EUROPEAN DATA PROTECTION SUPERVISOR

Opinion of the European Data Protection Supervisor on the Communication from the Commission on an Action Plan for the Deployment of Intelligent Transport Systems in Europe and the accompanying proposal for a Directive of the European Parliament and of the Council laying down the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other transport modes

(2010/C 47/02)

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty establishing the European Community, and in particular its Article 286,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular its Article 8,

Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,

Having regard to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector,

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, and in particular its Article 41,

Having regard to the request for an opinion in accordance with Article 28(2) of Regulation (EC) No 45/2001 received on 11 February 2009 from the European Commission,

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION

1. On 16 December 2008, the Commission adopted a Communication defining an Action Plan for the Deployment of Intelligent Transport Systems in Europe ('the Communication') [1]. The Communication is accompanied by a proposal for a Directive of the European Parliament and of the Council laying down the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other transport modes ('the Proposal') [2]. The Communication and the accompanying Proposal were sent by the Commission to the EDPS for consultation, in accordance with Article 28(2) of Regulation (EC) No 45/2001 [3].

2. The EDPS welcomes that he is consulted and recommends that reference to this consultation be made in the recitals of the proposal, in a similar way as in a number of other legislative texts on which the EDPS has been consulted, in accordance with Regulation (EC) No 45/2001.

I.1. The Commission Communication on an Action Plan for the Deployment of ITS in Europe

3. 'Intelligent Transport Systems' ('ITS') are advanced applications that use Information and Communication Technologies (ICT), which are embedded in different transport modes for interaction between them. In the field of road transport, ITS will provide innovative services on transport modes and traffic management to various users such as travellers, road transport infrastructure users and operators, fleet managers and operators of emergency services.

4. Taking stock of the growing deployment of ITS in various transportation modes [4] in the European Union, the Commission adopted an action plan to accelerate the

[1] COM(2008) 886 final. The Council adopted conclusions concerning the Communication at the 2935th Council Transport, Telecommunications and Energy meeting on 30 and 31 March 2009.

[2] COM(2008) 887 final.

[3] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

[4] There are many initiatives at EU level integrating ITS in various transportation modes including air transport (SESAR), waterway (RIS), railway (ERTMS, TAF-TSI), shipping (VTMIS, AIS, LRIT), and road transport (eToll, eCall), see COM(2008) 886 final, p. 3.

introduction and use of ITS applications and services in the field of road transport. The plan also aims at ensuring their interaction with other transport modes, which will facilitate the provision of multimodal services. The coherent deployment of ITS in Europe will serve various Community objectives, including transport efficiency, sustainability, safety and security, fostering the EU internal market and competitiveness. In view of the diversity of the objectives pursued for ITS deployment, the Communication outlines six priority areas for action in the period 2009-2014. To implement the plan, the Commission proposes that a legal framework is defined at EU level by means of a Directive, under which a number of measures in selected priority areas will be defined.

I.2. **Proposal for a Directive laying down the framework for the deployment of ITS in the field of road transport and for interfaces with other transport modes**

5. The Proposal sets out a framework for the transnational deployment of ITS applications that is intended to facilitate the provision of harmonised cross-border services, notably for traffic and travel information and traffic management. It requires Member States to take several technical measures to facilitate data exchanges between users, public authorities, relevant stakeholders and ITS service providers and to integrate in vehicles and road infrastructure ITS systems that are related to safety and security. Technical specifications for ITS applications and systems in four of the priority areas ([5]) listed in the action plan will be defined through a comitology procedure ([6]), whose core elements are specified in Annex II. The specific purposes for which ITS will be used in these areas are however not clear. Furthermore, the deployment of ITS may extend to many more areas than the four initially selected for the development of harmonised technical specifications. While the Proposal mainly deals with the deployment of future ITS applications and services, it shall also, where feasible, encompass existing or currently developing technologies in that field (such as eCall, eToll, etc.).

6. The Proposal was sent to the European Parliament, which adopted its position in first reading ([7]) on 23 April 2009. Further to a request for consultation from the Council on 29 January 2009, the European Economic and Social Committee adopted an opinion on the Proposal on 13 May 2009 ([8]).

I.3. **Focus of the opinion**

7. The EDPS welcomes the consultation on the proposed ITS deployment plan put forward by the Commission. This is not the first time that the EDPS deals with the issues raised in the ITS Action Plan. The EDPS issued an opinion on the Commission proposal on facilitating cross-border enforcement in the field of road safety ([9]) and contributed to the work of the Article 29 Working Party on a working document on eCall ([10]).

