Conference on European Data Protection Law

Delegation of the Bars of France, Brussels, 15 March 2013

Peter Hustinx

European Data Protection Supervisor

"Data Protection and Criminal Justice - The view of the EDPS"

I am pleased to be able to speak at this conference. The subject of today's event is an excellent example of the gradual evolution of European law and the way in which it interacts with national law. The subject is also very timely in view of the reform of the EU legal framework for data protection, which is now being debated in Parliament and Council.

Role of EDPS

Let me first briefly explain my role. The European Data Protection Supervisor (EDPS) is an independent authority at EU level, such as the CNIL in France. It has three main tasks:

- 1) monitoring EU institutions and bodies, when they are processing personal data, to ensure they comply with data protection principles;
- 2) advising the Commission, the European Parliament and the Council on new legislation that may have an impact on the protection of personal data, and
- 3) cooperating with national supervisory authorities, such as the CNIL and similar bodies in other member states, to improve consistency of data protection in the EU.

The supervisory task is perhaps less relevant today, but in view of the special focus in this part of the conference, let me mention that we also supervise EU bodies with a very clear link to criminal justice, such as the Anti-Fraud Office (OLAF). We also have an increasing role in the "Area of Freedom, Security and Justice" (AFSJ), which involves both immigration and asylum, and cooperation in the field of police and criminal justice.

The other two main tasks are more relevant today. That applies, first of all, to our advisory role in the context of the proposals for a General Data Protection Regulation and a separate Directive for data protection in criminal law enforcement. But more generally, a very large part of the legislative proposals on which we have advised over the last eight years, related to criminal law enforcement, either directly or indirectly. That also includes the Data Retention Directive which was discussed by the previous speaker.

However, the cooperation with national supervisory authorities is also relevant. For instance, together with them, we ensure a coordinated supervision of large scale information systems in the AFSJ, where the member states and the Commission both play an important role. This model will soon also apply to the second generation Schengen Information System (SIS II).

Lisbon Treaty

It is important to also mention the Lisbon Treaty: first of all, because it put a strong emphasis on fundamental rights. Due to the entry into force of the Lisbon Treaty, at the end of 2009, the EU Charter of Fundamental Rights is now a binding instrument, not only for EU institutions and bodies, but also for the member states, when acting within the scope of EU law. This also applies to Articles 7 and 8 of the Charter on privacy and data protection, to which I will come back in a minute.

The Lisbon Treaty is also relevant, because it introduced a general legal basis for "rules on data protection" in Article 16 of the Treaty on the Functioning of the European Union. This provision now serves as the basis for the current review of the EU legal framework on data protection, also in areas involving the former "third pillar" of the EU.

A third reason to mention the Lisbon Treaty is to underline that the Treaty changed the roles of the Commission and the European Parliament in the adoption of rules relating to the former "third pillar" of the EU. This means that the European Parliament is now a fully competent part of the EU legislature, also in policy areas affecting criminal law enforcement, as in the case of data protection.

Privacy and data protection

Article 7 of the Charter contains a right to the *respect* for everyone's private and family life, home and correspondence, which closely resembles Article 8 of the European Convention on Human Rights (ECHR). This is a classic fundamental right, which is directed against any

interference with private life, except when such interference is provided for by law and is necessary in a democratic society for a carefully defined legitimate purpose. These criteria are the basis for a now well developed case law of the European Court of Human Rights in Strasbourg on the scope of private life, the quality of a law providing for interference, the necessity and proportionality of such interference, and the need for adequate safeguards against any possible abuse.

Article 8 of the Charter contains a right to the *protection* of personal data, which confirms and consolidates the legal development in Europe over the last few decades. The concept of data protection was introduced in 1981 in a Convention of the Council of Europe (Convention 108), which was designed to provide structural safeguards in an Information Society that was likely to become more dependent on the use of information technologies. This Convention has been ratified by 44 countries, including all EU member states. It still contains the basic principles of data protection, regardless of their nature or context. The Convention also served as the basis for the current Data Protection Directive 95/46/EC, although the Directive further specified it in many ways.

The same basic principles for data protection are now also visible in Article 8 of the Charter:
- personal data must be processed fairly, for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law;
- everyone has the right of access to data which has been collected about them, and the right to have it rectified, and
- compliance with these rules shall be subject to control by an independent authority.

Relevance for law enforcement

This legal background is worth recalling here today, not only to emphasize the difference in character between the right to *respect* for private life in Article 7 of the Charter, and the *protection* of personal data in Article 8, which is more like a "system of checks and balances", consisting of rights and obligations, procedures and institutional oversight. It is also extremely relevant because of its consequences for criminal law enforcement.

First, it means that any special legal powers for criminal law enforcement or any practical arrangements with a view to such enforcement, which interfere with the right to respect for private life, will have to comply with the requirements of the case law of the European Court of Human Rights under Article 8 of the European Convention on Human Rights. These

requirements will now - very likely - also be applied by the European Court of Justice in Luxembourg under Article 7 of the Charter.

Secondly, it means that the general principles for data protection referred to in Article 8 of the Charter also apply to data protection in the area of criminal law enforcement, unless it is clear that the specific interests at stake in this area require that an exception is made from those principles. This will of course be subject to convincing arguments.

Moreover, any provision of data protection law in this field that interferes with the respect for private life, should meet the same requirements as any other interference with that right. In other words, it should be clear, precise and predictable, and both necessary and proportionate for the legitimate interest at stake.

So, let us now look at the specific subjects under discussion today. In that context, let me first make a few remarks on the Data Retention Directive, and then on the review of the EU legal framework for data protection.

