

**Data Protection in the Age of SWIFT, PNR, Prüm and E-Justice**  
**ERA Conference, Trier, 31 May 2010**

---

**"Data Protection for Law Enforcement after Lisbon"**

*Peter Hustinx*

*European Data Protection Supervisor*

Ladies and gentlemen,

This is the second conference on data protection and data exchange in the area of law enforcement. It is also the second time that ERA organised this event in cooperation with the European Data Protection Supervisor. I am delighted about this cooperation and its results so far.

This conference is rightly presented as a bi-annual event that serves to update academics and professionals in this area, and to raise awareness with academics and legal professionals that are not so familiar with data protection yet.

The audience is different from two years ago. This confirms that the professional community interested in data protection is quite large. However, in view of the programme, the conference could also have attracted the same audience as the first conference two years ago.

Many things are developing in this area of data protection which relates to the needs of law enforcement to use and exchange personal data, quite often of a very sensitive nature. This is therefore also about the needs of citizens to be protected against undue data processing or to make sure that developments take place in a fair and legitimate manner.

## Overview of the subjects

The title of this conference - referring to "Data Protection in the Age of SWIFT, PNR, Prüm and E-Justice" – nicely sums up some of the interesting issues that we will be discussing. However, it also covers a few more general questions: what is meant with the "age of SWIFT etc", what society are we dealing with when discussing these phenomena, and what kind of data protection is required in that society, which is after all the society in which WE are ALL now living more and more. In other words: what data protection is needed and what are the consequences of the various issues?

The recent developments in law and in policy making will be at the core of this conference. However, one important element is not mentioned in the title, but rightly comes up at this stage and is likely to run through the different sessions: i.e. the impact of the Lisbon Treaty.

The Lisbon Treaty entered into force on 1 December 2009 with a new and much stronger perspective for data protection - i.e. data protection as a fundamental right in the EU Charter, made binding for the EU institutions and bodies and for the Member States when they are applying Union law; a general and horizontal legal basis for data protection measures in Article 16 TFEU. It also put an end to the pillar structure, and introduced stronger roles for EP, COM and ECJ, which all result in a framework for decision making with far better safeguards and the functioning of a system of checks and balances. As to the EP, there is now much more co-decision and also a role in the field of international agreements.

But that is not all: the Stockholm Programme, also adopted in December under the scope of the Lisbon Treaty, introduced a policy framework with some very interesting and positive elements, including an EU Information Model, which aims to balance the business needs of law enforcement with data protection,

Only a few days ago a new step was set towards data protection in the transatlantic relations. On Wednesday last week, the Commission adopted a draft mandate to negotiate a personal data protection agreement between the EU and the US. Let me quote from the press release: "*The aim is to ensure a high level of protection of*

*personal information like passenger data or financial information that is transferred as part of transatlantic cooperation in criminal matters. The agreement would enhance the right of citizens to access, rectify or delete data, where appropriate. EU citizens would receive a right to seek judicial redress in the US if their data is unlawfully processed. Independent public authorities would be given a stronger role in helping people exercise their privacy rights and in supervising transatlantic data transfers."* All these actions in legislation and in legislative policy will be discussed these days.

On top of that, let me underline that it is equally challenging to look at developments in the recent case law. Since the last conference, the European Court of Human Rights specified its criteria for the lawfulness of storage of DNA-information in national databases, in the case of *S and Marper v the United Kingdom*, which has become famous in the meantime in fundamental rights circles. This judgement itself is not on the agenda here in Trier, but it is important for the functioning of the Prüm-system which will be discussed later on in the conference. I would be curious to know from tomorrow's debate whether Marper actually limits the possibilities of the authorities of the Member States to exchange DNA data and fingerprinting data on a large scale, and if so to what extent.

The agenda of this conference does however contain two more recent cases. In March, the European Court of Justice interpreted the notion of the independence of the data protection authorities. The wording 'acting in complete independence' is included in Directive 95/46. Independence is also laid down in Article 8 of the Charter as a corner stone of data protection in the EU, and equally in the new legal basis for data protection which is Article 16 TFEU.