8. Intelligent Transport Systems are based on the collection, processing and exchange of a wide variety of data, from public and private sources; they therefore constitute a data-intensive area. The deployment of ITS will rely to a large extent on geolocalisation technologies, such as satellite-positioning and contact-less technologies, such as RFID, which will facilitate the provision of a variety of public and/or commercial location-based services (e.g. real-time traffic information, eFreight, eCall, eToll, parking reservation, etc.). Some of the information that will be processed through ITS is aggregated — such as on traffic, accidents, and opportunities — and does not relate to any individual, while other information is related to identified or identifiable individuals and therefore qualifies as personal data within the meaning of Article 2(a) of Directive 95/46/EC.

9. The EDPS considers as essential that the actions planned for ITS deployment are consistent with the existing legal framework as cited in the Proposal, in particular Directive 95/46/EC on data protection ([11]) and Directive 2002/58/EC on e-privacy ([12]).

([5]) Article 4 of the Proposal envisages the definition of technical measures in the following areas: (i) optimal use of road, traffic and travel data; (ii) continuity of traffic and freight management ITS services on European corridors and in conurbations; (iii) road safety and security; and (iv) integration of the vehicle into the transport infrastructure.

([6]) The Proposal provides for a regulatory procedure with scrutiny, in accordance with Article 5(a)(1) to (4) and Article 7 of Decision 1999/468/EC.

([7]) European Parliament legislative resolution of 23 April 2009 on the proposal for a Directive of the European Parliament and of the Council laying down the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other transport modes, T6-0283/2009.

([8]) Opinion of the European Economic and Social Committee on the proposal for a Directive of the European Parliament and of the Council laying down the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other transport modes, TEN/382, 13 May 2009.

([9]) Opinion of the European Data Protection Supervisor on the proposal for a Directive of the European Parliament and of the Council facilitating cross-border enforcement in the field of road safety, 2008/C 310/02 (OJ C 310, 5.12.2008, p. 9).

([10]) Article 29 Working Party working document on data protection and privacy implications in eCall initiative, WP 125, 26 September 2006. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp125_en.pdf

([11]) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

([12]) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

10. Unresolved issues in privacy and data protection have been identified by the Commission as one of the main obstacles for promoting ITS. These issues will be developed as follows in this opinion:

— in Chapter II, the legal framework put forward by the Commission for the deployment of ITS will be analysed from a data protection perspective,

— Chapter III will highlight the data protection concerns that must be further addressed for the proper deployment of ITS:

— in a first point, the opinion will emphasize the need for 'privacy by design' in the development of ITS and will further outline the important issues that must be tackled in the design of ITS applications and data processing systems,

— the second point will focus on some of the privacy considerations that must be further addressed for the provision of ITS services.

II. ANALYSIS OF THE LEGAL FRAMEWORK PROPOSED FOR ITS DEPLOYMENT

11. The Commission proposal for a Directive contains two provisions (recital 9 and Article 6) dealing with privacy, security and re-use of information. Article 6(1) of the Commission Proposal requires that the operation of ITS is carried out in compliance with the data protection rules set out, inter alia, in Directive 95/46/EC and Directive 2002/58/EC. In the Commission Proposal, Article 6(2) envisages concrete data protection measures mainly from a security viewpoint: Article 6(2) of the Proposal states that 'Member States shall ensure that ITS data and records are protected against misuse, including unlawful access, alteration or loss'. Finally, Article 6(3) of the Commission Proposal provides that 'Directive 2003/98/EC shall apply'.

12. The European Parliament proposed in first reading amendments concerning Article 6. In particular, three new paragraphs are added in Article 6(1), which relate to the use of anonymous data where appropriate, to the processing of sensitive data only upon informed consent of the data subject, and to ensuring that personal data are only processed 'insofar as processing is necessary for the performance of the ITS application and/or service'. In addition, Article 6(2) is modified by adding that ITS data and records 'may not be used for purposes other than those referred to in the Directive.'

13. The EDPS welcomes that data protection has been taken into consideration in the drafting of the Proposal and that it is put forward as a general condition for the proper deployment of ITS in Europe. The EDPS acknowledges that there is a need for a coherent harmonisation of data processes at EU level in order to ensure the workability of ITS applications and services across Europe.

