

Towards more effective Data Protection in the Information Society *

Peter Hustinx

European Data Protection Supervisor

The publication of the 50th issue of *datospersonales.org* could not have been planned better than right now! It not only shows the vitality of this digital review supported by the Data Protection Authority of Madrid, but also comes in the midst of a thorough review of the main frameworks for data protection in the EU, the Council of Europe and the OECD, which have so far all played a crucial role in data protection, both in Europe and beyond. At the same time, we experience that our societies are becoming increasingly dependent on the continuous and wide spread use of various information and communication technologies. This means that data protection is also increasingly relevant and that we have to ensure its continued effectiveness as a fundamental right for all citizens in a changing world. In other words, the ongoing reviews offer a major window of opportunity to make data protection more effective and fit for purpose in the Information Society of 2015, 2020 and beyond.

Ongoing reviews

In the spring of 2009, the European Commission launched a public consultation on the need for review of the current EU legal framework for data protection in view of the challenges posed by new technologies and globalisation. The substantial input received from many sides allowed the Commission to embark on a major review, the outlines of which were presented in a Communication - *A comprehensive approach on personal data protection in the European Union* - in November 2010. On this basis and further input received from various stakeholders, the Commission is now likely to present a proposal - or a package of proposals - later this year. This will be subject to discussion in the European Parliament and the Council, which will together decide on the shape and substance of the EU legal framework for data protection in the future. This may well happen in 2013 or 2014, close to the end of the current mandates of the Parliament and the Commission.

* This article appeared in the [50th issue \(April 2011\) of *datospersonales.org*](#) - digital review published by the Data Protection Authority of Madrid.

In the meantime, the Council of Europe has also decided to undertake a review of its Convention 108 from 1981 which still forms the basis of most data protection laws in Europe, and in fact also of Directive 95/46/EC which specified and further developed it in many ways. The OECD Guidelines from 1980, adopted in parallel to Convention 108, have also influenced developments around the globe, mostly in non EU member states, and are now also subject of a review. The co-occurrence of three major reviews is a challenge, but also an opportunity for more global data protection, if undertaken in synergy. This is why the European Data Protection Commissioners at their recent Spring Conference in Brussels have called on the main stakeholders in these projects to coordinate their activities. Another recent development might help to create this synergy and also lead to more global consensus: the recent announcement of the US Administration to work towards a Bill of Rights for privacy and data protection. If delivered in good shape, this would of course be a very welcome development.

Review of EU framework

Now looking more closely at developments in the EU, it should be noted first that the object of review is *not only* Directive 95/46/EC, although this is still the most relevant instrument at EU level, with a large impact on the member states. However, other instruments have been adopted since, such as Directive 2002/58/EC on e-Privacy, Regulation EC 45/2001 for EU institutions and bodies, and most recently Council Framework Decision 2008/977/JHA on the protection of personal data in the context of police and judicial cooperation in criminal matters. This does not include various other specific instruments or provisions, either in the former "first pillar" or in the former "third pillar" of the EU. The ongoing review of the EU legal framework covers in principle this entire area, including various specific subjects. However, it may well be that for practical reasons the review - and the actual revision where needed - will be developed in stages.

Why is this review taking place? The answer to this question can be summarised in three main points. First, it is fair to say that the main instrument of the EU framework - i.e. Directive 95/46/EC - now requires some maintenance, if only because of the fact that it was adopted when the Internet was still rather invisible and in any case far from its present highly dynamic reality. Another aspect is that the Directive has succeeded

in accomplishing a certain degree of harmonisation, but after 15 years a great deal of diversity has developed among the national laws implementing the Directive. Much of this is unhelpful at an EU scale, either for economic reasons or for a lack of effective protection in cross-national issues.

Treaty of Lisbon

A second very important reason is the impact of the Lisbon Treaty. When the Treaty entered into effect in December 2009, it made the EU Charter of Fundamental Rights binding on the EU institutions and bodies, but also on the member states when acting within the scope of EU law. One of the new elements in the Charter was the explicit recognition of a right to the protection of personal data (Article 8), in addition to the right to respect for private life (Article 7). Moreover, Article 16 of the Treaty on the Functioning of the European Union (TFEU) has given data protection a prominent place among the general principles of the EU, including a general legal basis for the adoption of "rules" on the protection of personal data both at EU and at member state level. This horizontal provision has led to the need for a comprehensive review of existing rules on data protection in all fields of EU policy, regardless of their origin and status in the pre-Lisbon era.

A third reason is that data protection has now become such a relevant factor for other important policy fields that it can somehow be considered as a critical success factor for these other policies. This is clear from the Digital Agenda, one of the crucial parts of the EU 2020 Strategy, as well as from the Stockholm Programme on the policy for the Area of Freedom, Security and Justice, covering fields like migration, police and justice. Data protection is seen as a condition for trust in e-Health, e-Government and e-Commerce, and for trust among member states when exchanging sensitive data.