Data Retention Directive

The Data Retention Directive, adopted in March 2006, has been controversial from the very beginning. It requires all providers of electronic communication services to store traffic and location data of the communications of *all citizens*, for a period between six months and two years, for possible use for law enforcement purposes. This is a clear example of a measure that *interferes* with the right to private life and would need a convincing justification.

However, the EDPS Opinion issued in September 2005 on the Commission proposal was one of the first opinions to come to a *negative* conclusion. It concluded that both the necessity and the proportionality of the proposed measure were doubtful and that there was also a clear lack of adequate safeguards. Yet, in view of terrorist attacks in Madrid and London, the proposal was adopted, without major changes, after a fairly short legislative procedure.

It did not come to me as a surprise, that the implementation of the Directive at the national level would give rise to problems. In some member states, there has been a reluctance to adopt a national implementing law. In others, a decision was made for the shortest possible period of retention. However, the national law was still criticized in constitutional courts in a number of member states. At this stage, there have been at least three requests from national

courts for a preliminary ruling of the European Court of Justice on the compatibility of the Directive with the Charter of fundamental rights.

I have emphasized publicly that the evaluation of the Directive must be seen as *the moment of truth*. After some years of experience with data retention in practice, it should be possible to provide some convincing evidence to illustrate how important and effective the measure has been for law enforcement. However, it was surprising to see that it was actually *very difficult* for the Commission to collect *any* reliable evidence *at all* from the member states.

Evaluation report

After a careful analysis of the evaluation report, presented by the Commission in April 2011, we have concluded that the Directive does *not* meet the requirements of the fundamental rights to privacy and data protection, mainly for the following reasons:

- the necessity for data retention as provided for in the Directive has still not been sufficiently demonstrated;
- data retention could have been regulated in a much less privacy-intrusive way, and
- the current Directive leaves too much scope for member states to decide on the purposes for which the data might be used, and who can access the data and under which conditions.

The evaluation report was to play a role in possible decisions on the future of the Directive. In our view, the Commission should seriously consider all options, including the possibility of repealing the Directive, whether or not combined with a proposal for another, more targeted EU measure.

If, on the basis of new information, the necessity of an EU instrument on data retention would be demonstrated, we think that three basic requirements should be respected:

- it should be *comprehensive* and genuinely harmonise rules on the obligations to retain data, as well as on the access and further use of the data by competent authorities;
- it should be *exhaustive*, which means that it has a clear and precise purpose which cannot be circumvented, and
- it should be *proportionate* and not go beyond what is necessary.

However, the Commission seems to have postponed any decision to an uncertain date. This means that the Court of Justice may very well be the first to decide on the future of the Directive and on the conditions that may apply to a possible revision.

Data Protection Review

In the context of the current review of the EU legal framework for data protection, we have warmly welcomed the Commission proposals presented in January 2012. This applies more specifically to the Data Protection Regulation, which makes a huge step forward in providing more effective and more consistent data protection in a world which is increasingly driven by the use of information technology in all fields of life. More and more citizens are now almost permanently on line, and they do need such more effective and more consistent protection.

However, we have also mentioned that the proposals are less comprehensive than they should have been. First, they do not apply to the EU institutions and bodies themselves, but this will probably come as a further step. Secondly, they do not affect specific legislation, such as the e-Privacy Directive on electronic communications, which has a link with the Data Retention Directive, but this may also come as a further step.

Thirdly and more importantly, there is an obvious lack of balance between the proposed Data Protection Regulation and the proposed Directive for criminal law enforcement. First, there is the obvious difference in instruments, which will leave more discretion to member states in an area where the protection of private life and personal data is most critical, and where the need for cooperation between member states is also growing.

However, the most important problem is that the level of protection in the proposed Directive is much lower than in the proposed Regulation. This can be illustrated in many ways, but also in that law enforcement authorities - unlike other authorities and private business - would not have a general duty to demonstrate compliance with data protection requirements. Moreover, the powers of supervisory authorities would be much more limited. This is a negative signal and a missed opportunity to inspire trust and confidence in law enforcement.

The EDPS opinion on the reform proposals has therefore suggested a series of improvements to ensure more balance and consistency between the two proposals. This is important not only for citizens, but also for all public services at or around the borderline between the Regulation and the Directive. One of the problems is that data exchange between both sectors is growing and a lack of balance and consistency may have negative effects for all stakeholders.

The Article 29 Working Party has recently raised another important issue: the extent to which law enforcement authorities would be allowed to store and keep personal data on individuals which are completely *unrelated* to a particular criminal investigation or prosecution (in other words: who are no suspect, witness or victim). The current language of the proposed Directive leaves the categories of persons on whom personal data may be collected and processed fully open.

This is a good example of a data protection provision which interferes with the respect for private life and which should therefore meet the relevant requirements, in other words be clear and precise, and both necessary and proportionate. The WP29 has come up with more precise language for this very sensitive subject.

We were very pleased to see that the European Parliament is considering amendments which will bring considerable improvements to the proposed Directive, and we will look forward to the negotiations between Council and Parliament with great interest.

Closing remarks

Let me finally also make another point, as this event is hosted by a professional association of attorneys with a clear interest and a professional duty to contribute to the further development of the law, including the law on data protection.

I would agree in principle with the next speaker, that attorneys could play a useful role as an external data protection officer. This may be an area of growth in the near future, also in view of the new Regulation. However, there are also other options. In that context, I would like to argue for a more active role of attorneys in exploring the rights of data subjects and the legal effects of data protection in practice.

As data protection is a cross-cutting subject, this may involve different areas of legal practice, ranging from employment to competition, and certainly also including criminal procedure. If data protection is made more effective in practice, it will also have an impact on litigation and attorneys will be on different sides of the debate.

On that note, I would like to thank you for your attention and will be looking forward to an interesting debate.