

EUROPEISKA DATATILLSYNSMANNEN

Yttrande från Europeiska datatillsynsmannen om kommissionens meddelande handlingsplan för införande av intelligenta transportsystem i EU och det åtföljande förslaget till Europaparlamentets och rådets direktiv om en ram för införande av intelligenta transportsystem på vägtransportområdet och för gränssnitt mot andra transportsätt

(2010/C 47/02)

EUROPEISKA DATATILLSYNSMANNEN HAR ANTAGIT DETTA YTTRANDE

med beaktande av fördraget om upprättandet av Europeiska gemenskapen, särskilt artikel 286,

med beaktande av Europeiska unionens stadga om de grundläggande rättigheterna, särskilt artikel 8,

med beaktande av Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter,

med beaktande av Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation,

med beaktande av Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter, särskilt artikel 41, och

med beaktande av den begäran om ett yttrande i enlighet med artikel 28.2 i förordning (EG) nr 45/2001 som datatillsynsmannen den 11 februari 2009 mottog från Europeiska kommissionen.

HÄRIGENOM FRAMFÖRS FÖLJANDE.

I. INLEDNING

1. Den 16 december 2008 antog kommissionen ett meddelande där man fastställde en handlingsplan för införande av

intelligenta transportsystem i EU (nedan kallad *meddelandet*)⁽¹⁾. Meddelandet åtföljs av ett förslag till Europaparlamentets och rådets direktiv om en ram för införande av intelligenta transportsystem på vägtransportområdet och för gränssnitt mot andra transportsätt (nedan kallat *förslaget*)⁽²⁾. Kommissionen översände meddelandet och det åtföljande förslaget till Europeiska datatillsynsmannen för samråd i enlighet med artikel 28.2 i förordning (EG) nr 45/2001⁽³⁾.

2. Datatillsynsmannen välkomnar att samråd hålls och rekommenderar att det hänvisas till detta samråd i skälen till förslaget, på samma sätt som i ett antal andra lagstiftningstexter där samråd har hållits med datatillsynsmannen i enlighet med förordning (EG) nr 45/2001.

I.1 Kommissionens meddelande om en handlingsplan för införande av intelligenta transportsystem i EU

3. Intelligenta transportsystem (ITS) är avancerade tillämpningar för användning av informations- och kommunikationsteknik som finns inbyggd i olika transportsätt för samverkan dem emellan. På vägtransportområdet kommer ITS att tillhandahålla innovativa tjänster vad gäller transportsätt och trafikledning för olika användare, t.ex. resenärer, infrastrukturanvändare och infrastrukturoperatörer, vagnparksansvariga och larmtjänstoperatörer.

4. Efter en inventering av det ökande införandet av ITS i olika transportsätt i Europeiska unionen⁽⁴⁾ har kommissionen antagit en handlingsplan för att påskynda införandet och

⁽¹⁾ KOM(2008) 886 slutlig. Rådet antog slutsatser om meddelandet vid 2935:e mötet i rådet (transport, telekommunikation och energi) den 30–31 mars 2009.

⁽²⁾ KOM(2008) 887 slutlig.

⁽³⁾ Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter (EGT L 8, 12.01.2001, s. 1).

⁽⁴⁾ På EU-nivå finns många initiativ där ITS integreras i olika transportsätt, bl.a. lufttransporter (Sesar), vattenvägar (RIS), järnväg (ERTMS, TAF-TSI), sjöfart (VTMIS, AIS, LRIT) och vägtransporter (eToll, eCall), se KOM(2008) 886 slutlig, s. 3.

användandet av ITS-tillämpningar och ITS-tjänster på vägtransportområdet. Handlingsplanen syftar också till att säkerställa samverkan med andra transportsätt, vilket kommer att underlätta tillhandahållandet av multimodala tjänster. Ett konsekvent införande av ITS i EU kommer att gagna olika gemenskapsmål, bl.a. transporteffektivitet, hållbarhet och säkerhet, och främja EU:s inre marknad och konkurrenskraft. Med tanke på de många olika målen för ITS-införandet föreslås i meddelandet sex prioriterade åtgärdsområden för perioden 2009–2014. För genomförandet av planen föreslår kommissionen att det på EU-nivå fastställs en rättslig ram i form av ett direktiv, där ett antal åtgärder på utvalda prioriterade områden fastställs.

1.2 Förslag till direktiv om en ram för införande av intelligenta transportsystem på vägtransportområdet och för gränssnitt mot andra transportsätt

- I förslaget föreskrivs en ram för det transnationella införandet av ITS-tillämpningar i syfte att underlätta tillhandahållandet av harmoniserade gränsöverskridande tjänster, framför allt för trafik- och reseinformation och trafikledning. Enligt förslaget ska medlemsstaterna vidta flera tekniska åtgärder för att underlätta utbyte av uppgifter mellan användare, myndigheter, berörda intressenter och leverantörer av ITS-tjänster samt för att integrera säkerhets- och skyddsrelaterade ITS-system i fordon och väginfrastrukturer. Tekniska specifikationer för ITS-tillämpningar och system på fyra av de prioriterade områdena⁽⁵⁾ i handlingsplanen kommer att fastställas genom ett kommittéförfarande⁽⁶⁾, och de centrala aspekterna för dessa anges i bilaga II. Det framgår emellertid inte tydligt för vilka särskilda ändamål ITS kommer att användas på dessa områden. Dessutom kan införandet av ITS utvidgas till många fler områden än de fyra som ursprungligen valts ut för utvecklingen av harmoniserade tekniska specifikationer. Förslaget gäller huvudsakligen införandet av framtida tillämpningar och tjänster på ITS-området, men det ska också, där så är möjligt, omfatta teknik på detta område som redan finns eller är under utveckling (såsom eCall, eToll etc.).

- Förslaget översändes till Europaparlamentet, som antog sin ståndpunkt vid första behandlingen⁽⁷⁾ den 23 april 2009. Efter en begäran om samråd från rådet den 29 januari

⁽⁵⁾ Enligt artikel 4 i förslaget ska specifikationer för tekniska åtgärder införas på följande områden: i) optimal användning av väg-, trafik- och reseuppgifter, ii) kontinuitet i ITS-tjänster för trafikledning och godshantering i europeiska transportkorridorer och tätortsområden, iii) trafiksäkerhet och transportskydd samt iv) integration av fordon i transportinfrastrukturen.

⁽⁶⁾ Enligt förslaget ska ett föreskrivande förfarande med kontroll tillämpas, i enlighet med artikel 5a.1–4 och artikel 7 i beslut 1999/468/EG.

