Conference "Taking on the Data Retention Directive"
Brussels, 3 December 2010

"The moment of truth for the Data Retention Directive"

Peter Hustinx
European Data Protection Supervisor

Today we are discussing the *notorious* Data Retention Directive. As you all know, the adoption of the Directive was not warmly welcomed by all citizens and in all Member States.

We have been following the creation, implementation and evaluation of the Directive since 2005 in different ways: First as advisor to the legislator when the Directive was discussed. We were also involved in the data retention Expert group and participated in the Article 29 Working Party, which published a rather critical report about how the Directive was applied in practice, in July 2010. Finally, we intervened in the case before the Court of Justice about the legal basis of the instrument.

During those years, I have repeatedly emphasised the "huge impact" the Directive has on the application of data protection principles and its "substantial interference" with the rights to privacy and protection of personal data.

Let me underline this today once more: retaining communication and location data of all persons in the EU, whenever they use the telephone or the internet, constitutes a huge interference with the right to privacy of all citizens. The Directive is without doubt the most privacy invasive instrument ever adopted by the EU in terms of scale and the number of people it affects.

It goes without saying that such a massive invasion of privacy needs profound justification.

This justification is not established if the retention of all such information is only considered "a useful tool" for law enforcement authorities or if it just "helps" solving serious crimes. Current European law – including the Charter of Fundamental Rights - requires that the retention of such data is proportionate and strictly necessary for the purposes envisaged by it.

Strictly necessary means that the purposes of the privacy invasive measure can only be reached by applying that specific measure. A measure is not strictly necessary if the same or comparable results can be achieved by less-privacy intrusive means. The European Courts in Strasbourg and Luxembourg have been very clear on this point.

It is still highly doubtful whether the systematic retention of communication data on such a wide scale constitutes a strictly necessary measure. Alternatives which are less privacy intrusive, taking a targeted approach, have always been available.

The issue is in fact not whether access to *some* telephone and internet data may be necessary in the combat of serious crime, but whether this requires that traffic data of *all* citizens are retained routinely for periods up to two years?

In my opinion of 2005 on the proposal for a Directive, I insisted among other things on the obligation to evaluate the instrument. In my view this evaluation is crucial.

This is where we stand today. The evaluation, based on concrete numbers and figures, should consider the necessity of the instrument. At the moment, the Directive is only based on the *assumption* that it constitutes a necessary and proportionate measure. However, the time has come to actually provide sufficient evidence of this.

Without such evidence, the Data Retention Directive should be withdrawn or replaced by a more targeted and less intrusive instrument which does meet the requirement of necessity and proportionality.

To put if differently: the evaluation which is now about to take place is the moment of truth for the Data Retention Directive.

I find it quite interesting that the Commission was not able to meet the deadline of 15 September. Apparently, the Member States, many of which are represented today, were unable to come up with sufficient evidence in time. This is rather strange, as the Directive has been in force for several years now, and the law enforcement authorities have a clear interest to carry out such an analysis.

Of course, I will approach the evaluation with an open mind, but I have my doubts whether we can expect convincing evidence of the necessity of retaining data on such a large scale. Quite a few jurisdictions in the world seem to survive without it.

However, the evaluation might also serve another purpose. Concrete facts and figures presented in the report will enable us to assess whether the results presented in the evaluation could indeed have been achieved with less privacy intrusive means.

I am pleased to see that the important question about alternatives is on today's agenda, although a bit hidden in the first subject of Seminar 1 "purpose".

Let me now turn to the Directive itself.

Time does not allow me to present a thorough analysis of the different provisions of the Directive. Therefore, I would like to focus on the fact that the Directive failed to harmonise national legislation which has led to legal uncertainty for the citizens. It also resulted in a situation where the use of the retained data is not strictly limited to the combat of really serious crimes.

The Article 29 Working Party, in its report of last summer, found that there are 'significant discrepancies' between the implementation and application of the Directive in the different Member States.

In my view, these discrepancies are a consequence of the Data Retention Directive itself. Differences are in fact due to a number of weaknesses:
- the explicit possibility to have diverging implementing laws. The Directive, for example, leaves an unacceptably wide choice of retention period;
- the use of notions which are not clearly defined, such as 'serious crimes' or 'competent national authorities';
- the absence of rules on certain issues, such as the recovery of costs.

But the most worrying problem is that there is a loophole in the legal framework. Let me briefly explain.

The Data Retention Directive derogates from the obligation in the e-Privacy Directive to delete traffic data when it is no longer needed for the commercial purpose it was collected for. On the basis of Article 15 of the e-Privacy Directive, Member States can derogate from this obligation for law enforcement purposes. The objective of the Data Retention Directive is to harmonise the use of this derogation.

The obligation under the Data Retention Directive serves the purpose of investigating, detecting and prosecuting serious crimes. The Article 29 Working Party found that *in practice* the Data Retention Directive is not considered an exhaustive instrument.

To put it simple: Member States believe that they are still free, under Article 15 of the e-Privacy Directive, to put in place retention obligations for other reasons which are not covered by the Data Retention Directive: for instance, for the *prevention* of crime or for *other* than serious crime. The data which are retained under the Data Retention Directive can in this way be used for purposes that are not foreseen by that directive.

In my view, the possibility of such an interpretation undermines the purpose of the Data Retention Directive - an *internal market* instrument - which intends to create a level playing field for business, based on an equal and effective level of protection of the privacy of citizens and other users across the EU.

The Directive, as the basis for such large scale privacy intrusive measures, should be clear about its scope and create legal certainty for all users. It should be assured that the purpose limitation of the Data Retention Directive is not circumvented.

Of course, when implementing the Data Retention Directive, it is up to the Member States to assure that this is done in a way which respects fundamental rights. This is rightly emphasized in the ruling of the German *Bundesverfassungsgericht* which has put strict conditions on the German implementing law. However, users in *other* Member States should *also* enjoy a similar high level of protection.

Moreover, and this is another important shortcoming, the Directive tells only half the story. Rules on access to and further use of the data are not contained in the Directive.

Citizens must be in a position to trust that the EU legislator – where the retention of data is necessary - not only provides for adequate safeguards for such retention by the telecoms operators, but also for the use of these data by law enforcement authorities.

The Lisbon Treaty has brought about important changes in EU law. To a large extent, it did away with the pillar structure and created a single legal basis for legislation on data protection in Article 16 of the Treaty on the Functioning of the Union. It is now the time to also do away with "old pillar" thinking in "closed boxes".

In my view, an EU instrument containing rules on obligatory data retention should also contain rules on access and further use by law enforcement. I therefore count on the Commission not to propose any new instrument without specific rules on access and further use of the data, especially since the Lisbon Treaty has abolished legal and political obstacles.

Let me conclude.

The evaluation we are now waiting for is the moment of truth for the Data Retention Directive. Evidence is required that it really constitutes a necessary and proportionate measure. Without such evidence, the Directive should be withdrawn or replaced by an instrument which does meet the requirements of necessity and proportionality.

The Directive has clearly failed to harmonise national legislation. A new or adjusted EU instrument should be clear about its scope and create legal certainty for citizens. This means that it should also regulate the possibilities of access and further use by law enforcement authorities and not leave any room for Member States to use the data for additional purposes.