Political sensitivity

All these reasons together have led to much greater awareness and political sensitivity for the need of better data protection. The decision of the responsible "third term" Commissioner, Mrs Viviane Reding, to make this subject one of her top priorities, has also led to a dynamic environment. Initial positions in Parliament and Council suggest that there is a fairly large consensus about the need and potential for more effective data protection.

What direction will this review take? Here, an important reservation should be made, as the Commission is fully responsible for its own proposals and has not yet presented them. However, a few fairly accurate predictions can be made on the basis of public sources.

Horizontal approach

First of all, the strong emphasis on a "comprehensive approach" means that all fields of EU policy will be covered, including those of the former "third pillar", i.e. notably police and justice. This is very welcome for different reasons: it will lead to a more horizontal approach without distinctions between different policy fields that not fully correspond with reality. This approach is in line with the Lisbon Treaty that clearly mandates a horizontal and comprehensive approach. The present rules for police and justice are a patchwork of specific rules and a general framework of limited scope as it *only* applies to data flows *between* member states. A more comprehensive approach is therefore likely to lead to better rules overall.

This does not necessarily mean that there should be only one single instrument at the end. Specific additional rules may be needed for specific sectors, as has already been the case for the e-Privacy Directive, but those sector-specific additional rules should in no circumstances lower the level of protection, and should only allow for legitimate restrictions in accordance with general data protection principles.

More effectiveness

Secondly, it should be clear that this is not the time to reinvent data protection. It has been invented and now recognised as fundamental right in the Lisbon Treaty. Instead, much attention should be given to making data protection more effective in practice. This means a greater focus on implementation and enforcement of data protection principles and on the delivery of data subject's rights. A related concern is that some existing formal requirements could be simplified or abandoned, if they are no longer needed for effective data protection. The notification of data processing to supervisory authorities is a clear example of such a requirement.

Another point in this context is the need for greater harmonisation of rules across the EU. The present diversity of national rules - even within the scope of the Directive - is not helpful for effective data protection, and quite frankly counterproductive. The way forward may be either a more prescriptive Directive or a directly binding Regulation, or hybrid combinations of instruments. This is not only a legal issue - although Article 16 TFEU would allow different options - but also a sensitive political issue about the scope of EU law versus the member states.

Stronger roles

Thirdly, more effective data protection also requires a strengthening of the three main roles in data protection: those of the data subject, the controller and the supervisory authority. Data subjects should be enabled to exercise their present rights more easily and should be given a few additional rights to protect their interests where needed. An interesting example is the right to require that personal data are deleted or transferred to another provider – often referred to as the "right to be forgotten" or the "right to data portability" – which might be particularly useful in the context of social networks or other online services. Strengthening the rights of data subjects would also require a clarification of the situations where consent is required and the conditions that have to be met for valid consent. A lack of clarity about this often leads to a weaker position of data subjects, particularly in the online environment.

Data controllers are now responsible for compliance with data protection rules, but in practice this often only leads to formal arrangements and responsibility "at the end" if something goes wrong. Instead, data controllers should be mandated to be more active and to take all those measures which are necessary to ensure that data protection rules are complied with. This is referred to as the "principle of accountability" that would require data controllers to be able to demonstrate that they have taken all appropriate measures to ensure compliance. This requirement should of course be related to the context and "scalable" to avoid undue burdens for small and medium enterprise. The principle of "privacy by design" would fit in the same approach: controllers should be able to demonstrate that appropriate measures have been taken to ensure that privacy requirements have been met in the design of their systems.

Supervisory authorities should be given adequate resources and stronger powers of enforcement that are equivalent in all member states. Supervisory authorities should also be allowed to use these powers more strategically, including the possibility to be more selective (e.g. in the case of substantial risks or systematic wrongdoing). At the same time, the conditions for "complete independence" should be equivalent in all member states. This means that the judgment of the European Court of Justice of 9 March 2010 in case C-518/07 (Commission v Germany) is taken as a benchmark: data protection authorities "should be free from any - direct or indirect - influence in the exercise of their duties". These conditions are also essential for effective cooperation in cross-border situations.

Technology and globalisation

A legal framework that would provide the above elements would be much better in the position to deal with the challenges of technological change and globalisation. In addition to - or as a further specification of - these elements, it would be interesting to require impact assessments or regular audits for cases with specific risks. Other ideas would include the use of certification for privacy relevant goods or services to ensure adequate "privacy by design".

The growing international dimension would ideally require a global consensus on data protection principles and standards. Although this global consensus is developing in practice, it is still far from perfect. It is therefore also important to clearly define the external scope of EU data protection law (i.e. the applicability of EU law in relation to third countries). The concept that EU law should also apply where EU consumers are "targeted" - or more in general where services are provided to EU consumers - seems to attract more and more support. Finally, it will be important in this context to simplify the present requirements for data transfers to third countries. The process for the approval of binding corporate rules (BCR) could be mentioned as an example. The explicit recognition of BCR and the mutual recognition of national approvals would be a very welcome step forward.