The case on the independence of data protection authorities was decided by the European Court, dealing with the implementation of European law here in Germany. I can not deny my overall satisfaction with this judgement which sets high standards for the independence of the authorities. They have to act in full freedom, without any influence from political bodies, for the reason that it is their task to monitor the application of provisions on data protection, and strike a fair balance where needed.

The other case on the agenda, about data retention, is also from March this year and equally deals with implementation of a European directive in German law, more specifically the highly controversial Data retention directive. However, in this occasion, it is the German Constitutional Court that examines the implementation of the directive - but necessarily also the directive itself - in the perspective of the fundamental rights protected by the German constitution. In this context, let me just briefly mention that the 'Bundesverfassungsgericht' did not refer to the protection of fundamental rights on the European level, as laid down in the European Convention on Human Rights and in the EU-Charter.

A relatively new subject in the conference is e-Justice, a major project of the Council and the Commission to modernise the judicial exchanges between the Member States. Data protection will be important, for instance when e-Justice will be used for the exchange of insolvency data of the Member States, or for the exchange of criminal records. The emphasis tomorrow will be on 'privacy by design', in other words how privacy and data protection can be included in the architecture of e-Justice. In my view, e-Justice is the perfect opportunity for 'privacy by design' since the e-Justice system will be built up from scratch. There is no need for any difficult adaptation of existing systems.

### **Towards a new legal framework**

Having said this, I would now like to continue with the possibly most important development in data protection: the review of the data protection framework which the Commission is preparing right now. Let me recall that the Stockholm Programme announces the need for a comprehensive legal framework in its chapter on the fundamental rights of the citizen. Vice-President Reding has mentioned this review of data protection law as one of her main priorities, if not her top priority. A legislative proposal is foreseen for the end of 2010.

On several occasions, I have expressed my views about this proposal which I consider as extremely important. In a speech recently held before the European Conference of data protection commissioners in Prague, I emphasised that the stakes are not more

and not less than "how to ensure privacy and data protection in a highly developed Information Society of 2015, 2020 or beyond".

In my view, the Commission should be very ambitious. It should propose measures that ensure effective protection in a highly globalised information society. It is my conviction that despite all new phenomena like the Internet of things or cloud computing, the main principles of data protection remain valid. New instruments however are needed, to ensure effective enforcement.

This is why we propose integration of "privacy by design" and "privacy by default" in information and communication technologies. E-Justice was just an example, but "privacy by design" should apply to all ICT-architecture, in the private as well as in the public sector.

Another issue is more accountability for controllers: data controllers should be made more accountable to ensure compliance with data protection rules in practice. This would bring significant added value for an effective implementation of data protection and would considerably help data protection authorities in supervision and enforcement. In other words: data controllers should be more responsible, more in control and be able to demonstrate that they have taken all measures necessary to ensure compliance.

This conference will focus on the meaning of a new legal framework for the area of freedom, security and justice. Also in that area, the notions of "privacy by design" and "accountability" should become leading for the national and European authorities that process personal data, quite often of a very sensitive nature. In this area, we not only deal with data relating to criminal offences, but also personal data of vulnerable groups of immigrants and asylum seekers are processed on a wide scale.

Another challenge will be how to include the specific data protection regimes for police and judicial cooperation in the comprehensive framework. With the growing exchange of data between sectors and authorities the existing legal framework does no longer seem up to date. It has been often called a patchwork, with some more or less general rules in Framework Decision 2008/977, which differ from Directive 95/46 on

many points of substance, and are not applicable to domestic situations in the Member States, nor to European bodies such as Europol and Eurojust, that have their own rules. I recall that, for instance, also the Prüm decision has a separate data protection regime that is largely based on national rules that have not been harmonised. It is not so evident how this regime relates to Framework Decision 2008/977.

In my view, it is clear that police and justice should in the future be included in the general framework for data protection. This does not exclude that some additional specific rules for police and justice might be needed, nor does it exclude that some parts of the comprehensive framework would be allowed to 'phase in' only gradually.

