



European Economic and Social Committee Hearing on the Deployment
of Intelligent Transport Systems - Ostrava, 26 March 2009

Intelligent Data Protection for Intelligent Transport Systems

Giovanni Buttarelli

Assistant European Data Protection Supervisor

Introductory remarks

- I am glad to be here today and would like to thank the organizers for their invitation.
- I would like to start by briefly explaining why it is important that the EDPS is here today. The EDPS, now at the beginning of the second five-years mandate, is an EU independent authority with mainly three tasks: supervising the processing of personal data carried out by Community institutions and bodies (*supervision*); advising EU institutions on EU legislation having an impact on the protection of personal data, which may be proposals for legal instruments, but also communications and other measures (*consultation*); cooperating with other Data Protection Authorities, established both at national and European level, with a view to a more uniform application and enforcement of the EU data protection legal framework (*cooperation*).
- In the area of Intelligent Transport Systems, the EDPS consultation and cooperation roles are relevant. Indeed, the EDPS was formally consulted by the Commission on the ITS action plan and will soon present a document on

Postal address: rue Wiertz 60 - B-1047 Brussels

Offices: rue Montoyer 63

E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu

Tel.: 02-283 19 00 - Fax : 02-283 19 50

this subject. Furthermore, this is not the first time that the EDPS and national Data protection authorities deal 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 in May 2008, and, together with the WP29, a working document on E-call in September 2006. Recently, the EDPS has also provided informal comments on the text of a draft Commission decision on the European Electronic Toll Service and is contributing to a memorandum on road pricing drafted by the International Working Group on data protection in Telecommunications (which is likely to be adopted by the end of April).

- This close link between intelligent transport systems and data protection is not surprising. Intelligent Transport Systems are based on the growing use of emerging Information and Communication technologies, requiring the collection and processing of a massive amount of data. Therefore they constitute a data-intensive area. In many cases, these data are personal data, in the sense that they refer to identified or identifiable persons. Indeed, the concept of personal data is not limited to biographical information, but it does include, for example, information relating to the geolocalisation of persons, to the way they drive, to their use of telecommunications systems, to the sanctions they may be subject to.
- Therefore, also when dealing with objectives which are lawful and pursue an important public interest, like in the case at stake, it is crucial to determine how information should be used.

Relevant data protection principles in the area of Intelligent Transport Systems

- Against this background, I would like to highlight some data protection principle and aspects which may be particularly relevant in the context of Intelligent Transport Systems. These principles stem from relevant

European legislation, and in particular the "privacy" Directive 95/46 and Directive 2002/58 on privacy in telecommunications.

- Legal grounds for processing. Processing of personal data should be based on one of the legal grounds laid down by data protection legislation, inter alia the consent of the concerned person or a legal obligation with which the controller shall comply (Article 7 Directive 95/46/EC). Therefore, it is essential to clearly define whether the various processing activities stemming from the ITS initiatives will be carried out on a voluntary or mandatory basis, or on a combination of both (see WP29 E-call working document). A voluntary basis would entail that the user shall be in a position to freely give (and withdraw) his/her consent. A mandatory basis would entail that the obligation to process data is laid down in a legal framework which duly takes into account data protection principles. A mixed system would entail that certain processing activities are mandatory and other are subject to the opt-in of the user, for example with regard to additional services and features. In any case, even a system based on a legal obligation should duly take into account data protection. In this context, it is important to ensure as far as possible that users have a right to "switch off" their device.
- Purpose limitation principle. Purposes for which personal data may be processed should always be clearly defined, taking into account that the use for further incompatible purposes is possible only when specific circumstances are met. In principle, a massive retention of personal data "just in case", for example with a view to law enforcement purposes, should be excluded
- Data Minimisation/Necessity. Intelligent Transport Systems are "fuelled" by data - and, in particular, geolocalisation data - and could not exist without them. But the single features should be carefully analyzed according to the pursued purposes. In particular, with regard to the different transport systems, and especially in road transport, general information - such as traffic, accidents, opportunities - shall be distinguished from

specific information relating to individuals, and sometimes legal persons. If information is not selected accurately, there is the concrete risk of a massive and disproportionate collection of personal data. In this context, it is important to highlight that information relating to identifiable vehicles and plate numbers are personal data.

