

**Conference on Law Enforcement Information Exchange and Modern
Technologies (COPE 09)**

Stockholm, 17-18 September 2009

"An EU Information Model and Data Protection"

Hielke Hijmans

Coordinator Consultation and Court Proceedings

European Data Protection Supervisor

I. A balance between the needs of law enforcement and data protection

This is the title of this workshop at the COPE Conference. It also reflects the ongoing discussion in recent years in this area. 'Striking the right balance' was the objective of many legislative and non legislative initiatives. It was also one of the central points Minister of Justice Ask mentioned when she presented the ambitions for a Stockholm-programme in the European Parliament earlier this month.

There is no discussion about the objective itself, the discussions are about the substance of the objective and the consequences of its application. Here, one can notice a clash between what is usually called the law enforcement community and the data protection community. A balance requires taking into account the perspective of other stakeholders and that is not always evident.

Misunderstandings

Let me, as representative of the data protection community, try to take away some misunderstandings that might give rise to this clash:

1. Data protection does not hamper law enforcement authorities to do their proper job. Personal data may be used if necessary for the public security or the prevention or combat of criminal offences.

The essential criterion is that of necessity. Legal instruments facilitating the storage and exchange of data should only be adopted if there is evidence that these measures effectively contribute to law enforcement.

2. A second criterion is proportionality. The impact of a measure on individuals must not be disproportionate. In the famous case *S and Marper* the European Court of Fundamental Rights clarified the need for proportionality and decided that the DNA data bases in the UK did not fulfil this criterion. The Court did not say that DNA data bases are not allowed, but it required for instance that persona data are removed if there is no direct link with the combat of crime any more.
3. Thirdly, purpose limitation is one of the building blocks of data protection. In principle, personal data should only be used for the purpose for which they are collected. This requirement means for instance that data bases can only be interlinked under specific conditions.
4. Fourthly, the main effect of data protection law is that safeguards and guarantees are needed to protect legitimate interests of individuals. Important elements of data protection are the rights of the data subject, to be informed, to have access and to request for rectification or deletion.

Burdens for law enforcement?

5. At first sight, these requirements seem burdensome for law enforcement:
 - a. Only data processing where necessary. But how can one prove in advance whether a measure is necessary?
 - b. Proportionality. Does this not run the risk that not all data can be stored and exchanged, or that data will be deleted whereas they might become important for law enforcement?
 - c. Purpose limitation. Will that not make it impossible to use personal data that once had been collected for the purpose of a specific crime, for other useful objectives relating to the combat of crime?
 - d. Safeguards and guarantees. Will they not hamper investigations and/or enhance the costs in a significant way? Will it not increase the administrative burdens?

There are no significant burdens

6. This all may be true, but:
 - a. Law enforcement operates under the rule of law. Where government authorities intrude in the private lives of citizens, they should be accountable.
 - b. Information management and cross border information exchange must be based on trust. This means that (1) the users of information in another Member State can rely on the quality of the information, (2) the judiciary in other Member states trust the information so that it can

be used in its criminal procedure, and (3) citizens must be sure that their data are used in a responsible way.

- c. Therefore, a sensible information management leads to limitations in the availability of data. Information management takes a targeted approach, limiting the availability of information. The approach should be that information is gathered provided that there is evidence that this is useful and necessary, not that all available information is gathered avoiding any risk that information will be missed that might in future possibly be useful. As was emphasised by Prof. Cleiren in her contribution: Select before you collect.
- d. In this context: Minister Ask emphasised within the European Parliament that the EU should promote that useful information can be exchanged, not that information on all citizens should be registered, in particular possibly sensitive information.
- e. This requires the evaluation of the effectiveness of existing legal instruments before proposing new legislative measures, as well as an *ex ante* evaluation of the new proposals. The EDPS has regularly asked for such evaluations and, as I understand the Swedish government well, their importance will be emphasised in the Stockholm Programme.
- f. It would be an improvement, not only for data protection, but also for effective and efficient use of police resources, if these evaluations are taken serious within the legislative process. Recently, that was not always the case. An example was the EU PNR proposal. There was no

evidence that this proposal would have real added value on top of information that is already available in data bases like SIS, Prüm and Europol, and flight data that is already required under a Directive from 2004.