### **An EU Information model**

The first session this morning will discuss the EU Information model as a means to accommodate the needs of law enforcement, but with full respect of data protection.

One of the guiding principles of the EU strategy is commonly known as 'select before you collect'. The EDPS embraced this principle as a very useful step forward in reaching the right balance between the different interests at stake when personal data are requested for law enforcement purposes.

Authorities should only collect information which is necessary for a specific purpose, and not create enormous databases with personal data, in case personal information might eventually be needed for the combat of a crime, or to allow data mining within these data bases. This could in fact better to be defined as 'collect before you select'.

One could discuss whether this idea of 'targeted collection' is indeed reflected in all other elements of the Stockholm programme. For instance, the Stockholm Programme emphasises the need for a European PNR-system. The proposal for such a system was discussed in Council and heavily criticised, also because the added value of a data base of air passengers, on top of all other available information, was not sufficiently demonstrated. In any event these discussions, which were particularly intensive under the French EU Presidency, did not lead to a conclusion.

Undeniably, the PNR system offers other possibilities than most existing databases, since its aim is apparently not to find known criminals or suspects of crimes, but to find the unknown. On the basis of travel patterns and unusual flight reservations, it should be possible to find people with criminal intentions. But does PNR not seem the perfect example of 'collect before you select', the contrary of the targeted approach mentioned as 'select before you collect'? A huge database is created with passenger information, in order to be able to monitor behaviour in case of a specific threat or crime, but possibly also in the absence of such event or specific risk.

I look forward to the following panel, that certainly will address the question how the balanced approach of the Stockholm Programme can be elaborated in legislation and in practices.

### **The EU External Action**

The Lisbon Treaty makes a change for the external action of the EU in the area of freedom, security and justice. We noticed this early this year, when the EP rejected the Swift agreement. This agreement on the exchange of financial data for terrorist tracking was signed under the old Treaty rules, on 30 November 2009, but could not be formally concluded in time and was only applicable on a provisional basis.

Under the Lisbon Treaty, the EP has to approve agreements, also in the area of police and justice. In this area, it replaces the powers that in a number of Member States were assumed by the national parliaments, that had a constitutional power to approve or veto agreements.

In February, the EP used the first occasion and rejected an agreement, despite the pressure which was put on it, not to think too lightly of this instrument in the fight against terrorism. Even the US Secretary of State, Mrs Clinton, was involved in this discussion. Luckily, in its considerations, the EP based itself clearly on privacy and data protection. It did not reject the agreement purely for political reasons of using a new institutional power, although some of this may have been part of the equation.

The Swift case does not stand alone. The PNR agreements with the US and Australia might in principle end up in the same way. However, let us wait and see what will happen with those agreements that currently are applied in a provisional way. Until now, the EP has postponed its decision and tried to use its political capital for the development of a horizontal approach - covering all PNR situations - that would be more consistent.

In this respect, I find it very interesting to see the effects of the Lisbon Treaty on the mandate for negotiations with the USA on a general agreement on data protection. I mentioned the mandate already and quoted the press release.

The Commission proposes a mandate that clearly aims to give effective protection. And it does so in a transparent way. Although the negotiation mandate in itself is kept secret, the Commission is very open about its ambitions.

And those ambitions go far. A high level of protection, application to personal data required from private companies like airlines and banks, judicial redress, independent data protection authorities: all this is included in the press release that I have quoted before.

This is not self evident, since the preparations of the agreement - in the first place by a so called 'High level contact group' of civil servants on both sides of the ocean - have shown that some results are not easy to achieve with the US. A good example is judicial redress for European citizens before US tribunals against improper use of their personal data. Such redress is not foreseen under the US Privacy Act and would require a change of internal US legislation.

Another topic in the discussion with the US is on all occasions the role of the independent data protection authorities. Such authorities do not exist in the US, in any case not in the relevant area. Supervision on data processing by government agencies is organised in a different way, with Privacy Officers acting within the Administration but with a certain degree of autonomy, since they report directly to Congress.

Nevertheless, the Commission openly includes these topics in its negotiation mandate and puts the bar quite. Not achieving these results might be seen as a failure. I am curious how the panel members this afternoon will see this.