⁽⁷⁾ Europaparlamentets lagstiftningsresolution av den 23 april 2009 om förslaget till Europaparlamentets och rådets direktiv om en ram för införande av intelligenta transportsystem på vägtransportområdet och för gränssnitt mot andra transportsätt, T6-0283/2009.

2009 antog Europeiska ekonomiska och sociala kommittén ett yttrande om förslaget den 13 maj 2009⁽⁸⁾.

1.3 Yttrandets huvudsakliga inriktning

- Datatillsynsmanen välkomnar samrådet om den plan för införande av ITS som kommissionen lagt fram. Detta är inte första gången som datatillsynsmanen behandlar frågorna i ITS-handlingsplanen. Datatillsynsmanen yttrade sig över kommissionens förslag om att underlätta gränsöverskridande uppföljning av trafikförseelser⁽⁹⁾ och bidrog till arbetet i artikel 29-gruppen med ett arbetsdokument om eCall⁽¹⁰⁾.
- Grunden för intelligenta transportsystem är insamling, behandling och utbyte av många olika uppgifter, från offentliga och privata källor. Detta är därför ett dataintensivt område. Införandet av ITS kommer i stor utsträckning att bygga på teknik för geolokalisering, t.ex. satellitbaserad positionsbestämning och kontaktlös teknik såsom radiofrekvensidentifiering, som kommer att göra det enklare att tillhandahålla en mängd olika offentliga och/eller kommersiella platsbaserade tjänster (t.ex. trafikinformation i realtid, e-transport, eCall, eToll, parkeringsbokning etc.). Vissa av de uppgifter som kommer att behandlas i ITS har sammanställts – t.ex. uppgifter om trafik, olyckor och olika möjligheter – och avser inte enskilda individer, medan andra uppgifter avser identifierade eller identifierbara enskilda individer och uppfyller därför villkoren för personuppgifter enligt artikel 2 a i direktiv 95/46/EG.
- Europeiska datatillsynsmanen anser att det är av avgörande betydelse att de åtgärder som planeras för införande av intelligenta transportsystem är förenliga med den befintliga lagstiftning som anges i förslaget, särskilt direktiv 95/46/EG om skydd av personuppgifter⁽¹¹⁾ och direktiv 2002/58/EG om integritet och elektronisk kommunikation⁽¹²⁾.

⁽⁸⁾ Yttrande från Europeiska ekonomiska och sociala kommittén om Förslag till Europaparlamentets och rådets direktiv om en ram för införande av intelligenta transportsystem på vägtransportområdet och för gränssnitt mot andra transportsätt, TEN/382, den 13 maj 2009.

⁽⁹⁾ Yttrande från Europeiska datatillsynsmanen om förslaget till Europaparlamentets och rådets direktiv om gränsöverskridande uppföljning av trafikförseelser 2008/C 310/02, EUT C 310, 5.12.2008, s. 9.

⁽¹⁰⁾ Artikel 29-gruppens arbetsdokument om dataskydd och personlig integritet i samband med eCall-initiativet, WP 125, 26 september 2006 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp125_sv.pdf

⁽¹¹⁾ Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter, EGT L 281, 23.11.1995, s. 31.

⁽¹²⁾ Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation), EGT L 201, 31.7.2002, s. 37.

10. Olösta frågor om integritet och skydd av uppgifter är enligt kommissionen ett av de största hindren för att främja intelligenta transportsystem. Dessa frågor kommer att tas upp på följande sätt i detta yttrande:

— I kapitel II görs en analys av den rättsliga ram som kommissionen föreslår för införandet av intelligenta transportsystem, utifrån ett uppgiftsskyddsperspektiv.

— I kapitel III belyses de frågor om uppgiftsskydd som måste behandlas för att intelligenta transportsystem ska kunna införas på ett riktigt sätt.

— o I ett första avsnitt betonas i yttrandet behovet av inbyggda skyddsmekanismer för att skydda den personliga integriteten ("privacy by design") i utvecklingen av ITS samt de viktiga frågor som måste tas upp vid utformningen av ITS-tillämpningar och system för behandling av uppgifter.

— o Det andra avsnittet fokuserar på några av de överväganden avseende integritet som måste göras när det gäller tillhandahållande av ITS-tjänster.

II. ANALYS AV DEN RÄTTLIGA RAM SOM FÖRESLÅS FÖR INFÖRANDET AV ITS

11. Kommissionens förslag till direktiv innehåller två bestämmelser (skäl 9 och artikel 6) om personlig integritet, säkerhet och återanvändning av information. I artikel 6.1 i kommissionens förslag krävs att tillämpningen av ITS sker i enlighet med reglerna för skydd av personuppgifter i bl.a. direktiven 95/46/EG och 2002/58/EG. I artikel 6.2 i kommissionens förslag anges konkreta säkerhetsåtgärder till skydd för personuppgifter. Där föreskrivs det att "medlemsstaterna särskilt ska se till att ITS-data och register skyddas mot missbruk, inklusive olaglig åtkomst, ändring eller förlust". Slutligen anges i artikel 6.3 i kommissionens förslag att "direktiv 2003/98/EG ska tillämpas".

12. Europaparlamentet föreslog vid första behandlingen ändringar av artikel 6. Framför allt har tre nya punkter lagts till i artikel 6.1, som gäller användande av anonyma uppgifter då detta är möjligt, behandling av känsliga uppgifter endast efter informerat medgivande från den registrerade, och säkerställande av att personuppgifter "endast behandlas

i de fall då detta är nödvändigt för användandet av ITS-tillämpningar och/eller tjänster". Dessutom har artikel 6.2 ändrats genom tillägget att ITS-data och register "inte får användas för andra ändamål än de som nämns i detta direktiv".

13. Datatillsynsmannen hälsar med tillfredsställelse att uppgiftsskyddet har beaktats vid utarbetandet av förslaget och att det förs fram som ett allmänt villkor för att intelligenta transportsystem ska kunna införas på ett riktigt sätt i EU. Datatillsynsmannen är medveten om behovet av en sammanhållen harmonisering av processer för uppgiftshantering på EU-nivå för att säkerställa att ITS-tillämpningar och ITS-tjänster fungerar i hela Europa.