- Anonymisation. Pursuant to data protection rules, if personal data are not necessary - or are necessary only at an early stage -, they should not be collected or should be anonymised as soon as possible. If data are further used for statistical or market analysis purposes, they have to be anonymised. For example, when it comes to providing useful information to the public on the basis of aggregated data (such as alternative routes, traffic conditions, etc), it is necessary to cut the link with identifiable individuals, especially if one takes into account that aggregated data often stem from delicate information, such as telephone traffic and geolocalisation. In this context, it should be highlighted that the mere encryption of data does not amount to anonymisation, in so far as data can be referred to an identifiable individual.
- Proportionality. Processing activities should be proportionate to the purpose(s) pursued. This embraces a broad range of elements, such as the quantity and kind of data collected and exchanged, the storage periods, the modalities and architecture of the systems. For example, will the data be pushed from the user to the system or will they be pulled directly from the system? To which extent the data subjects will be in control of the exchange of data? Where will payment data be stored?
- Information to users. Users should be duly informed about the main elements of the processing activities and their rights. In particular, they should be informed whether (and which of) the processing of personal data is mandatory or voluntary and about the opportunities and the risks that may stem from the processing of their personal data. This information may be provided by means of a unique contract or through various contracts.

However, the latter option might entail the risk of fragmentation, i.e. that users lose sight of the general picture about how their data are processed

- Data subjects' rights: some basic rights for the users of the system should be ensured, such as the right to have access to their personal data, to have them rectified, or to object to their processing in certain cases.
- Security of the information is also a key element, and I am glad to see that data security is explicitly mentioned in the Action Plan. Security means not integrity of the system, but also availability of information and stability of the system. In this context, it is important to ensure security not only during the functioning of the system (i.e., when a car is circulating on a road), but also beyond the functioning of the system (by preventing misuse and collateral effects of devices: ensuring, for example, 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)
- With regard to guarantees, some information may have a "neutral" nature, while other information, even if not sensitive, may entail a prior checking by the competent data protection authority, since it reveals where are people, how they use transport systems or even whether certain individuals should be subject to sanctions, such as fines.

Conclusions

When considering the ITS Action plan, the EU legislator, including the Economic and Social Committee, have a unique occasion to take into account data protection principles and thus to develop a successful vision for the deployment of Intelligent Transport Systems in Europe. A long-term vision, which takes into account not only currently available applications, but also possible future developments of the systems.

It is therefore important to profit from this occasion to determine at an early stage the architecture of the system infrastructure, the flows of data (vehicle to infrastructure and vehicle to vehicle), the categories of data and the purposes

for which they are used, the modalities of processing information, the retention period of data, the possible reuse of information as well as the role of the different actors within the envisaged systems. This is particularly important in integrated systems in which it's necessary to clarify roles and responsibilities, for example with regard to the different providers contributing to the system and how they shall ensure the security of the network.

Therefore, it is paramount to consider privacy issues from the very beginning when defining the architecture of the Intelligent Transport Systems ("privacy by design") as well as when implementing the system. Furthermore, the use of privacy enhancing technologies (PETs) should be promoted.

In this context, I recommend that data protection issues are addressed in further details at EU level, by providing adequate guidance, with regard to the application of data protection principles to Intelligent Transport Systems. Otherwise, different national interpretations and unsolved cross-border data protection issues may hinder the deployment and the interoperability of the envisaged system.

If privacy principles are disregarded, there are high risks, not only of incompliance with law, but also of misuse of the system, and ultimately loss of consumer trust. Here it is at stake also the freedom of movement, interpreted in a dynamic form as being free to move without leaving a permanent trace and thus loosing the right to move anonymously.

Data protection is not an obstacle to an efficient exchange of information, as the experience of the data protection community has shown so far with regard to the use of Information and Communication technologies in other contexts, such as internet and the use of mobile phones. The EDPS wants to contribute constructively to the efficient and lawful use of ICTs in the transport sector.

However, the deployment of Intelligent Transport Systems cannot result in users loosing their right to move anonymously.

Therefore, I want to stress that duly taking into account data protection in the architecture and the implementation of the system is a key element of success for ITS projects: Intelligent Transport Systems need Intelligent Data Protection.