### **Judgment on Data retention**

Let me now turn to a completely different subject. On 2 March, the German Constitutional Court ruled that a few provisions of the German Telecommunications Act, implementing the Data retention directive 2006/24, are unconstitutional since they violate the fundamental right to the secrecy of telecommunications, as protected under the German Constitution.

This judgement deals with a highly controversial directive from early 2006. This directive requires from telecommunication providers that they store traffic data of their customers for a certain period for the combat of serious crime. The providers should keep the data available for law enforcement authorities, whereas the EU law normally requires that the data are deleted when they are no longer needed for the original purpose of their collection, which is in this case connecting people and sending them bills for their calls.

The Data retention directive was adopted shortly after the bombings of the London Underground in July 2005 and was criticised for a number of reasons, also by me.

In the first place, it asks for storage of data of all citizens, so not only those that are related to a crime. In the second place, it leaves a lot of discretion to the Member States, for instance on the storage period and on the use of the data by national law enforcement authorities. This may be harmful to the effective protection of the citizen but also to the level playing field for providers in the EU. In the third place, the legal basis in the internal market provisions in the Treaty was not evident and was contested before the European Court of Justice.

This third issue was solved by the Court of Justice in the case Ireland v Parliament and Council, an important judgement which further determines the dividing line between internal market provisions and the area of freedom, security and justice, as a

follow up to the famous PNR cases. After the entry into force of the Lisbon Treaty, this seems to be no longer a problem.

The other matters - lack of harmonisation, indiscriminate data storage - have led to several cases before national courts.

It is good to underline that the German case does not stand by itself. Last year, the Rumanian Constitutional Court declared the directive unconstitutional, a case is pending before the Hungarian Constitutional Court and, recently, the Irish High Court ruled in favour of a request to challenge the Data Retention Directive at the European Court of Justice. The complainant in Ireland had claimed the directive was in breach of fundamental rights under the EU treaties, the European Convention on Human Rights and the EU Charter of Fundamental Rights. The Irish court ruled that, in this matter, a reference to the ECJ was required. This reference to the Court of Justice is expected in the next weeks.

This brings me to the judgement of the 'Bundesverfassungsgericht' itself. It will be discussed tomorrow, I presume in particular on the examination of the compatibility of the German implementing law with the Constitution.

However, I would like to focus on the lawfulness of the directive itself in Germany. The Court does not have any doubts about the validity of the directive, contrary to the Courts in Rumania and Ireland. If the 'Bundesverfassungsgericht' would have had such doubts, this would have required a preliminary ruling under Article 267 TFEU as requested by the complainants in Germany. The Court rejected this request.

It came to this conclusion on the basis of the following reasoning. According to the Court, the German Constitution does not prohibit data retention in all circumstances. More specifically, retention of telecommunication traffic data for six months is not per se incompatible with the German Constitution. Such storage might be necessary for strictly defined purposes of law enforcement, which excludes in any event less serious crimes.

The Court then analysed the main content of the directive, which is essentially limited to obligations on private companies to store data, leaves the Member States a lot of freedom to determine the conditions of storage and does not govern the access to or the use of the data by national authorities.

What strikes me here most is that the Court upholds the directive because of its lack of harmonisation, especially where it comes to storage time and use of the data by the judicial authorities. In other words, the directive is upheld due to one of its weakest elements. This suggests that the judgement of the Court is likely to have a great impact on the current discussions about the evaluation of the directive and of course about its possible revision.

### **Final remarks**

Let me conclude my remarks at this point. I only wanted to touch a few subjects of the conference, as a start of hopefully very fruitful debates.

I thank ERA once again for providing this forum to discuss data protection in these interesting times. I hope that this reflective academic atmosphere of Trier will bring our thinking and our understanding of the issues on an even higher level.

I also hope that our discussions will contribute to better solutions in the near future and to more effective data protection in an area where the stakes are high, and where the opportunities for data protection are perhaps also greater than before, due to the entry into force of the Lisbon Treaty.

Thank you very much, and I wish you all a very fruitful conference.