14. Datatillsynsmannen noterar dock att den föreslagna rättsliga ramen är alltför vid och allmän för att på ett tillfredsställande sätt bemöta farhågorna i samband med integritet och uppgiftsskydd vid införande av intelligenta transportsystem i medlemsstaterna. Det framgår inte när användandet av ITS-tjänster kommer att leda till insamling och behandling av personuppgifter, för vilka särskilda syften behandling av uppgifter sker eller vilken rättslig grund som motiverar sådan behandling. Vidare innebär användandet av lokaliseringsteknik i samband med ITS en risk för att tjänster utvecklas som inkräktar på privatlivet om de medför insamling och behandling av personuppgifter. I förslaget anges inte heller tydligt vilka roller och vilket ansvar som de olika operatörerna vid införandet av ITS har, och det är följaktligen svårt att veta vilka operatörer som kommer att vara registeransvariga och därmed ansvariga⁽¹³⁾ för att skyldigheterna i fråga om uppgiftsskydd uppfylls. ITS-operatörer kommer att ställas inför betydande problem om inte alla dessa frågor klargörs i lagstiftningen, eftersom det är de som i slutändan kommer att ha ansvaret för att tillämpa åtgärderna i det föreslagna direktivet.

15. Det finns därför en risk för att bristen på tydlighet i den föreslagna rättsliga ramen kommer att skapa skiljaktigheter vid införandet av ITS i Europa och att detta i stället för att minska skillnaderna mellan medlemsstaterna kommer att leda till en stor osäkerhet, splittring och bristande överensstämmelse, på grund av olika nivåer av uppgiftsskydd i Europa. Detta kan också leda till bristande efterlevnad av grundläggande åtgärder för uppgiftsskydd. Datatillsynsmannen betonar behovet av ytterligare harmonisering i dessa frågor på EU-nivå. Datatillsynsmannen föreslår därför förändringar av den föreslagna rättsliga ramen ur uppgiftsskyddssynpunkt. Datatillsynsmannen rekommenderar starkt att parlamentet och rådet i förslaget inför de föreslagna förändringarna och, där så är möjligt, ytterligare bestämmelser för att förtydliga olösta frågor (t.ex. definitioner av och ansvar för ITS-operatörer, utveckling av harmoniserade avtal för tillhandahållande av ITS-tjänster etc.).

⁽¹³⁾ Enligt artiklarna 2 d, 6.2 och 23 i direktiv 95/46/EG, som nämns i fotnot 11.

Vidare betonar datatillsynsmannen att medlemsstaterna också kommer att vara ansvariga för att genomföra direktivet på ett riktigt sätt, så att operatörer kan utveckla system och tjänster med en lämplig nivå av uppgiftsskydd i hela Europa.

II.1 Behandling av uppgifter måste bygga på en lämplig rättslig grund

16. Det framgår inte tydligt när behandling av personuppgifter börjar då ITS-utrustningen redan finns integrerad i ett fordon och på vilka rättsliga grunder som behandlingen sker. Operatörerna kan åberopa olika rättsliga grunder för behandlingen av uppgifter, bl.a. otvetydigt samtycke från användare eller ett avtal eller en rättslig förpliktelse som den registeransvarige ska fullgöra. Det finns ett behov av att harmonisera den rättsliga grunden för behandlingen av uppgifter i ITS för att säkerställa att systemen fungerar i hela Europa och att användare inte blir lidande av att man behandlar uppgifter olika i olika EU-länder.
17. I ett antal fall kommer ITS-system att som standard integreras i fordon. Så är det bland annat med säkerhets- och skyddsrelaterade ITS-system, som enligt förslaget måste finnas inbyggda i fordon. I förslaget definieras dock inte "säkerhets- och skyddsrelaterade ITS-system", och det bör därför förtydligas vilka särskilda ITS-tillämpningar och system som måste finnas inbyggda i fordon. Vidare bör det framgå huruvida aktivering och användning av anordningen kommer att vara frivillig eller obligatorisk för användare. Obligatorisk uppgiftsbehandling bör endast ske för särskilda ändamål med hänsyn till tvingande skäl (t.ex. spårning av gods vid godshantering) och med lämpliga skyddsåtgärder vid behandlingen av uppgifter som rör enskilda individer. Om användningen av ITS sker på frivillig grund bör lämpliga skyddsåtgärder vidtas för att förhindra att användarna ska anses ha samtyckt underförstått till att använda systemet enbart på grund av att det finns i fordonet.
18. Datatillsynsmannen förordar att ITS-tjänster tillhandahålls på frivillig basis. Detta innebär att användarna måste kunna välja fritt om de samtycker till att använda systemet och till de särskilda ändamål som det kommer att användas för. Då den tjänst som tillhandahålls bygger på lokalisering-uppgifter måste användaren få lämplig information (i enlighet med framför allt artikel 9 i direktiv 2002/58/EG) och kunna dra tillbaka sitt samtycke. Rent konkret krävs för detta att det införs ett enkelt sätt att avaktivera anordningen och/eller funktionen⁽¹⁴⁾, utan några tekniska eller ekonomiska följder, när användaren inte längre samtycker till användningen av systemet och/eller en särskild funktion. Ytterligare skyddsåtgärder bör vidtas så att användare inte diskrimineras när de vägrar att använda en tjänst.
19. I fall då viss behandling är obligatorisk medan annan behandling kräver användarens samtycke måste insyn garanteras i fråga om de olika typer av uppgiftsbehandling som

sker, genom lämplig information till användarna om omfattningen av varje specifik behandling och huruvida den är obligatorisk och/eller frivillig. Dessutom kommer lämpliga säkerhetsåtgärder att krävas så att uppgifter inte samlas in eller behandlas utöver vad som är lagstadgat och/eller föremål för samtycke.

20. Med tanke på de transnationella effekterna av ITS-tjänster rekommenderar datatillsynsmannen också att alleuropeiska standardkontrakt utarbetas för att säkerställa att tjänster som tillhandahålls via ITS erbjuder samma uppgiftsskydd i hela Europa, särskilt att informationen till användarna är tillräckligt tydlig i fråga om vilka särskilda funktioner som används samt effekterna för uppgiftsskyddet av användandet av särskild teknik och hur användarna kan utöva sina rättigheter. När nya funktioner läggs till bör ytterligare åtgärder vidtas av tjänsteleverantörerna för att ge användarna tydlig och specifik information om dessa tilläggsfunktioner och för att vid behov erhålla användarnas samtycke till att dessa nya funktioner används.