14. The EDPS, however, notes that the proposed legal framework is too broad and general to adequately address the privacy and data protection concerns raised by ITS deployment in the Member States. It is not clear when the performance of ITS services will lead to the collection and processing of personal data, what are the specific purposes for which a data processing occurs, nor what is the legal basis that justifies such processing. Furthermore, the use of location technologies for ITS deployment raises the risk of developing services that are intrusive from a privacy viewpoint if they entail the collection and exchange of personal data. Moreover, the Proposal does not clearly set out the roles and responsibilities of the various operators intervening in the chain of ITS deployment, and it is thus difficult to know which operators will be data controllers and will therefore be responsible ([13]) for compliance with data protection obligations. ITS operators will be faced with considerable problems if all these issues are not clarified in the law, since they will ultimately be the ones in charge of applying the measures set out in the proposed Directive.

15. There is therefore a risk that the lack of clarity of the proposed legal framework will create diversity in the implementation of ITS in Europe and that, instead of reducing divergences amongst Member States it will, on the contrary, lead to considerable uncertainty, fragmentation and inconsistencies, due to different levels of data protection in Europe. This may also lead to a lack of compliance with essential safeguards for data protection. The EDPS emphasizes the need for further harmonisation on these issues at EU level. The EDPS will hereby suggest modifications to the proposed legal framework from a data protection viewpoint. He strongly recommends that Parliament and Council insert in the Proposal the proposed modifications as well as, where feasible, additional provisions to clarify outstanding issues (such as definition and responsibilities of ITS actors, development of

([13]) According to Articles 2(d), 6(2) and 23 of Directive 95/46/EC, mentioned in footnote 11.

harmonised contracts for the provision of ITS services, etc.). He further stresses that Member States will also bear responsibility in implementing the Directive in a proper fashion so that operators can develop systems and services that offer an appropriate level of data protection across Europe.

II.1. **Data processing activities must rely on an appropriate legal basis**

16. It is not clear when processing of personal data will start once ITS equipment is integrated in a vehicle and on which legal ground the processing will be performed. Different legal bases may be relied upon by operators for the data processing, inter alia unambiguous consent of users, a contract or a legal obligation with which the controller shall comply. There is a need to harmonise the legal basis upon which the processing of data through ITS will be carried out in order to ensure that the systems work throughout Europe and that users do not suffer from divergences in the way processing occurs in each EU country.

17. In a number of cases, ITS systems will be integrated in vehicles by default. This is notably the case for safety and security-related ITS systems, which must be embedded in vehicles pursuant to the Proposal. The Proposal does not however define what 'safety and security-related ITS systems' are, and it should therefore be further clarified what the specific ITS applications and systems are that must be embedded in vehicles. Furthermore, it should be made clear whether the activation and use of the device will be done on a voluntary or on a compulsory basis for users. The choice to perform a data processing on a mandatory basis should only be made for specific purposes in consideration of compelling justifications (e.g. good tracking for freight management) and with appropriate safeguards as concerns the processing of data relating to individuals. If the use of ITS is made on a voluntary basis, appropriate safeguards should be implemented to prevent that by reason of the mere presence of the system in the vehicle users are deemed to have implicitly consented to its use.

18. The EDPS favours the choice that ITS services are provided on a voluntary basis. This entails that users must be able to freely consent to the use of the system and to the particular purposes for which it will be used. When the service provided relies on location data, appropriate information must be provided to the user (in accordance notably with Article 9 of Directive 2002/58/EC), who must be in a position to withdraw this consent. In practical terms, this requires that an easy way of de-activation of the device and/or feature must be introduced, without technical or financial constraint for the user ([14]), when the user no longer agrees to the use of the system and/or of a particular feature. Further safeguards should be implemented so that users are not discriminated against when they refuse to use a service.

19. In cases where certain processing activities are mandatory and others are subject to the consent of the user, transparency must be ensured about the various data processing operations performed, by providing appropriate information to users about the mandatory and/or voluntary nature of each particular processing and the scope of such processing. Furthermore, it will be crucial to implement appropriate security safeguards so that no data are collected and processed outside the scope of what has been legally defined and/or voluntary agreed.

20. In consideration of the transnational effect of ITS services, the EDPS further recommends developing pan-European standard contracts to ensure that services provided through ITS offer the same data protection safeguards across Europe, and in particular that information provided to users is sufficiently clear about the specific features used, the impact on the use of specific technologies on the protection of their data, and how they can exercise their rights. When new features are added, further steps should be taken by service providers to provide clear and specific information to users in respect of these additional features and to obtain their appropriate consent to the use of new features.

