Data Retention Conference: "Towards the Evaluation of the Data Retention Directive", Brussels, 14 May 2009

"Ensuring the Right Balance between Law Enforcement and Data Protection"

Peter Hustinx
European Data Protection Supervisor

I welcome the opportunity to contribute to this conference on the implementation of the Data Retention Directive, with some introductory remarks from the point of view of privacy and data protection.

To focus your attention, let me share with you right away the 'bottom lines' of my remarks. These are essentially two main points:

- First, the need to ensure the *right balance* between the needs of law enforcement and the requirements of data protection;
- Second, the need to ensure the existence of an *effective protection in practice.*

Let me explain what I mean with these two points in the context of this discussion on the implementation of the Data Retention Directive.

There should be no doubt that the retention of traffic and location data in accordance with the provisions of the Directive is a substantial interference with the right to the respect for private life and correspondence as guaranteed in Article 8 of the European Convention on Human Rights. It is clear from the case law of the Strasbourg Court that the safeguards of Article 8 also apply to traffic and location data relating to any kind of protected communication.

The retention of these data for law enforcement purposes, beyond what is necessary for communication purposes, without consent of the person concerned, is an exception to the strict rules on the deletion of such data that applied before and were

intended to protect the privacy and confidentiality of communications. So much is clear from the history of the Data Retention Directive itself.

This starting point of analysis has a number of consequences that continue to be relevant today.

It means that both the Directive itself and the national legislation implementing it should meet the conditions laid down in Article 8 for a lawful restriction of the right to respect for private life and correspondence: any such restriction should be '*in accordance with the law*' and '*necessary in a democratic society*' for a legitimate purpose, such as for example the prevention or repression of crime.

The first condition - '*in accordance with the law*' - does not only require a formal legal basis, but one that meets certain quality criteria, such as clarity, precision, predictability and existence of adequate safeguards against possible abuse. The case law of the Strasbourg Court is clear about these requirements (see Liberty and others v. UK, July 2008).

The second condition - '*necessary in a democratic society*' - is perhaps even more relevant in this discussion. It means that a measure should not only be useful, but *necessary* and *proportionate* in a democratic society to satisfy a pressing social need. The case law of the Strasbourg Court is also very instructive about what this means (see in particular the Grand Chamber judgment in S. and Marper v. UK, December 2008).

It is an interesting and still open question whether the Directive fully satisfies these requirements, seeing the political pressure under which it was adopted, the limited explanations in the preamble and the wide margins for implementation left to the Member States. However, the national legislation under the Directive should of course also meet these requirements. And so should the national practice under the wide diversity of national laws that now is emerging.

I would not be surprised if this situation would give rise to interesting court decisions, including eventually from both the Luxembourg and the Strasbourg courts. In fact, as you all know, decisions of national courts on these issues are already in the pipeline.

Let me emphasize, in this context, that the evaluation of the Directive should throw light on the *necessity* and *effectiveness* of these measures. That means for instance that not only statistics on numbers of cases in which access was provided to retained data, but more substantive evidence will be required.

That brings me to a second set of remarks, which I can conveniently link to the recent judgment of the European Court of Justice in the case of Ireland v. Parliament and Council (February 2009). The first and most obvious point is of course that the Court has confirmed that the Directive was adopted on a correct legal basis.

A second point is that the Court explicitly stated that the action brought by Ireland related *solely* to the choice of legal basis and not to any possible infringement of fundamental rights arising from interference with the exercise of the right to privacy contained Directive 2006/24 (see paragraph 57). This is why that question is still essentially open.

A third point is that the Court has analysed the Directive as an *exception* to Article 15 of the e-Privacy Directive, but also as a *specification* of both the e-Privacy Directive and the general Data Protection Directive. That means that the implementation of the Data Retention Directive at the national level should also fully take into account the relevant requirements of these two other Directives.

Most of all, this means that there should be *adequate* and *effective* safeguards that retained data are *not* accessed or otherwise used for *other* purposes than those for which the obligation to retain these data was introduced. The arrangements under which these communication data may be stored in practice could lead to particular challenges, including different issues of centralised storage and storage in another Member State, and in the latter case issues of applicable law and diverging national requirements.

This is why, more in general, it is crucial that the applicable national law ensures a fully adequate and effective data protection in the business reality of telecom and internet providers and in the way access for law enforcement is implemented and provided in practice.

If the risks of security breaches or irregular or unlawful conduct is underestimated, there can be little doubt that both breaches and irregular conduct will happen in practice and that this will certainly undermine the legitimacy and credibility of data retention, also where it would be fully justified.

I am sure you know that the Article 29 Working Party with representatives of all data protection authorities is currently undertaking a joint investigation into the way the Data Retention Directive has been implemented in practice. There will also be in-situ inspections as part of this exercise. The results of this joint investigation will hopefully contribute to a more complete picture for the evaluation of the Directive.

The same applies essentially to the activities of the experts group in which we take part, and hopefully also to the results of this conference.

With these brief remarks, let me wish you a very useful discussion that will contribute to greater clarity, more specifically about the issues that I have mentioned.