II.2 Syftet med och formerna för behandling av uppgifterna måste preciseras ytterligare

21. Datatillsynsmannen noterar att det inte preciseras i förslaget för vilka särskilda tjänster och ändamål som ITS-tillämpningar kan användas, vilket följaktligen lämnas öppet. Detta möjliggör i praktiken flexibilitet, men det innebär att olösta frågor om integritet och uppgiftsskydd – enligt kommissionen ett av de största hindren för att främja intelligenta transportsystem (se punkt 10) – inte löses och kan hindra att de föreslagna åtgärderna genomförs på ett välavvägt sätt.
22. Datatillsynsmannen betonar vikten av att behandlingen av uppgifter för tillhandahållande av särskilda ITS-tjänster sker i enlighet med en lämplig rättslig grund och dessutom för särskilda, uttryckligt angivna och berättigade ändamål, samt att den planerade behandlingen är proportionerlig till och nödvändig för dessa ändamål (artikel 6 i direktiv 95/46/EG). Man bör därför överväga om det finns behov av ytterligare lagstiftning på EU-nivå om särskild användning av ITS för att skapa en harmoniserad och ändamålsenlig rättslig grund för behandling av uppgifter samt för att undvika skillnader mellan medlemsstaterna vid införandet av ITS-tjänster.
23. I den föreslagna ramen finns ännu inte något beslut om formerna för behandling och utbyte av uppgifter vid användning av ITS. Många tekniska parametrar kommer att bli föremål för beslut först i ett senare skede, genom kommittéförfarandet, och valet av dessa kommer att få olika konsekvenser för integritet och uppgiftsskydd. Med hänsyn

⁽¹⁴⁾ Se WP 125 om eCall s. 4, nämnt i fotnot 10.

till det särskilda skyddet för privatlivet och för uppgifter som skyddade grundläggande rättigheter enligt artikel 8 i den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna samt enligt artiklarna 7–8 i Europeiska unionens stadga om de grundläggande rättigheterna kan det ifrågasättas om och i vilken utsträckning definitioner av behandling av uppgifter bör beslutas genom ett kommittéförfarande.

24. I ett demokratiskt samhälle bör beslut om grundläggande principer och metoder som påverkar grundläggande rättigheter fattas inom ramen för ett fullständigt lagstiftningsförfarande som inbegriper lämpliga kontroller och avvägningar. I detta fall innebär det att beslut som får avgörande konsekvenser för enskilda individers integritet och uppgiftsskydd, såsom ändamål och former för obligatorisk uppgiftsbehandling och definitioner av formerna för införandet av ITS på nya områden, bör beslutas av Europaparlamentet och rådet och inte genom ett kommittéförfarande.
25. Utifrån detta förordar datatillsynsmannen starkt att artikel 29-gruppen och datatillsynsmannen där så är relevant deltar i arbetet i den kommitté som inrättats enligt artikel 8 i förslaget och i framtida åtgärder som rör införandet av ITS, genom samråd i ett tillräckligt tidigt skede innan sådana åtgärder utarbetas.
26. Vidare noterar datatillsynsmannen de ändringar som Europaparlamentet antagit när det gäller artikel 6 i förslaget. Först och främst noterar datatillsynsmannen att den ändring där användandet av anonyma uppgifter då detta är möjligt uppmuntras, trots att den i princip är välkommen, inte kommer att lösa alla problem med uppgiftsskydd eftersom många uppgifter som samlas in och utbyts genom ITS kan uppfylla villkoren för personuppgifter. För att behandlingen av personuppgifter ska ske anonymt får det inte vara möjligt för någon att i något skede av behandlingen – med hänsyn till alla medel som rimligen kan komma att användas antingen av den registeransvarige eller av någon annan person – kunna koppla ihop uppgifterna med uppgifter som berör en identifierad enskild individ, om inte sådana uppgifter utgör personuppgifter enligt artikel 2 a i direktiv 95/46/EG⁽¹⁵⁾. Vidare rekommenderar datatillsynsmannen på grundval av de ändringar som Europaparlamentet föreslagit att artikel 6 i förslaget ändras på följande sätt:

- Bedömningen av om det är nödvändigt att behandla personuppgifter i ITS bör göras mot bakgrund av de berättigade och särskilda ändamål för vilka uppgifterna behandlas (i enlighet med artiklarna 6–7 i direktiv

95/46/EG). Användande av ITS-tillämpningen⁽¹⁶⁾ kan inte i sig vara ett berättigat ändamål som motiverar uppgiftsbehandling, eftersom tillämpningen bara är ett hjälpmedel för att samla in och utbyta uppgifter och användandet av den bör inriktas mot särskilda ändamål.

- Den ändring⁽¹⁷⁾ som rör förbud mot användande av ITS-uppgifter och register "för andra ändamål än de som nämns i detta direktiv" innebär inte tillräckliga garantier, i synnerhet som de särskilda ändamål och tjänster som ITS kommer att användas för inte anges tydligt och fullständigt i direktivet. Med tanke på att olika typer av uppgiftsbehandling kommer att ske genom ITS för helt olika ändamål bör det säkerställas att uppgifter som samlas in under behandling för ett visst ändamål inte används för andra ändamål som är oförenliga med detta så som det föreskrivs i artikel 6.1 b i direktiv 95/46/EG. Datatillsynsmannen rekommenderar därför att artikel 6.2 ändras ytterligare för att säkerställa att ITS-uppgifter och register inte används för andra ändamål än de för vilka de samlades in och på ett sätt som är oförenligt med dessa ändamål.

III. UPPGIFTSSKYDD I INTELLIGENTA TRANSPORTSYSTEM

27. Det är särskilt viktigt att klargöra rollerna för olika aktörer i ITS för att identifiera vem som har ansvar för att säkerställa att systemen fungerar på vederbörligt sätt ur ett uppgiftsskyddsperspektiv. Därför bör det förtydligas ytterligare vem som bör vara ansvarig för att genomföra tillämpningar och system vars utformning kommer att preciseras genom kommittéförfarandet och vem av aktörerna i kedjan som kommer att vara ansvarig för att uppgiftsbehandlingen sker i enlighet med lagstiftningen om uppgiftsskydd (närmare bestämt de registeransvariga). Datatillsynsmannen framhåller i det följande vissa av de frågor rörande integritet och uppgiftsskydd som bör hanteras inom ramen för kommittéförfarandet och av registeransvariga vid utformningen av tillämpningar och systemarkitektur. Dessutom behandlas några av de uppgiftsskyddsfrågor som måste tas upp av lagstiftaren och registeransvariga när det gäller ITS-tjänster.

III.1 Inbyggda skyddsmekanismer för att skydda den personliga integriteten ("privacy by design")

28. En riktig tillämpning av principerna för uppgiftsskydd i direktiv 95/46/EG är ett centralt villkor för att införandet av ITS i gemenskapen ska lyckas. Dessa principer får konsekvenser för utformningen av systemarkitekturen och tillämpningarna. Datatillsynsmannen rekommenderar att ett arbetssätt med inbyggda skyddsmekanismer för att skydda den personliga integriteten ("privacy by design") används i

⁽¹⁵⁾ I skäl 26 i direktiv 95/46/EC anges följande: "För att avgöra om en person är identifierbar skall härvid beaktas alla hjälpmedel som i syfte att identifiera vederbörande rimligen kan komma att användas antingen av den registeransvarige eller av någon annan person".

