

"Data Protection in the Light of the Lisbon Treaty and the Consequences for Present Regulations"

Peter Hustinx

European Data Protection Supervisor

Ladies and gentlemen,

My colleague, the Federal Data Protection Commissioner, Peter Schaar elaborated in his speech on the need to keep data protection up-to-date and fully effective in a changing world. My contribution will deal with the same subject, but from a somewhat different perspective. I will go into the development of data protection in Europe, more precisely from the perspective of the European Union after the possible adoption of the Lisbon Treaty.

1. Important developments

These are interesting and challenging times, and important developments are also taking place on the EU-level. On the institutional level, I could mention the elections for the European Parliament which are still fresh in our minds. Moreover, a new European Commission will probably be appointed later this year. It is of course difficult to predict what impact these institutional events will have on the protection of personal data in Europe.

I would therefore like to focus on other developments that are likely to have more direct consequences for the development of data protection in our part of the world.

- On 19 and 20 May the European Commission has organised a conference on the protection and use of personal data. This conference gave all the stakeholders the possibility to express their views on data protection and can be seen as the public

start of a process that might possibly lead to the revision of Directive 95/46. The intentions of the Commission are still unclear, but it is likely that this conference will have a significant follow up.

- Later this June, the Commission will present a communication on the future of the Area of Freedom, Security and Justice. This communication will seek a balance between security, mobility and privacy. This communication and the 'Stockholm-program' to be adopted later this year by the European Council are meant to set the parameters for the legislation in the coming years. I hope that this legislation will seriously take into account the concerns of data protection.
- There is an increasing emphasis on the external activities of the Union that should facilitate and protect the processing of personal data of European residents outside the EU. For example, negotiations are expected to take place with the United States on the exchange of law enforcement related data, on the basis of a report of a so called 'High level contact group'. In another forum discussions are taking place on the need for and the substance of global standards for data protection.
- Last but not least, the Lisbon treaty, the main subject of my contribution.

I have been asked to speak about the consequences of the Lisbon Treaty for the laws on data protection. I am glad to do so, but of course still in uncertainty about the fate of this treaty. We will have to wait for the second referendum in Ireland to know whether there will be a Lisbon Treaty. And, even if the Irish population would say yes, this does not automatically mean that the treaty will enter into force. For instance, the German Constitutional Court is investigating complaints that have been brought before it. You must be familiar with this procedure of 'Verfassungsbeschwerde'.

If, however, the Lisbon Treaty would finally come into force at the end of this year or early next year, the consequences for data protection would be significant.

2. Three main consequences

I would like to distinguish three main consequences.

First, an important consequence of the Lisbon Treaty will be the abolition of the pillar structure. The area of police and judicial cooperation in criminal matters - now the subject matter of the third pillar - will be integrated in the EC-Treaty (first pillar). This Treaty will be renamed into the 'Treaty on the Functioning of the European Union (TFU)'. Title V of this Treaty - the Area of Freedom, Security and Justice - will not only deal with police and judicial cooperation, but also with other aspects of this area like policies on border checks, asylum and immigration, as well as the civil law cooperation.

For data protection this abolition of the third pillar will have the positive effect that difficult discussions about the borderlines between the different pillars will no longer be needed. These discussions have in the recent years led to two important judgments of the European Court in Luxembourg. This Court decided in May 2006 that the transfer of personal reservation data by airlines to the United States was not covered by the first pillar. But the Court also decided in February 2009 that the storage of traffic data by telecommunications providers for the purpose of combating serious crime could be regulated under this first pillar. These two judgments show that it is difficult to find a borderline. They also show that such a borderline makes less sense in recent years, since it has become more common that law enforcement authorities use personal data that have been collected earlier by private companies for different purposes.

Second, also in the Area of Freedom, Security and Justice, new legislation will be subject to what will be called the ordinary legislative procedure, which means adoption by Council and European Parliament and Qualified Majority Voting within Council. This procedure is common in most other areas of European law, but not yet in the area of law enforcement.

Nowadays, legislation dealing with the exchange of information for law enforcement purposes is a responsibility of the Council of Ministers alone. The Parliament is only asked for advice. It happens in this area quite often that the Parliament is very critical about a proposal, for instance because it questions the need for certain processing

operations, but that the proposal is nevertheless adopted by Council. This happened for instance when the Treaty of Prüm was transposed into a Council decision. That situation will change!

Third, the provisions on data protection will fundamentally change and will become more prominent in the new Treaties. I want to discuss those changes in more detail.