II.2. **The purposes and modalities of data processing must be further defined**

21. The EDPS notes that the Proposal does not precisely define the specific services and purposes for which ITS applications could be used, which are thus left open. This allows flexibility in practice, but means that unresolved issues in privacy and data protection — identified by the Commission as one of the main obstacles for promoting ITS (see point 10) — may remain unresolved and could hamper a balanced implementation of the proposed measures.

22. The EDPS emphasizes that it is particularly important that the processing operations undertaken for the provision of specific ITS services are not only done pursuant to an appropriate legal basis, but also for specified, explicit and legitimate purposes, and that the envisaged processing is proportionate and necessary for those purposes (Article 6 of Directive 95/46/EC). Consideration should therefore be given to the possible need to further legislate at EU level in respect of specific uses of ITS in order to provide a harmonised and adequate legal basis for the processing activities to be undertaken, and in order to avoid discrepancies in the deployment of ITS services between Member States.

23. Under the proposed framework there is no decision as yet about the modalities of the data processing and of the data exchanges for the use of ITS. Many technical parameters, the choice of which will have different privacy and data protection implications, will only be decided at a later stage through comitology. Taking into account the particular protection granted to privacy and data

([14]) See WP 125 on eCall, p. 4, mentioned in footnote 10.

protection as fundamental rights protected in Article 8 of the European Convention of Human Rights and Fundamental Freedoms and in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, it can be questioned whether and to which extent the definition of the data processing operations should be decided through comitology procedure.

24. In a democratic society, decisions on essential principles and modalities that impact fundamental rights should be taken within a full legislative procedure, which includes the appropriate checks and balances. In this case, this means that decisions that have a major impact on the privacy and data protection of individuals, such as purposes and modalities of mandatory data processing activities and the definition of modalities for the deployment of ITS in new areas should be decided by European Parliament and Council and not through comitology procedure.

25. In this perspective, the EDPS strongly advises that the Article 29 Working Party and the EDPS are involved, where relevant, in the work of the Committee created under Article 8 of the Proposal and in future actions taken concerning the deployment of ITS, through consultation at a sufficiently early stage before the development of relevant measures.

26. Furthermore, the EDPS takes note of the amendments adopted by the European Parliament in relation to Article 6 of the Proposal. The EDPS first notes that the amendment relating to encouraging the use of anonymous data where appropriate, although very welcome in principle, will not solve all data protection concerns as many data collected and exchanged through ITS may qualify as personal data. For the processing of personal data to be done on an anonymous basis, there must be no possibility for any person at any stage of the processing — taking account of all the means likely reasonably to be used either by the controller or by any other person — to link the data with data relating to an identified individual, otherwise such data constitute personal data in the meaning of Article 2(a) of Directive 95/46/EC ([15]). Further, on the basis of the amendments proposed by the European Parliament, the EDPS recommends that Article 6 of the Proposal is modified as follows:

— the assessment of the necessity of processing personal data through ITS should be made in view of the legitimate and specific purposes for which data are processed (in accordance with Articles 6 and 7 of Directive 95/46/EC). The performance of the ITS application ([16]) itself cannot be a legitimate purpose justifying the data processing, as the application is only a means of collecting and exchanging data, the use of which should necessarily be oriented towards particular purposes,

— the amendment ([17]) relating to the prohibition to use ITS data and records 'for purposes other than those referred to in this Directive' does not provide sufficient guarantees, in particular as the specific purposes and services for which ITS will be used are not clearly and exhaustively set out in the Directive. Considering that various data processing activities will be carried out through ITS for very different purposes, it should be ensured that the data collected in the course of processing for one particular purpose are not used for other purposes that are incompatible, as provided in Article 6(1)(b) of Directive 95/46/EC. The EDPS therefore recommends that Article 6(2) should be further modified to ensure that ITS data and records are not used 'for purposes other than the ones for which they were collected in a way incompatible with those purposes'.

III. DATA PROTECTION IN INTELLIGENT TRANSPORT SYSTEMS

27. It is particularly crucial that the roles of the different actors involved in ITS are clarified in order to identify who will bear the responsibility to ensure that systems work properly from a data protection perspective. It should therefore be further clarified who should be responsible for implementing the applications and systems the design of which will be specified through comitology, and who will be responsible amongst the chain of actors for compliance of the data processing with data protection law (i.e. the data controllers). The EDPS will underline below some of the privacy and data protection concerns that should be addressed in comitology and by data controllers when designing the applications and systems architecture. Further, he will outline some of the data protection issues that must be addressed by the legislator and data controllers in respect of the provision of ITS services.