⁽¹⁶⁾ Ändring 34 innebär att en ny artikel 6.1 b införs med lydelsen "Personuppgifter ska endast behandlas i de fall då detta är nödvändigt för användandet av ITS-tillämpningar och/eller tjänster".

⁽¹⁷⁾ Ändring 36 innebär att följande text läggs till i artikel 6.2: "samt att de inte får användas för andra ändamål än de som nämns i detta direktiv".

- ett tidigt skede av utformningen av ITS, för att fastställa arkitektur, drift och förvaltning av tillämpningar och system. Detta arbetssätt framhävs framför allt i direktiv 1999/5/EG⁽¹⁸⁾ när det gäller utformningen av radioutrustning och teleterminalutrustning.
29. Utformningen av ITS-tillämpningar och system kommer att ske i flera steg och av olika operatörer som samtliga bör ta hänsyn till integritet och uppgiftsskydd. Kommissionen och ITS-kommittén kommer genom kommittéförfarandet inledningsvis att ha ett särskilt ansvar vid fastställandet av de åtgärder, standardiseringsinitiativ, förfaranden och bästa metoder som ska främja inbyggda skyddsmekanismer för att skydda den personliga integriteten.
30. Inbyggda skyddsmekanismer för att skydda den personliga integriteten bör uppmuntras i alla skeden av processerna och i alla former av processer.
- På organisatorisk nivå bör integriteten beaktas vid fastställandet av de förfaranden som krävs för utbyte av uppgifter mellan alla relevanta platser för utbyte – detta kan få direkta följder för vilken typ av utbyte som sker och vilka uppgifter som utbyts.
 - Integritets- och säkerhetskrav bör införlivas i standarder, bästa metoder, tekniska specifikationer och system.
 - På teknisk nivå rekommenderar datatillsynsmannen att man tar fram bästa tillgängliga teknik⁽¹⁹⁾, t.ex. genom kommittéförfarandet, för integritet, uppgiftsskydd och säkerhet inom särskilda sektorer och/eller för särskilda ändamål, där de olika säkerhetsparametrar som måste genomföras under hela systemets livslängd fastställs för att garantera att EU:s regelverk följs.
31. Datatillsynsmannen tar i det följande upp några av de frågor som särskilt måste behandlas vid utformningen av tillämpningarna och systemarkitekturen. De berör de insamlade uppgifterna, systemens driftskompatibilitet och skyddet för uppgifter.
- III.1.a) *Dataminimering och anonymitet*
32. I enlighet med artikel 6.1 c i direktiv 95/46/EG får endast personuppgifter som är nödvändiga och relevanta för särskilda ändamål samlas in och behandlas.
33. Datatillsynsmannen betonar vikten av att på ett lämpligt sätt klassificera information och uppgifter som ska behandlas i ITS innan tillämpningar och system utformas, för att undvika att personuppgifter i onödan samlas in i stor skala. I samband med detta bör hänsyn tas till
- varifrån uppgifterna kommer (offentliga källor, telekommunikationsleverantörer, leverantörer av ITS-tjänster, andra operatörer, fordon, användare av fordon eller andra registrerade),
 - uppgifternas art (t.ex. aggregerad information, anonyma uppgifter, personuppgifter, känsliga uppgifter),
 - de ändamål som uppgifterna är avsedda för, och
 - i fråga om samverkande system bör det klargöras vilka uppgifter som hämtas/lämnas från fordonet, som utbyts med andra fordon och/eller infrastrukturer och från infrastruktur till infrastruktur samt för vilka ändamål.
34. De enskilda funktionerna bör analyseras noga utifrån ändamålen för att bedöma om det är nödvändigt att samla in personuppgifter. Datatillsynsmannen betonar vikten av att göra en riktig avvägning mellan de registrerades grundläggande rättigheter och de olika berörda aktörernas intressen, vilket innebär att så få personuppgifter som möjligt ska behandlas. I största möjliga utsträckning bör tillämpningarnas och systemens arkitektur utformas så att endast de personuppgifter som är absolut nödvändiga för ändamålen samlas in.
35. Om personuppgifter inte är nödvändiga, eller är nödvändiga endast i ett tidigt skede av behandlingen, bör de inte samlas in eller också bör de anonymiseras så snart som möjligt. Det är alltså särskilt viktigt att man inte bara bedömer om det är nödvändigt att samla in uppgifter utan också om det är nödvändigt att de lagras i olika system. Särskilda tidsgränser för lagring av personuppgifter bör fastställas för alla olika aktörer i tjänstekedjan och de bör differentieras utifrån uppgiftstyp och det ändamål för vilket de samlades in⁽²⁰⁾. Följaktligen bör personuppgifter, när det inte längre är nödvändigt att behålla dem för att uppnå de ändamål för vilket de samlades in eller behandlades, anonymiseras, dvs. inte längre avse en identifierad eller identifierbar enskild individ.
36. Utformningen av systemarkitekturen och förfarandena för utbyte av uppgifter bör ligga till grund för att så få personuppgifter som möjligt behandlas. Därvidlag bör alla skeden av behandlingen och alla aktörer i leveranskedjan för ITS-tjänster beaktas. Vissa uppgifter kan utbytas och behandlas anonymt medan andra, även om utbytet sker anonymt, kan kopplas ihop med uppgifter om identifierade enskilda individer och kommer därför att utgöra personuppgifter

⁽¹⁸⁾ Främst i artikel 3.3 c i Europaparlamentets och rådets direktiv 1999/5/EG av den 9 mars 1999 om radioutrustning och teleterminalutrustning och om ömsesidigt erkännande av utrustningens överensstämmelse.

⁽¹⁹⁾ Med bästa tillgängliga teknik avses det mest effektiva och avancerade skedet i utvecklingen av åtgärder och deras funktionssätt och som anger en viss tekniks praktiska lämplighet att i princip ligga till grund för att tillämpningar och system för informationsteknik och datasäkerhet iakttar kraven på personlig integritet, dataskydd och säkerhet i EU:s regelverk.