- g. This leads to data protection. It is good to have in mind that it is a system of checks and balances aiming to protect certain values but that does not prohibit the storage, use and exchange of personal data. It only makes these activities conditional upon the fulfilment of certain requirements. I mentioned this before.
- h. In the system of data protection data quality has a significant importance. Data quality implies for instance that data must be adequate, relevant and not excessive in relation to the purposes for which they were collected. Moreover, data must be accurate and kept up to date. It goes without saying that fulfilment of those conditions does not only protect the data subject but is also in the interest of data users.
- i. To be more specific, there have been discussions to include in data protection law obligations for controllers of data bases to distinguish factual information from soft information, based on personal opinions. Such distinction might be useful to data users as well.

II. Instruments for striking the right balance

The EDPS opinion of 10 July 2009 on the Communication of the Commission on an area of freedom, security and justice serving the citizen calls at several places for reflection and for the need for a clear and long term vision.

These reflections are meant to contribute to the development of instruments that effectively strike the right balance. Some of these ideas were mentioned by Peter Hustinx in his speech to the Ad Hoc Group on Information Exchange on 6 July.

The first instrument, choosing the right architecture. This is the start of it all. The EDPS opinion stresses that data protection requirements should be an integral part of all system development. Use should be made of the concepts of 'privacy by design' and need to identify 'Best Available Techniques'. Information systems which are designed for purposes of public security should always be built in accordance with the principle of 'Privacy by design'. The reasons are clear: once a system is in place, it would be much more burdensome to include data protection friendly solutions, which for instance guarantee the right level of security, gives different levels of access and ensures the rights of the data subjects.

The second instrument, avoiding automatic interoperability between systems. Interoperability of systems is not a purely technical issue but also has consequences for data protection. Interoperability of systems can have advantages: no double storage is needed. But there are also disadvantages: interoperability and mutual access to systems could have as an effect that personal data will be used for other purposes than the purpose of collection, without restrictions. Interoperability can even be a driver to such use. If information is easily accessible for other purposes, it will be used. Therefore, we plead for avoiding automatic interoperability: only on the basis of

a specific political choice. In other words, data bases should only become interoperable, if a real need for the exchange between the systems is demonstrated.

Another instrument (number 3) could be systematically choosing for decentralised storage, understood as storage of data on the level of the Member States without the involvement of any central European body. Decentralised storage is the model chosen in the Prüm decision, whereas the Schengen Information System or Europol are examples of a central model.

However, this is a complicated area. A decentralised system has advantages from the perspective of data protection:

- No double storage of data by the authority of the Member State and by the central system.
- Clear responsibility for the data: the authority of the Member State will be the controller.
- No doubts about applicable law.

But it also has disadvantages:

- When data are exchanged with other jurisdictions, it must be ensured that information is kept up to date both in the country of origin and the country of destination.
- How to ensure responsibility for the technical system for the exchange.

These are just a few arguments showing how difficult but also how important the choice is between a central or decentralised system. Too make it even more difficult, in practice the distinction between a central and a decentralised system is not always fully clear. Decentralised systems with a strong coordination and/or a common

infrastructure can be attractive options, but it also requires clarity about which actor is responsible for which part of the system.

Finally, equally important but less difficult is the choice for coherence and consistency between the pillars of the Treaty and of the data protection requirements which are included in a number of legal instruments.

In my view, there is much to win if a single legal framework for data protection would replace the complicated patchwork that exists today in the area of freedom, security and justice.

The police have to deal with instruments of the first pillar, like for instance the data protection directive from 1995, but also the data retention directive from 2006. In the third pillar, the Data protection Framework Decision of 2008 has to be implemented by the Member States. However, this does not apply to personal data that remain within the jurisdiction of one Member State. In that case, the Member States base the national law on a Convention of the Council of Europe of 1981. On top of this, many legal instruments contain specific chapters on data protection. I just mention the Prüm decision, the legal instruments on SIS, the Criminal Records Exchange etc.

Improving and simplifying the legal framework would be in the interest of us all, I would say. If we do this in the best way, we can really strike the right balance between the needs of law enforcement and data protection. Hopefully, the Lisbon Treaty will give us the right tools to do so.