III.1. 'Privacy by design'

28. The correct application of the data protection principles set forth in Directive 95/46/EC is a core condition for the success of the deployment of ITS in the Community. These principles have implications for the design of the systems architecture and applications. The EDPS recommends that a 'privacy by design' approach is adopted at an early stage of the design of ITS, to define

([15]) As set out in recital 26 of Directive 95/46/EC, 'to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person.'

([16]) Amendment 34 introducing a new Article 6(1)(b) provides: 'Personal data shall only be processed insofar as processing is necessary for the performance of the ITS application and/or service.'

([17]) Amendment 36 adds to Article 6(2) the following text: 'and may not be used for purposes other than those referred to in this Directive.'

the architecture, operation and management of the applications and systems. This approach is notably emphasised in Directive 1999/5/EC ([18]) as concerns the design of radio and telecommunications terminal equipment.

29. The design of ITS applications and systems will be done in several stages, by various actors, who should all take into account privacy and data protection. The Commission and the ITS Committee will bear specific initial responsibility in the definition, through the comitology procedure, of measures, standardisation initiatives, procedures and best practices that should promote 'privacy by design'.

30. 'Privacy by design' should be encouraged at all stages of the processes and in all forms of the processes:

— at an organisational level, privacy should be considered in the definition of the necessary procedures for data exchange between all relevant points of exchange — this may have direct impact on the type of exchange and on which data are exchanged,

— privacy and security requirements should be incorporated within standards, best practices, technical specifications, and systems,

— at the technical level, the EDPS recommends the development, for instance through comitology, of Best Available Techniques ([19]) (BATs) for privacy, data protection and security in specific sectors and/or for particular purposes, in which the different security parameters that must be implemented throughout the lifecycle of the system would be defined in order to guarantee compliance with the EU regulatory framework.

31. The EDPS outlines some of the issues that must be specifically addressed in the design of the applications and the architecture of the systems below. They relate to the data collected, to the interoperability of systems, and to the security of the data.

III.1(a) *Data minimisation and anonymity*

32. In accordance with Article 6(1)(c) of Directive 95/46/EC, only personal data that are necessary and relevant for specific purposes may be collected and processed.

33. The EDPS stresses the importance of undertaking an appropriate classification of the information and data to be processed through ITS before designing the applications and systems, in order to avoid a massive and inappropriate collection of personal data. In this respect, account should be taken of:

— the source of the data (whether from a public source, telecommunication provider, ITS service provider, other operators, vehicle, user of vehicle or other data subjects),

— the nature of the data (e.g. aggregated information, anonymous data, personal data, sensitive data),

— the purpose(s) for which the data are intended to be used, and

— with respect to cooperative systems, it should be clarified which data is pushed/pulled from the vehicle, exchanged with other vehicle and/or infrastructure, and from infrastructure to infrastructure, and for what purposes.

34. The single features should be carefully analyzed according to the pursued purposes in order to assess the necessity of collecting personal data. The EDPS stresses the importance of striking a proper balance between the fundamental rights of data subjects and the interests of the different actors involved, which implies that as few personal data as possible are processed. To the greatest extent, the architecture of the applications and systems should be designed in such a way that only the personal data that are strictly necessary for fulfilling the purposes to be achieved are collected.

35. If personal data are not necessary or are necessary only at an early stage of the processing, they should not be collected or should be anonymised as soon as possible. It is thus particularly important not only to assess the necessity of collecting data, but furthermore of retaining them in the different systems. Specific time limits for storage of personal data should be defined for all different actors in the service chain, which should be differentiated according to the type of data and purpose for which they were collected ([20]). As a result, when it is no longer necessary to keep personal data to achieve the purposes for which they were collected or further processed, they should be rendered anonymous, i.e. no longer relate to an identified or identifiable individual.

36. The design of the systems architecture and the data exchange procedures should support the processing of as few personal data as possible. In this respect, all stages of the processing and all actors in the chain of provision of

([18]) Mainly the Article 3.3(c) of Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity.

([19]) Best Available Techniques shall mean the most effective and advanced stage in the development of activities and their methods of operation which indicate the practical suitability of particular techniques for providing in principle the basis for ITS applications and systems to be compliant with privacy, data protection and security requirement of the EU regulatory framework.

([20]) For example, the retention of traffic data and of location data processed in connection with the provision of publicly available electronic communication services in public communications networks is regulated in Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

ITS services should be taken into account. While some data may be exchanged and processed on an anonymous basis, other data, even if exchanged on an unidentified basis, may be linked to data relating to identified individuals and will therefore constitute personal data in the meaning of Article 2(a) of Directive 95/46/EC ([21]). Given the purposes for which ITS will be used, it seems difficult to ensure that a large amount of the data gathered through ITS will be processed on an anonymous basis, as the identity of the individual will be needed at some point for specific purposes, such as invoicing. It would, as a result, at least take special — technical, organisational and legal — measures to ensure anonymity in certain domains.