⁽²⁰⁾ T.ex. regleras lagring av trafikuppgifter och lokaliseringssuppgifter som behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster i allmänna kommunikationsnät i Europaparlamentets och rådets direktiv 2006/24/EG av den 15 mars 2006 om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG.

enligt artikel 2 a i direktiv 95/46/EG ⁽²¹⁾. Mot bakgrund av de ändamål som ITS kommer att användas för förefaller det svårt att säkerställa att en stor mängd uppgifter som samlats in genom ITS kommer att behandlas anonymt, eftersom den enskilda individens identitet vid någon tidpunkt kommer att krävas för särskilda ändamål, t.ex. fakturering. Därför skulle det åtminstone krävas särskilda – tekniska, organisatoriska och juridiska – åtgärder för att garantera anonymitet på vissa områden.

III.1.b) Driftskompatibilitet, uppgifternas kvalitet och ändamålsbegränsning

37. Driftskompatibilitet mellan tillämpningar och system är av central betydelse för ett lyckat införande av ITS. Harmonisering kommer att ske i form av fastställande av tekniska specifikationer för gränssnitt som ska integreras i tillämpningar och system, så att de fungerar tillsammans med andra tillämpningar som finns inbyggda i andra transportsätt och/eller system. Driftskompatibla system kommer att bidra till att underlätta tillhandahållandet av ett antal olika tjänster och till att säkerställa kontinuitet inom dessa i hela Europa men innebär samtidigt ett antal risker från uppgiftsskyddssynpunkt, t.ex. risker för att uppgifter används på felaktigt sätt eller missbrukas. Varje sammankoppling av databaser bör göras med vederbörlig respekt för principerna om uppgiftsskydd ⁽²²⁾ och praktiska skyddsåtgärder (se även avsnitt III 1.c).
38. Principen om uppgiftskvalitet i artikel 6 d i direktiv 95/46/EG är särskilt viktig i samband med driftskompatibilitet mellan tillämpningar och system. De tekniska specifikationer som ska fastställas för utformningen av gränssnitt bör säkerställa att korrekta uppgifter erhålls vid sammankoppling av tillämpningar och system.
39. Med tanke på att driftskompatibla system kommer att underlätta sammankoppling av databaser och jämförelse av uppgifter för ytterligare ändamål betonar datatillsynsmannen att varje sammankoppling noga bör övervägas i förhållande till principen om ändamålsbegränsning i artikel 6.1 b i direktiv 95/46/EG. Det är särskilt viktigt att utformningen av systemarkitekturen för ITS förebygger all vidare användning av uppgifter för andra ändamål än dem för vilka uppgifterna samlades in. Lämpligt skydd måste byggas in i systemet för att förebygga felaktig användning, otillåten spridning av eller otillåten tillgång till uppgifter samt sideeffekter av anordningar. Exempelvis bör tillräckligt skydd finnas så att obehöriga tredje parter inte kan få tillgång till flyttbara anordningar och så att dessa inte används för att identifiera och spåra personer utöver ändamålen med systemet.

⁽²¹⁾ Se fotnot 15.

⁽²²⁾ Se även datatillsynsmannens kommentarer om kommissionens meddelande om interoperabilitet mellan europeiska databaser av den 10 mars 2006 http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/News/06-03-10_EO_EDPS_MoU_EN.pdf

40. När det gäller själva sammankopplingens lagenlighet kommer denna att behöva bedömas från fall till fall, med hänsyn till arten av de uppgifter som görs tillgängliga och utbyts genom systemen och till de ändamål för vilka de ursprungligen var avsedda.

III.1.c) Datasäkerhet

41. Säkerheten för personuppgifter är central vid införandet av ITS. Datatillsynsmannen hälsar med tillfredsställelse att säkerheten uttryckligen nämns i handlingsplanen och förslaget till direktiv. Säkerheten bör tas med i beräkningen inte bara under driften av ITS-anordningen (i det fordonsintegrerade systemet och i kommunikationstransportprotokollet) utan även när det gäller de databaser där uppgifterna behandlas och/eller lagras. Lämpliga tekniska, administrativa och organisatoriska krav bör fastställas för alla skeden av behandlingen som säkerställer en tillräcklig säkerhetsnivå i enlighet med artiklarna 16–17 i direktiv 95/46/EG (samt artiklarna 4–5 i direktiv 2002/58/EG, i tillämpliga fall).
42. Lämpliga säkerhetsåtgärder bör fastställas först efter en noggrann bedömning av de särskilda ändamål för vilka ITS kommer att användas och av formerna för behandlingen. I detta sammanhang rekommenderar datatillsynsmannen att konsekvensanalyser avseende integritets- och uppgiftsskydd görs för särskilda sektorer och/eller ändamål för användningen (t.ex. för säkerhetsrelaterade ITS-system, godshanteringsystem etc.) Genomförande av konsekvensanalyser avseende integritets- och uppgiftsskydd och användandet av bästa tillgängliga teknik för integritet och uppgiftsskydd kommer att bidra till att fastställa vilka säkerhetsåtgärder som är lämpligast för en specifik behandling av uppgifter.

III.2 Ytterligare överväganden om uppgiftsskydd och integritet när det gäller tillhandahållande av ITS-tjänster

43. Det krävs ytterligare harmonisering av formerna för införande av ITS-tjänster på EU-nivå för att undvika skillnader vid införandet av dessa tjänster. Datatillsynsmannen vill i detta avseende framhålla framför allt följande två frågor som kommer att kräva ytterligare överväganden från integritets- och uppgiftsskyddssynpunkt:
- Användandet av lokaliseringsverktyg för tillhandahållande av platsbaserade offentliga och kommersiella tjänster kräver ytterligare skyddsåtgärder. I detta sammanhang bör man särskilt uppmärksamma om och när platsbaserade ITS-tjänster används för privata ändamål eller för yrkesmässiga ändamål och hur enskilda individer som använder ett fordon yrkesmässigt kan påverkas av ett sådant system.
 - Det är särskilt viktigt i integrerade system att roller och ansvar för de olika parterna vid ITS-införandet klargörs.