3. Data protection under the present treaties

The new provisions on data protection can be qualified as a fundamental change since in the present treaties the mentioning of data protection is incomplete or, in other words, somehow hidden or disguised.

Data processing was primarily regulated under the provisions for the internal market. It is for this reason that the general Data Protection Directive 95/46 combines two goals: protecting the fundamental right to data protection and ensuring a free flow of personal data within the internal market. The same goes for the ePrivacy directive 2002/58 which is currently subject of a revision process.

The present EC-Treaty only deals with data protection in one of its last provisions, Article 286, a somewhat obscure corner in the treaty. It was inserted by the Treaty of Amsterdam in 1999 and lays down that EU-data protection law applies to processing by institutions of the EU. Article 286 also gives the legal basis for the establishment of a European Supervisor. Both elements are further elaborated in Regulation (EC) 45/2001 which established the EDPS. In 1999, Article 286 was needed to avoid a legal vacuum, ensuring that also the EU institutions should respect the rules of data protection. Despite this limited purpose, Article 286 became the first real provision on data protection in the EC-Treaty.

However, there is a second provision that I would like to mention. The area of police and judicial cooperation in criminal matters (the so called third pillar) contains a more or less general legal basis for data protection, albeit disguised. Article 30 (1) (b) of the EU-Treaty requires that rules on storage and exchange of personal data are complemented by data protection rules. This provision is the legal basis for Council

Framework Decision 2008/977/JHA, the recently adopted framework decision on data protection that is now being transposed by the Member States into their national laws.

Finally, I want to mention that several other legal instruments under the third pillar contain specific frameworks for data protection (e.g. Schengen, Europol, Eurojust and Prüm). One could see those specific frameworks in the light of this Article 30 (1) (b) of the EU-Treaty, already mentioned. All these frameworks contain tools facilitating the cross border exchange of personal data. In this context, mechanisms are needed in order to provide for protection when data are actually used in a cross border setting. This was all the more important before the adoption of the framework decision for data protection in the third pillar, when general EU-rules on data protection did not yet exist in this area.

In short, Articles 286 EC and 30 (1) (b) EU recognise data protection but do not provide for an adequate legal basis for a comprehensive system of data protection. The most important legal instrument for data protection - Directive 95/46 - could and can still today only be based on a legal basis designed to promote the internal market.

4. The Lisbon Treaty

The Lisbon Treaty is quite different. It leads to a fundamental change because of the introduction of a general provision on data protection, a general framework for data protection applicable to all situations. This provision is not hidden, nor disguised, but has a prominent place in the Treaty. This provision is Article 16 of the Treaty on the Functioning of the European Union, which Treaty also applies to police and judicial cooperation. I already mentioned this.

I emphasise that in the Lisbon Treaty the provision on data protection is upgraded from an obscure corner in the Treaty to its Title II "Provisions of general application". This title lists some important provisions such as the consistency of EU-law, the combat of discrimination and the public access to documents.

Article 16 does a number of things, which may have far reaching consequences.

Under its paragraph (1), every natural person has a subjective right to data protection. Paragraph (1) copies Article 8 of the Charter of the Fundamental Rights that also foresees in an explicitly formulated right to data protection. The charter was signed in the year 2000, but lacks until now binding force. The nature of the Charter will change after the Lisbon Treaty. It will become binding.

Article 8, paragraph (2) of the Charter lays down the core elements of data protection in European law:

- 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 concerning him or her, and
- the right to have it rectified.

These core elements are based on longer existing instruments, such as the Council of Europe Convention 108. Slightly different concepts at national level, such as the right to informational "self-determination", are not affected by this provision.

In short, the individual will have a subjective right which is guaranteed in two places. What is even more important is that the right is formulated in such a way that it has direct effect. In this sense it is comparable to other rights given under the EU-Treaties, like for instance the right of the EU-citizen to move and reside freely within the territory of all the Member States.

As a consequence, everyone will have a right to data protection, even in the absence of specific rules specifying the right. Those persons can invoke the right before a judge. Of course, the exercise of this right by individuals is not unlimited. It can be subject to conditions and limitations under EU-law. But, I would argue, due to its nature as a subjective and a fundamental right, these conditions can not render impossible the exercise of the core elements of the right to data protection, mentioned in the Charter.

This brings me to the second element of Article 16. Its paragraph (2) obliges the European Parliament and the Council to lay down the rules relating to the protection of individuals with regard to the processing of personal data. This obligation applies to processing by Union institutions, bodies, offices and agencies. It also applies to processing by the Member States when carrying out activities which fall within the scope of Union law. This certainly covers the public sector. However, although not very clearly formulated, it also applies to all processing operations in the private sector. The text of Article 16 states that the European Parliament and the Council should lay down the rules relating to the free movement of such data.