III.1(b) *Interoperability, data quality and purpose limitation*

37. Interoperability of applications and systems is a core element for successful ITS deployment. Harmonisation work will be done through which the technical specifications of the interfaces to be integrated in applications and systems will be defined, in order to allow them to interoperate with other applications embedded in other transport modes and/or systems. While interoperability of systems will help facilitate the provision of a variety of services and will contribute to ensuring their continuity throughout Europe, it poses a certain number of risks from a data protection viewpoint, such as the risks of misuse or abuse of the data. Any interconnection of databases should be done with due respect for data protection principles ([22]) and practical safeguards on security (see also section III.1(c)).

38. The principle of data quality enunciated in Article 6(d) of Directive 95/46/EC is particularly crucial in the context of interoperability of applications and systems. The technical specifications to be defined for the design of the interfaces should ensure the accuracy of the data to be obtained as a result of the interconnection of applications and systems.

39. Given that the interoperability of systems will facilitate the interconnection of databases and the matching of data for further purposes, the EDPS emphasizes that any interconnection should be done with careful consideration of the purpose limitation principle set forth in Article 6(1)(b) of Directive 95/46/EC. It is particularly important that the design of ITS systems architecture prevents any further use of the data for other purposes than those for which they were collected. Appropriate security protections must be built in the system to prevent misuse, unauthorised disclosure or access, as well as collateral effects of devices. For example, sufficient protections should be implemented so that nomadic devices are not accessed by unauthorised third parties and are not used to identify and track people beyond the purposes of the system.

40. As to the lawfulness of the interconnection itself, this will need to be assessed on a case-by-case basis, taking account of the nature of the data that are made available and exchanged through the systems and of the purposes for which they are originally intended to be used.

III.1(c) *Security of data*

41. Security of personal data is a key element of ITS deployment. The EDPS welcomes the fact that security is explicitly mentioned in the action plan and in the proposal for a Directive. Security should be envisaged not only during the functioning of the ITS device (in the in-vehicle system and in the communication transport protocol) but also beyond the functioning of the device — in the databases where the data are processed and/or stored. Appropriate technical, administrative, and organisational requirements should be defined for all stages of the processing which ensure an adequate level of security in accordance with Articles 16 and 17 of Directive 95/46/EC (as well as Articles 4 and 5 of Directive 2002/58/EC, where relevant).

42. The definition of appropriate security measures should only be done after a careful assessment of the specific purposes for which ITS will be used and of the modalities of the processing has been done. In this respect, the EDPS recommends that privacy and data protection impact assessments are conducted in relation to particular sectors and/or purposes of use (e.g. for security-related ITS systems, for freight management systems, etc.). The conduct of a privacy and data protection impact assessment and the use of BATs for privacy and data protection will contribute to defining the most appropriate security measures relevant to the specific processing performed.

III.2. **Further data protection and privacy considerations for the provision of ITS services**

43. Further harmonisation of the modalities of deployment of ITS services is necessary at EU level in order to prevent discrepancies in the deployment of ITS services. In this regard, the EDPS would like to point out two issues that will notably require further consideration from a privacy and data protection viewpoint below:

— the use of location tools for the provision of location-based public and commercial services requires that additional safeguards are implemented. In such a context, particular attention should be paid to whether and when ITS location-based services are used for private purposes or for professional purposes, and how individuals using a vehicle in a professional context might be impacted by the use of such a system,

— it is particularly important in integrated systems that the roles and responsibilities of the different parties involved in ITS deployment are clarified.

([21]) See footnote 15.

([22]) See also comments of the EDPS on the Communication of the Commission on interoperability of European databases, 10 March 2006. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2006/06-03-10_Interoperability_EN.pdf

III.2(a) *Safeguards for the use of location tools for the provision of ITS location-based services*

44. The deployment of ITS will support the development of applications for 'tracking and tracing' of goods and will allow for the deployment of location-based commercial and public services. Such services will rely on the use of technologies such as satellite-based positioning and RFID tags ([23]). Navigation, tracking and tracing systems are intended to be used for a variety of purposes such as remote in-route monitoring of vehicles and cargo (e.g. for the transport of dangerous goods or living animals), invoicing vehicles on a variety of parameters including distance travelled and time of day (e.g. road pricing, electronic road toll systems), and monitoring drivers for enforcement purposes such as checking driving times (through digital tachographs) and imposing sanctions (through electronic vehicle identification).

