

CLECAT - 9th Freight Forwarders Conference

Brussels, 3 December 2009

"Intelligent transport systems and data protection - ensuring the right balance between the protection of privacy and the efficient use of ICT in logistics"

Peter Hustinx

European Data Protection Supervisor

Ladies and Gentlemen,

Let me first thank the organizers for inviting me to this conference. Today's discussions on how to deal with technological innovation in the field of freight transport logistics and customs touch on many of the challenges with which operators are faced. Among these challenges, there are also some in the area of privacy and data protection, and this is the reason of my presence here.

Please note that the European Data Protection Supervisor is *not* a part of the European Commission. His first task is, after all, to monitor and ensure that the Commission and other European institutions and bodies comply with data protection rules that also apply in the Member States. Other tasks are to advise the Commission, the Council and the European Parliament on proposals for legislation that have an impact on the protection of personal data, and to cooperate with national supervisory authorities in order to ensure a consistent data protection in the European Union.

In recent years, I have been consulted by the European Commission on a number of legislative initiatives in the field of transport which involve the use of Information and Communication Technologies (ICT) - for example in the field of road transport, road safety, and recently on Intelligent Transport Systems. Various initiatives in the customs field have also been on my agenda.

In my opinions on these initiatives, I have outlined a number of data protection and privacy concerns. Some of these challenges must be addressed by the legislator; others

must be taken into account by stakeholders before implementing data processing systems. I will highlight a few in my contribution.

Looking more specifically at your business sector, it is clear that the growing use of ICT in the field of freight transport logistics and customs services is rapidly changing the way in which logistics and customs service providers operate. These new developments are welcome as they help to improve and facilitate the provision of logistics and customs services. But they also raise a number of issues for operators.

One of these concerns is the risk of undue monitoring and misuse of personal data, if the implementation and use of ICT is not done in a manner compliant with privacy and data protection rules. I will therefore focus in my remarks on the importance of **reaching a right balance** between the efficient use of ICT in logistics and customs and the protection of citizens' privacy.

First of all, I would like to recall that it is a **legal obligation** for operators to comply with the data protection legal framework when processing and exchanging personal data. This legal framework exists both at European and national level with two main purposes. First, it ensures a high level of protection for everyone in the European Union, and secondly, it ensures a level playing field for operators, when they are active anywhere in the European Union.

The right to privacy and the right to protection of personal data are fundamental rights that have received explicit recognition in the Lisbon Treaty, which as you probably know entered into force only a few days ago.

This is also increasingly relevant in your sector. For instance, fleet management systems allow for the processing of a wide variety of data. While most of these are commercial and related to business activities, a number of them also relate to individuals who may be involved in the course of their professional activity.

These data may concern truck drivers, legal representatives and contact persons of any operator involved in the logistics and customs services chain. When data about individuals are concerned, the collection and exchange of these data fall within the scope

of data protection law. Their processing must be guided by a number of data protection principles, which I will now briefly highlight.

I. Data protection principles that must guide the introduction of ICT in the field of transport logistics and customs services

These principles stem from relevant European legislation and in particular the Data Protection Directive 95/46/EC and the e-Privacy Directive 2002/58/EC. It is crucial that these principles are carefully taken into account at an early stage of the design of the processes so that they can be built into the systems. Flexibility is highest at an early stage of development and adequate attention at that stage will help find better solutions. In any case, you should avoid seeing this as an issue to be dealt with by your legal department in order to fix some paperwork at the end.

- First, before implementing any system, it is essential to assess the **legitimacy** and the **necessity** of the data processing. Personal data should only be collected for specified, explicit and legitimate purposes. This must be determined carefully by the responsible persons in an organisation that wants to implement a data processing system.
- The processing must be based on a valid **legal basis**. Sometimes the legislator will impose the collection and processing of data, the details of such processing will be explicitly stated in the law. In other cases where operators themselves initiate a processing, they must often seek the explicit consent of the individuals concerned. There are other options, but they require careful thought.
- Who is the **data controller**? It is important to determine who is responsible and accountable for the processing. It is the data controller who will bear the responsibility of ensuring that the system works properly from a data protection perspective. In many cases, this role will be for the operator as a legal entity, but it is important to organise this internally in a practical sense. In some cases, the customs authorities will be data controller, which raises the issue of the borderline or interface between your and their responsibility.