These rules will contain the conditions and limitations for the exercise of the right to data protection, just like the present European instruments contain such conditions and limitations.

Finally, I would like to mention that Article 16 contains two more elements. In the first place, the article states that there must be independent authorities controlling the application of the rules on data protection. The principle of control by an independent authority is currently subject of a case before the European Court involving Germany, more specifically the requirement in Directive 95/46 that such authorities "should act with complete independence". The outcome of this case will have consequences for the impact of the Lisbon Treaty.

In the second place, Article 16 refers to a specific legal basis for data protection in the area of the common foreign and security policy of the EU. Data processing by national security services for instance will not be covered by Article 16, but by this specific legal basis. This is an exception to the general scope of Article 16. I will not go further in this specific provision which is deep in the specific part of the Treaty on the Common foreign and security policy.

5. Article 16 and the current legislative arrangements

An interesting question is of course which consequences Article 16 will have for the current legislative arrangements.

My first remark might come as a surprise after what has been said on Article 16. The Lisbon Treaty and its Article 16 will *not* affect Directive 95/46. This directive seems to fulfil the criteria of Article 16. It was adopted by the Council and the European Parliament and it offers the protection required under the Lisbon Treaty. I am inclined to take the same position as to Regulation 45/2001 on the protection of personal data by the EU itself. This is of course without prejudice to any revision of Directive 95/46 that might take place for other reasons.

However, for data protection in the area of police and justice, the situation is more complicated. The entry into force of the Lisbon Treaty leads to the end of the pillar structure, but that does not mean that Directive 95/46 will automatically apply to police and judicial cooperation. The scope of this directive is limited. It now excludes activities of the State in the area of criminal law. Only a precise amendment of the Directive on that point could change this situation.

How about the new framework decision on data protection? Will that apply?

According to Protocol No. 10 of the Lisbon Treaty, the legal effects of the framework decision will be preserved, until the act is repealed, annulled or amended. The Framework Decision will thus continue to apply under the new Treaty.

However, the obligation of Article 16 on the Council and the European Parliament to lay down rules on data protection, also applies to the area of police and judicial cooperation. It is the task of the Commission to adopt a proposal in this sense.

This being the case, there is an obligation for Council and Parliament to lay down rules applicable to police and judicial cooperation, on the basis of Article 16 TFEU. It is safe to assume that the framework decision does not fulfil the requirements of Article 16 TFEU, because (1) it is a measure taken by Council alone and not by Council and Parliament and (2) the framework decision only applies to parts of the area of police and judicial cooperation. Processing operations that do not involve more than one Member State are excluded from the scope of the framework decision.

To be complete, this obligation under Article 16 applies immediately after the entry into force of the Lisbon Treaty, since it is not touched by any of the transitory provisions in the protocols that were added to the Lisbon Treaty.

So there is an obligation to legislate, but the question is: who can enforce this obligation? Under the EU-system there is no possibility for an individual to address himself to a Court if he is of the opinion that constitutional values were violated. Constitutional complaints ('Verfassungsbeschwerde') are not foreseen. However, one could imagine that the Parliament would claim that its prerogatives are violated, in case no legislative proposal for data protection in the area of law enforcement would be made by the Commission. This possibility could motivate the Commission not to wait too long before it issues a proposal.

Another, more logical solution would be to use the current discussions on Directive 95/46 for the development of a new instrument on data protection which replaces or amends the directive and at the same time fixes the deficient situation in the third pillar.

However, the Lisbon Treaty does not necessarily have to lead to *one* instrument applicable to *all* kinds of processing. A separate instrument for police and/or justice is not excluded and is even supported by a Declaration added to the Treaty stating that specific rules on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation may prove necessary because of the specific nature of these fields. In other words, this is a political decision for Council and Parliament as "equal partners". However, the new instruments should have a general scope and be fully consistent with each other. Both are certainly not the case now.

I now come to the end. Although I have only briefly touched the Lisbon Treaty, it should be clear that data protection will have a prominent place in the Treaty. There will thus also be important opportunities for the improvement of data protection, especially in the present third pillar. I have also pointed out that much depends on how the legislator will act in order to fully use these opportunities for improvement.

I realise that this is just a first and superficial taste. There is much more to say. For the moment however, and still not sure about the entry into force, I limit myself to these first remarks.

Thanks for your attention.