III.2.a) Skyddsåtgärder för användningen av lokaliseringssverktyg vid tillhandahållande av platsbaserade ITS-tjänster

44. Införandet av ITS kommer att stödja utvecklingen av tillämpningar för spårning av gods och möjliggöra införande av platsbaserade kommersiella och offentliga tjänster. Sådana tjänster kommer att bygga på användning av t.ex. satellitbaserad positionsbestämning och RFID-etiketter⁽²³⁾. Navigations- och spårningssystem är avsedda för många olika ändamål, bl.a. distansövervakning av fordon och gods längs färdvägen (t.ex. vid transport av farligt gods eller levande djur), fakturering av fordon utifrån en mängd olika parametrar såsom tillryggalagt avstånd och tid på dygnet (t.ex. differentierade vägavgifter, elektroniska väg-tullsystem) samt övervakning av förare för efterlevnad av bestämmelser genom kontroll av körtider (med hjälp av digitala färdskrivare) och utdömmande av påföljder (genom elektronisk fordonsidentifiering).
45. Användningen av lokaliseringsteknik är särskilt inkräktande från integritetssynpunkt eftersom den gör det möjligt att spåra förare och samla in en stor mängd olika uppgifter om deras körvanor. Som artikel 29-gruppen betonade⁽²⁴⁾ är behandlingen av lokaliseringssuppgifter en särskilt känslig fråga som berör centrala ting som friheten att kunna röra sig anonymt, där det krävs särskilda skyddsåtgärder för att förhindra att enskilda individer övervakas och att uppgifter används på felaktigt sätt.
46. Datatillsynsmannen betonar att användningen av lokaliseringssverktyg måste följa lagen, dvs. bygga på en korrekt rättslig grund för uttryckligt angivna och berättigade ändamål samt vara proportionerlig mot dessa ändamål. Huruvida det är tillåtet att behandla uppgifter kommer i stor utsträckning att bero på hur och för vilket ändamål lokaliseringssverktyg används. Som artikel 29-gruppen underströk i sitt yttrande om eCall kan man "ur uppgiftsskydssynpunkt inte acceptera system med permanent uppkoppling som gör det möjligt att lokalisera fordon när som helst, även om eCallsystemet inte aktiverats"⁽²⁵⁾. Det är därför viktigt att ytterligare klargöra de särskilda omständigheter under vilka ett fordon kommer att spåras och effekterna av det för användaren. Under alla förhållanden bör användningen av lokaliseringssutrustning motiveras av ett berättigat behov (t.ex. övervakning av godstransporter) och begränsas till vad som är absolut nödvändigt för det

ändamålet. Det är följaktligen viktigt att precisera vilka lokaliseringssuppgifter som samlas in, var de lagras och hur länge, med vem och för vilka ändamål de utbyts samt att vidta alla åtgärder som krävs för att undvika att uppgifterna missbrukas eller används på felaktigt sätt.

47. Behandlingen av lokaliseringssuppgifter som gäller användare av allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster regleras strikt i artikel 9 i direktiv 2002/58/EG. Där krävs bland annat att behandlingen av lokaliseringssuppgifter ska ske anonymt eller efter informerat samtycke från användaren. Det innebär att användare, innan de samtycker till att lokaliseringssverktyg används, måste få lämplig information, inbegripet om vilken typ av lokaliseringssuppgifter som kommer att behandlas, behandlingens syfte och varaktighet samt om huruvida uppgifterna kommer att vidarebefordras till tredje part för tillhandahållande av mervärdestjänsten. Det måste finnas ett enkelt sätt för användare att kostnadsfritt tillfälligt kunna motsätta sig behandlingen av lokaliseringssuppgifter för varje uppkoppling till nätet eller för varje överföring av kommunikation. Behandlingen av lokaliseringssuppgifter ska begränsas till personer som handlar på uppdrag av leverantören av ett allmänt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst eller den tredje part som tillhandahåller mervärdestjänsten.
48. Ytterligare skyddsåtgärder måste vidtas när lokaliseringssuppgifter samlas in från fordon som används vid yrkesmässig verksamhet, för att hindra att lokaliseringsteknik används för otillbörlig övervakning av anställda. Under alla förhållanden bör behandlingen begränsas till lokaliseringssuppgifter som samlats in under arbetstid – anställda ska följaktligen kunna stänga av lokaliseringssfunktionen utanför arbetstid och/eller när fordonet används för privat bruk.
49. Det finns en risk att tredje parter (t.ex. försäkringsbolag, arbetsgivare och brottsbekämpande myndigheter) kräver tillgång till uppgifter som samlats in genom navigations- och spårningssystem för berättigade och särskilda ändamål (såsom spårning av gods, betalning av vägtull etc.) för användning för bisyften, t.ex. att kontrollera körtider och viloperioder eller för att kontrollera att trafikbestämmelser följs och utdöma påföljder. I princip är det inte tillåtet med tillgång till uppgifter för bisyften om syftet därmed är oförenligt med de ändamål för vilka uppgifterna samlades in. Tillgång till uppgifter kan endast medges genom undantag från denna princip om villkoren för detta uppfyller de stränga kraven i artikel 13 i direktiv 95/46/EG. Därför bör tredje parter endast få tillgång till lokaliseringssuppgifter i enlighet med lagen och på ett sätt som medger insyn, på

⁽²³⁾ Se frågor om integritet och uppgiftsskydd med anledning av användningen av RFID i yttrandet från Europeiska datatillsynsmannen om meddelandet från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén och Regionkommittén "Radiofrekvensidentifiering (RFID) i Europa: på väg mot en strategi" KOM(2007) 96, EUT C 101, 23.4.2008, s. 1 http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-12-20_RFID_EN.pdf

⁽²⁴⁾ Artikel 29-gruppen, yttrande om användning av lokaliseringssuppgifter för att tillhandahålla mervärdestjänster, WP 115, november 2005 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp125_sv.pdf

⁽²⁵⁾ Se WP 125 om eCall s. 5, nämnt i fotnot 10.

grundval av lagstiftning där lämpliga förfaranden och former anges för tillgången till uppgifter för särskilda ändamål, med tillräckliga skyddsåtgärder för enskilda individer i enlighet med de vidare ändamål som deras uppgifter kan användas för.

III.2.b) Roller och ansvar för ITS-aktörer

50. Det står ännu inte klart vem som är registeransvarig vid varje del av behandlingen av uppgifter. I många fall är det sannolikt att leverantörer av ITS-tjänster kommer att vara registeransvariga, antingen ensamma ansvariga för personuppgifter som behandlas för tillhandahållande av deras egna ITS-tjänster eller ansvariga tillsammans med andra registeransvariga i fall där behandlingen görs tillsammans med dessa. Roller och ansvar, som registeransvariga och registerförare, för operatörer som deltar i ITS i olika egenskaper, bör vara tydligt angivna för varje del av behandlingen (t.ex. för teleoperatörer som tillhandahåller både kommunikationstjänster och ITS-tjänster).
51. När dessa personer handlar som registeransvariga kommer de att ha ansvaret⁽²⁶⁾ för att garantera att systemen och tjänsterna uppfyller alla skyldigheter rörande uppgiftsskydd, särskilt för att förverkliga system med inbyggda skyddsmekanismer för att skydda den personliga integriteten, där uppgiftskvalitet och principer om ändamålsbegränsning iaktas och som garanterar en lämplig nivå av datasäkerhet, som beskrivs i III.1).
52. Registeransvariga kommer att behöva säkerställa att lämpliga skyddsåtgärder vidtas på alla nivåer i kedjan med aktörer i ITS-införandet. Detta kommer framför allt att kräva att de ingår lämpliga avtal med alla intressenter som deltar i utbytet och behandlingen av uppgifter, med tillräckliga åtgärder för uppgiftsskydd (särskilt med iakttagande av artiklarna 16 och 17 i direktiv 95/46/EG och artiklarna 4 och 5 i direktiv 2002/58/EG). Det är viktigt att notera från ett uppgiftsskyddsperspektiv att registeransvariga måste säkerställa uppgiftsskyddet i alla skeden av behandlingen och att de samtidigt har ansvar för behandlingen och inte kan friskriva sig från sitt ansvar genom avtal.