- The processing must be **proportionate** to the purposes to be achieved. This embraces a broad range of elements, such as the quantity and type of data collected and exchanged, the storage periods, the modalities and architecture of the systems. This must be assessed in concrete terms in view of all parameters.
- **Data minimisation**: only the data that are strictly necessary should be processed. General information - such as information on traffic and transit of goods - should be distinguished from specific information relating to individuals. If information is not selected appropriately, there is a risk of a massive and disproportionate collection of personal data.
- The exchange of data must be guided by the "**purpose limitation principle**": data should only be processed for further purposes that are compatible with the purposes for which they were collected. A number of technical and administrative **security measures** must be adopted to prevent against any misuse of the data. These measures should ensure that data are not further accessed by unauthorised third parties or for purposes that are incompatible with the original ones.
- **Data subjects' rights**: the data controller must ensure that individuals concerned are duly informed about the main elements of the processing and their rights to have access to their personal data and to have them rectified.
- Finally, the issue of **external oversight**: for instance, the data controller must verify whether the data processing is subject to prior checking by the competent data protection authority, in which case he must notify the details of the processing to the competent authority so that it can take place.

II. Assessment of the privacy risks posed by the technologies used and the need for "Privacy by Design" in the development of the systems

Some technological developments pose specific privacy concerns. A number of technologies that are increasingly being used for logistics and customs services, such as RFID, satellite-based-localisation systems and digital tachographs, have great privacy impact. These technologies are all promising in terms of improving logistical processes, but they have great impact on individuals' privacy if used to monitor their behaviour.

Indeed, they may be used not only to track vehicles and goods but also to monitor drivers' driving habits and compliance with working hour requirements or with road regulations.

To avoid building systems that are intrusive to the privacy of individuals, it is particularly crucial that adequate measures are taken before implementing such systems so that they do not result in undue surveillance of individuals. The specificities of the technology used must be taken into account.

This will notably require carrying out a privacy and data protection impact assessment in order to identify potential threats. As a result of such impact assessment, the data controller will be able to define the most appropriate safeguards and security measures that must be built into the system to guarantee that it is not violating privacy.

As part of my advisory role with regard to new policies and legislation, I have provided guidance on many occasions, on how systems integrating these technologies should be designed so that they are privacy friendly. For example, I provided recommendations on RFID in December 2007, which were fully integrated in the Recommendation of the Commission adopted in May of this year concerning the implementation of privacy and data protection principles in RFID applications.

With respect to the use of localisation tools and digital tachographs, I want to refer to the Opinion adopted in July 2009 on Intelligent Transport Systems, which you can find at the EDPS website. I also want to mention the guidance of the Article 29 Working Party and in particular its opinion 5/2005 on the use of location data.

To illustrate this point, let's look at an example of processing relying on geo-localisation technologies. Adequate measures adopted by the data controller in this case would notably include specifying the specific circumstances in which a vehicle will be tracked, how the use of the data is limited to what is strictly necessary for that purpose, and what security measures are adopted in order to ensure that location data are not disclosed to unauthorized recipients. In addition, the data controller should provide appropriate information to users on the details of the processing done and on the impact of the use of specific technologies on their privacy.

As underlined before, I strongly encourage operators to design systems that are compliant with privacy and data protection requirements from a sufficiently early stage of the development of the systems. This is the so-called concept of "Privacy by Design", which helps define the architecture, operation and management of ICT systems at all stages of the processes. Logistics and customs operators should not wait until the implementation of the systems to do so, or they will have to face the burden and costs of having to fix their systems at the most crucial moment, when they were supposed to go live.

Conclusion

As a conclusion, I would like to stress how important it is that the rules and practices of the Member States in this context are sufficiently harmonised in practice in order to allow a level playing field for operators and to avoid undue bureaucracy and costs.

Sufficient harmonisation of the processes and safeguards across Europe is also needed to ensure that the many benefits offered by these systems are not hampered by a lack of compliance with essential safeguards for data protection.

If privacy principles are disregarded, there are high risks, not only of a lack of compliance with the law, but also of misuse of the systems and ultimately loss of trust from business partners and individuals concerned.

Thanks for your attention.