45. The use of location technologies is particularly intrusive from a privacy viewpoint as it allows for the tracking of drivers and for the collection of a wide variety of data relating to their driving habits. As was stressed by the Article 29 Working Party ([24]), the processing of location data is a particularly sensitive matter involving the key issue of the freedom to move anonymously, and which requires the implementation of specific safeguards in order to prevent surveillance of individuals and misuse of the data.

46. The EDPS emphasizes that the use of location tools must be lawful, i.e. based on a proper legal ground, for explicit and legitimate purposes, and proportionate to the purposes to be achieved. The lawfulness of the data processing undertaken will much depend on the manner in which and the purposes for which location tools will be used. As the Article 29 Working Party underlined in its opinion on eCall, 'it would not be acceptable, from a data protection viewpoint, to have such devices permanently connected and vehicles thus permanently be trackable in view of the possible activation of eCall devices' ([25]). It is therefore important to clarify further the specific circumstances in which a vehicle will be tracked and its impact on the user. In any event, the use of location devices should be justified by a legitimate need (e.g. monitoring the transport of goods) and strictly limited to what is necessary for that purpose. Thus, it is important to precisely define which location data are collected, where they are stored and for how long they are kept, with whom and for which purposes they are exchanged, and to take all necessary steps to avoid any misuse or abuse of the data.

47. Furthermore, the processing of location data relating to users of public communications networks or publicly available electronic communication services is strictly regulated in Article 9 of Directive 2002/58/EC. It notably requires that processing of location data should be done on an anonymous basis, or otherwise upon informed consent of the user. This means that users must, prior to agreeing to the use of a location tool, be provided with appropriate information, including the type of location data processed, the purposes and duration of the processing, and whether the data will be transmitted to a third party for the purpose of providing the value added service. There must be a simple means, free of charge, for users to temporarily refuse the processing of location data for each connection to the network or for each transmission of a communication. The processing of location data should be strictly limited to persons acting under the authority of the provider of the public communications network or publicly available communication service or of the third party providing the value added service.

48. Additional safeguards must be adopted when location data are collected from vehicles that are being used in the course of professional activity, to prevent the location technology being used to unduly monitor employees. In any event, the processing should be limited to location data collected during the working time — thus employees shall be able to switch off the location function outside the working hours and/or when using the vehicle for private purposes.

49. There is a risk that third parties (such as insurance companies, employers, and law enforcement authorities) require access to data collected through navigation and tracking systems for legitimate and specified purposes (such as tracking of goods, electronic payment of toll, etc.) in order to use them for secondary purposes, such as checking driving times and rest periods or verifying compliance with road regulations and imposing sanctions. As a principle, access to the data for secondary purposes is not allowed if this access serves purposes which are incompatible with the ones, for which they were collected. Access can only be allowed by way of derogation to this principle if the conditions for such access meet the strict requirements of Article 13 of Directive 95/46/EC. As a consequence, any access to location data by third parties should only be provided in accordance with the law and in a transparent way, on the basis of a legal measure that sets out appropriate procedures and modalities for access to the

([23]) See the privacy and data protection issues raised by the use of RFID in the opinion of the European Data Protection Supervisor on the communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on 'Radio Frequency Identification (RFID) in Europe: steps towards a policy framework' COM(2007) 96, OJ C 101, 23.4.2008, p. 1. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-12-20_RFID_EN.pdf

([24]) Article 29 Working Party, Opinion on the use of location data with a view to providing value-added services, WP 115, November 2005. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_en.pdf

([25]) See WP 125 on eCall, p. 5, mentioned in footnote 10.

data for specific purposes, and that provides adequate safeguards to individuals in accordance with the further purposes for which their data could be used.

III.2(b) *Roles and responsibilities of ITS actors*

50. It is not yet clear who the data controller will be in respect of each part of the processing. In many cases, ITS service providers will likely be the controllers of the data, whether alone in respect of the personal data processed for the provision of their own ITS services or jointly in the cases where the processing is carried out together with other data controllers. Operators involved in ITS in different capacities should have their role and responsibilities, as data controller and as data processor, clearly specified in respect of each part of the processing (e.g. telecommunication operators providing communications services as well as ITS services).

51. Those persons acting as data controllers will be responsible ([26]) for ensuring compliance of the systems and services with all data protection obligations, and in particular for implementing systems that embed 'privacy by design', that respect data quality and purpose limitation principles, and that guarantee an appropriate level of security of the data, as described in III.1.