IV. SLUTSATSER

53. Datatillsynsmannen välkomnar den föreslagna planen för införande av ITS som kommissionen har lagt fram, som syftar till en harmonisering av uppgiftsbehandlingen i hela Europa för att underlätta tillhandahållandet av ITS-tjänster och där man för fram uppgiftsskydd som ett centralt villkor för att ITS ska kunna införas på korrekt sätt i Europa.
54. Datatillsynsmannen noterar att det föreslagna direktivet innehåller en allmän ram som ger upphov till ett antal frågor som rör integritet och uppgiftsskydd som måste

behandlas mer ingående på EU-nivå och nationell nivå, bl.a. följande:

- Det finns en risk för att bristen på tydlighet i den föreslagna rättsliga ramen kommer att leda till skillnader i införandet av ITS i Europa vilket kommer att leda till olika nivåer av uppgiftsskydd i Europa. Datatillsynsmannen betonar behovet av ytterligare harmonisering i dessa frågor på EU-nivå för att klargöra kvarstående frågor (t.ex. fastställande av roller och ansvar för ITS-aktörer, vilka särskilda ITS-tillämpningar och system som måste finnas inbyggda i fordon, utarbetandet av harmoniserade avtal för tillhandahållande av ITS-tjänster, de särskilda ändamålen och formerna för användningen av ITS etc.) Det är särskilt väsentligt att fastställa vilka som är registeransvariga när det gäller uppgiftsbehandlingen, eftersom de kommer att ha ansvar för att garantera att integritet och uppgiftsskydd beaktas på alla nivåer i uppgiftsbehandlingskedjan.
- Beslut som rör vissa former av behandlingen som kan få allvarliga följder för rättigheter avseende enskildas privatliv och uppgiftsskydd bör fattas av Europaparlamentet och rådet, och inte genom ett kommittéförfarande.
- Det är av yttersta vikt att ta hänsyn till integritet och uppgiftsskydd tidigt i behandlingen och i alla skeden av behandlingen. Införandet av inbyggda skyddsmekanismer för att skydda den personliga integriteten ("privacy by design") bör uppmuntras vid utformningen av ITS-tillämpningar och system, och de bör införlivas i standarder, bästa metoder, tekniska specifikationer och system.
- All sammankoppling av tillämpningar och system bör göras med vederbörlig respekt för principer för uppgiftsskydd och praktiska skyddsåtgärder.
- Med tanke på den osäkerhet som fortfarande råder om formerna för införande av ITS välkomnar datatillsynsmannen särskilt kommissionens initiativ i meddelandet att genomföra en utredning om integritetsaspekter senast 2011. Datatillsynsmannen rekommenderar vidare starkt att konsekvensanalyser avseende integritets- och uppgiftsskydd görs för särskilda sektorer och/eller ändamål för fastställande av lämpliga säkerhetsåtgärder och att bästa tillgängliga teknik för integritet, uppgiftsskydd och säkerhet i ITS utvecklas.
- Datatillsynsmannen betonar också att medlemsstaterna kommer att vara ansvariga för att genomföra direktivet på korrekt sätt, så att ITS-operatörer inför system och tjänster med en lämplig nivå av uppgiftsskydd i hela Europa.

⁽²⁶⁾ Se fotnot 13.

- Lämpliga skyddsåtgärder bör införas av registeransvariga som tillhandahåller ITS-tjänster så att användningen av lokaliseringsteknik, t.ex. satellitbaserad positionsbestämning och RFID-etiketter, inte inkräktar på enskilda individers integritet när de använder fordon i ett rent privat eller yrkesmässigt sammanhang. Detta kommer framför allt att kräva att behandlingen begränsas till uppgifter som är absolut nödvändiga för ändamålet, garantier för att lämpliga säkerhetsåtgärder finns inbyggda i systemen så att lokaliseringssuppgifter inte lämnas ut till obehöriga mottagare samt att användare på ett effektivt sätt kan avaktivera lokaliseringsanordningen/lokaliseringsfunktionen.
55. Datatillsynsmannen rekommenderar att artikel 6 i förslaget ändras, i enlighet med direktiv 95/46/EG, på följande sätt:
- Dataminimering bör uppmuntras för uppgiftsbehandling som görs i ITS. Ur denna synvinkel rekommenderas en ändring av artikel 6.1 b i förslaget enligt följande: "Personuppgifter ska endast behandlas i de fall då detta är nödvändigt för det särskilda ändamål för vilket ITS används och i enlighet med en lämplig rättslig grund".
- Det är viktigt att personuppgifter som behandlas genom driftskompatibla system inte används för ytterligare ändamål som är oförenliga med de ändamål för vilka de samlades in. Därför rekommenderas en ändring av artikel 6.2 enligt följande formulering "samt att de inte får användas för andra ändamål än de ändamål för vilka de samlades in på ett sätt som är oförenligt med dessa ändamål".
- Datatillsynsmannen rekommenderar att en uttrycklig hänvisning till begreppet "inbyggda skyddsmekanismer för att skydda den personliga integriteten" ("privacy by design") vid utformningen av ITS-tillämpningar och system läggs till i artikel 6 i förslaget. Dessutom rekommenderar datatillsynsmannen att artikel 29-gruppen och datatillsynsmannen får information om och rådfrågas om ytterligare åtgärder som vidtas i denna fråga genom kommittéförfarandet.
56. Datatillsynsmannen rekommenderar att en hänvisning till detta samråd görs i skälen i förslaget.
57. Mot bakgrund av ovanstående rekommenderar datatillsynsmannen att dataskyddsmyndigheter, särskilt genom artikel 29-gruppen, och datatillsynsmannen deltar i nära samverkan i initiativ som rör införandet av ITS, genom samråd på ett tillräckligt tidigt stadium innan relevanta åtgärder utarbetas.
- Utfärdat i Bryssel den 22 juli 2009.
- Peter HUSTINX
Europeisk datatillsynsman