsesniveauer i Europa. EDPS understreger, at der er behov for yderligere EU-harmonisering på disse områder for at afklare udestående spørgsmål (som f.eks. fastlæggelsen af ITS-aktørers roller og ansvar, de specifikke ITS-applikationer og -systemer, der skal indbygges i køretøjer, udarbejdelsen af harmoniserede kontrakter med henblik på levering af ITS-tjenester og de specifikke formål og nærmere regler for brugen af ITS). Det er specielt vigtigt at fastsætte, hvem der bliver de registeransvarlige for så vidt angår den databehandling, der skal udføres, da de får ansvaret for at sikre, at der tages hensyn til beskyttelse af privatlivets fred og databeskyttelse i alle behandlingskædens led.
- Beslutninger vedrørende bestemte regler for behandling, der vil kunne få alvorlige virkninger for fysiske personers ret til beskyttelse af privatlivets fred og databeskyttelse, bør træffes af Europa-Parlamentet og Rådet og ikke efter en udvalgsprocedure.
- Det er af altafgørende betydning, at der tages hensyn til beskyttelse af privatlivets fred og databeskyttelse på et tidligt stadium af behandlingen og derefter på alle stadier af behandlingen; der bør tilskyndes til at anvende »privacy by design«-tilgangen i forbindelse med udformningen af ITS-applikationer og -systemer, og den bør indarbejdes i standarder, bedste praksis, tekniske specifikationer og systemer.
- Enhver sammenkobling af applikationer og systemer bør foregå under behørig hensyntagen til databeskyttelsesprincipperne og praktiske sikkerhedsgarantier.
- Hvad angår de usikkerhedsmomenter, der fortsat består på nuværende tidspunkt med hensyn til reglerne for ibrugtagning af ITS, hilser EDPS det specielt velkommen, at Kommissionen i sin meddelelse har taget initiativ til, at der foretages en vurdering af beskyttelsen af privatlivets fred senest i 2011. Han råder desuden kraftigt til, at der foretages konsekvensanalyser for så vidt angår beskyttelse af privatlivets fred og databeskyttelse i relation til bestemte sektorer og/eller anvendelsesformål med henblik på fastsættelsen af passende sikkerhedsforanstaltninger, og at der udvikles en bedste tilgængelig teknik for beskyttelse af privatlivets fred, databeskyttelse og sikkerhed i ITS.
- EDPS understreger endvidere, at medlemsstaterne har ansvaret for at gennemføre direktivet korrekt, således at ITS-operatørerne kan implementere systemer og tjenester, der giver et passende databeskyttelsesniveau i hele Europa.

<sup>(26)</sup> Se fodnote 13.

- Registeransvarlige, der leverer ITS-tjenester, bør iværksætte passende garantier, således at brugen af lokaliserings teknologi som f.eks. satellitbaseret stedsbestemmelse og RFID-tags ikke bliver privatlivskrænkende for fysiske personer, der bruger køretøjer til rent privat brug eller i erhvervssammenhæng. Dette vil navnlig kræve, at databehandlingen begrænses til, hvad der er strengt nødvendigt til et bestemt formål, at det sikres, at der indbygges passende sikkerhedsforanstaltninger i systemerne, således at lokaliseringsdata ikke videregives til ikke-autoriserede modtagere, og at brugere får en effektiv metode til at deaktivere lokaliseringsudstyr og/eller -mekanismer.
55. EDPS anbefaler, at artikel 6 i forslaget ændres som følger i overensstemmelse med direktiv 95/46/EF:
- Der bør tilskyndes til dataminimering, når det gælder ITS-databehandling. Det anbefales på den baggrund at ændre artikel 6, stk. 1b, i forslaget således: »Personoplysninger behandles kun, hvis behandlingen er nødvendig til det specifikke formål, som ITS bruges til, og er baseret på et passende retsgrundlag.«
- Det er vigtigt, at personoplysninger, der behandles i interoperable systemer, ikke bruges til videre formål, som er uforenelige med de formål, hvortil de blev indsamlet. Det anbefales derfor at ændre artikel 6, stk. 2, således: »og ikke anvendes til andre formål end dem, hvortil de blev indsamlet, på en måde, som er uforenelig med disse formål«.
- Han anbefaler, at der i artikel 6 i forslaget tilføjes en udtrykkelig henvisning til begrebet »privacy by design« i forbindelse med udformningen af ITS-applikationer og -systemer. Han anbefaler også, at Artikel 29-Gruppen og EDPS informeres og høres om yderligere foranstaltninger, der træffes på dette område efter udvalgsproceduren.
56. EDPS anbefaler endvidere, at der henvises til denne høring i forslagens betragtninger.
57. I betragtning af ovenstående anbefaler EDPS, at databeskyttelsesmyndighederne, navnlig gennem Artikel 29-Gruppen, og EDPS involveres tæt i initiativer vedrørende udbygning og ibrugtagning af ITS, ved at de høres på et tilstrækkeligt tidligt stadium inden udviklingen af de relevante foranstaltninger.

Udfærdiget i Bruxelles, den 22. juli 2009.

Peter HUSTINX

*Den Europæiske Tilsynsførende for Databeskyttelse*