52. Data controllers will need to ensure that appropriate safeguards are put in place at all levels of the chain of actors involved in ITS deployment. This will notably require that they enter into appropriate contractual schemes with all stakeholders involved in the exchange and processing of data, which should provide adequate data protection safeguards (in particular in respect of Articles 16 and 17 of Directive 95/46/EC, and Articles 4 and 5 of Directive 2002/58/EC). It is important to note that from a data protection perspective, while data controllers must ensure that data protection is ensured at all stages of the processing, they remain responsible for the processing and cannot exclude their responsibility by contract.

IV. **CONCLUSIONS**

53. The EDPS welcomes the proposed ITS deployment plan put forward by the Commission that aims at harmonising the data processes throughout Europe in order to facilitate the provision of ITS services, and in which data protection is put forward as a core condition for the proper deployment of ITS in Europe.

54. The EDPS notes that the proposed Directive sets forth a general framework which raises a number of privacy and data protection issues that need to be further addressed at EU and national level:

— there is a risk that the lack of clarity of the proposed legal framework will create diversity in the implementation of ITS in Europe which will lead to different levels of data protection in Europe. The EDPS emphasizes the need for further harmonisation on these issues at EU level to clarify outstanding issues (such as definition of the roles and responsibilities of ITS actors, which specific ITS applications and systems must be embedded in vehicles, the development of harmonised contracts for the provision of ITS services, the specific purposes and modalities of use of ITS, etc.). It is particularly crucial to identify who the data controllers will be in respect of the data processing performed, as they will bear the responsibility to ensure that privacy and data protection considerations are implemented at all levels of the chain of processing,

— decisions concerning certain modalities of the processing that could seriously impact on the privacy and data protection rights of individuals should be taken by the European Parliament and the Council, and not through comitology procedure,

— it is paramount to consider privacy and data protection from an early stage of the processing and in all stages of the processing; the implementation of 'Privacy by design' should be encouraged for the design of ITS applications and systems, and should be incorporated within standards, best practices, technical specifications, and systems,

— any interconnection of applications and systems should be done with due respect for data protection principles and practical safeguards on security,

— in regard of the uncertainties that remain at this stage concerning the modalities of deployment of ITS, the EDPS particularly welcomes the initiative put forward by the Commission in its Communication that a privacy assessment be conducted by 2011. He furthermore strongly advises that privacy and data protection impact assessments are conducted in relation to particular sectors and/or purposes of use for the definition of appropriate security measures and that Best Available Techniques for privacy, data protection and security in ITS are developed,

— the EDPS further stresses that Member States will bear responsibility in implementing the Directive in a proper fashion so that ITS operators implement systems and services that offer an appropriate level of data protection across Europe,

([26]) See footnote 13.

— appropriate safeguards should be implemented by data controllers providing ITS services so that the use of location technologies, such as satellite positioning and RFID tags, is not intrusive of the privacy of individuals using vehicles in a purely private or in a professional context. This will notably require limiting the processing to the data strictly necessary for that purpose, ensuring that appropriate security measures are built in the systems so that location data are not disclosed to unauthorised recipients, and providing users with an effective means of deactivation of the location device/feature.

55. The EDPS recommends that Article 6 of the Proposal is amended, in line with Directive 95/46/EC, as follows:

— data minimisation should be encouraged for the data processing performed through ITS. In this view, it is recommended to amend Article 6(1)(b) of the Proposal as follows: 'Personal shall only be processed insofar as processing is necessary for the specific purpose for which ITS is used and pursuant to an appropriate legal basis',

— it is important that personal data processed through interoperable systems are not used for further purposes that are incompatible with those for which they were collected. It is therefore recommended to modify Article 6(2) as follows: 'and may not be used for purposes other than the ones for which they were collected in a way incompatible with those purposes',

— he recommends adding an explicit reference to the notion of 'privacy by design' for the design of ITS applications and systems in Article 6 of the Proposal. Moreover, he recommends that the Article 29 Working Party and the EDPS are informed about and consulted on further actions taken on this issue through the comitology procedure.

56. The EDPS further recommends that reference to this consultation be made in the recitals of the Proposal.

57. In consideration of the above, the EDPS recommends that data protection authorities, in particular through the Article 29 Working Party, and the EDPS are closely involved in initiatives related to the deployment of ITS, through consultation at a sufficiently early stage before the development of relevant measures.

Done at Brussels, 22 July 2009.

Peter HUSTINX
European Data Protection Supervisor