The Reform of EU Data Protection: towards more effective and more consistent data protection across the EU[1]

Peter Hustinx
European Data Protection Supervisor

Today, I would like to inform you about the main lines of the current reform of the EU legal framework for data protection. After a brief introduction, I would like to discuss the main drivers of the review, the main elements of the Commission proposals submitted in January 2012, and the likely next steps in the reform process.

The main focus in my remarks is on ensuring "more effective and more consistent" data protection across the EU. Data protection can *only* serve its purpose if it is applied *in practice*, and its value in practice depends upon the *protection* it is able to provide. Here, we have some work to do in our increasingly technology driven and globalising world. The need for more effective and consistent protection will therefore come back at different stages in my remarks.

Role of EDPS

First, a few words on the role of the European Data Protection Supervisor (EDPS). This is an independent authority, clearly different from the European Commission, with a number of specific tasks versus the Commission and other EU institutions. The EDPS is an EU body of its own. Its first task is to monitor the Commission and other EU institutions and to ensure that they comply with EU Data Protection law when they process personal data. For this purpose, it has far reaching supervision and enforcement powers.

Its second task is to advise the Commission, the Council and the Parliament on new legislation with an impact on data protection. In some cases, it can also request the Court of Justice to be admitted in intervention and thus contribute its views on a

[1] Revised version of the lecture delivered at the 5th Swiss Data Protection Law Day on 15 June 2012 at the University of Fribourg, Switzerland. Published in: Astrid Epiney /Tobias Fasnacht (Hrsg./ed.), "Die Entwicklung der europarechtlichen Vorgaben im Bereich des Datenschutzes und Implikationen für die Schweiz" / "Le développement du droit européen en matière de protection des données et ses implications pour la Suisse", Zürich 2012, p. 15-21.

certain case, with interesting data protection aspects. On our website, you will find various examples of such cases. Here, the EDPS can only rely on convincing arguments.

The third task is cooperating with other data protection authorities, mostly at national level, to improve the consistency of data protection in the EU. Here again, the EDPS can only rely on authority and diplomacy, as all national data protection authorities are independent, and the EDPS is only competent at EU level. These roles are based on Regulation (EC) Nr 45/2001, with basically implemented the Data Protection Directive 95/46/EC at EU level.

The Review of the EU legal framework for data protection is a subject that obviously comes within the second and the third tasks. We have therefore been consulted about the Commission proposals, and worked with national colleagues to provide input and feedback to the Commission, at different points in time. At the EDPS website you will find more information on these activities.

EU Data Protection

Secondly, let me remind you that "protection of personal data" is a concept that is separate from, but also closely related to the right to "respect for private life" laid down in Article 8 of the European Convention on Human Rights (ECHR). Basic principles for data protection were set out in the Council of Europe's Convention on Data Protection, also known as Convention 108, which was ratified by more than 40 European states, including Switzerland. This convention enabled a more proactive and systematic protection of personal data, as it applies, in principle, to all personal data, regardless of whether the right to privacy is at stake.

The principles of Convention 108 were implemented into national laws. The emerging risk of divergence among national laws caused the EU to become involved. This led to adoption of Directive 95/46/EC and a number of more specific instruments such as Directive 2002/58/EC, also known as the e-Privacy Directive. A more recent step in 2008 was the adoption of general rules in the area of police and judicial cooperation in criminal matters. In other words, the EU legal framework for data protection involves more instruments than Directive 95/46.

Charter and Lisbon Treaty

Two more elements should be mentioned: first, the adoption of the European Charter of fundamental rights in 2000, initially only as a political document. Although based on the European Convention on Human Rights, it also contained innovations, such as the recognition of a right to the protection of personal data (Article 8), in addition to a right to respect for private and family life (Article 7).

Secondly, the entry into force of a set of new treaties for the EU (Lisbon Treaty), at the end of 2009, which turned the Charter into a binding document, and also inserted a horizontal legal basis for legislation on data protection, no longer dependent on the needs of the internal market, but fully reflecting the nature of data protection as a fundamental right, with specific characteristics in a modern information society (Article 16 TFEU). This confirmed a legal development of almost four decades.

Drivers of EU Review

Now back to the current review of the EU legal framework for data protection. Why is this review taking place? This is basically for three reasons. The first reason is that there is a need to update the current framework, and more specifically Directive 95/46 which is still the key element of the framework. And "updating" means in this case, most of all, ensuring its continued effectiveness in practice.

When the Directive was adopted, the Internet barely existed, and we now live in a world where all this is becoming increasingly relevant, so we also need stronger safeguards that deliver good results in practice. The challenges of new technologies and globalisation really require some imaginative innovation to ensure a more effective protection.

The second reason is that the current framework has given rise to increasing diversity and complexity, if only for the reason that a Directive is transposed into national law – that is its nature – and we now have ended up with 27 versions of the same basic principles. That is simply too much, and translates into costs, but also a loss of effectiveness.

In other words, there is a need to scale up harmonisation, and make the system not only stronger and more effective in practice, but also more consistent. This will lead to a reduction of *unhelpful* diversity and complexity.

The third reason has to do with the new legal framework of the EU. The Lisbon Treaty has put a strong emphasis on fundamental rights. Among them a special provision on the protection of personal data in Article 8 of the Charter of fundamental rights, and a new horizontal legal basis in Article 16 TFEU providing for comprehensive protection in all EU policy areas, regardless of whether it relates to the internal market, law enforcement, or almost any other part of the public sector.

So, the review of the framework is all about stronger, more effective, more consistent, and more comprehensive protection of personal data.

If we now look at what is on the table, we see a package of at least two main proposals: a Directive for – briefly put – the law enforcement area, and a directly binding Regulation for what is now still Directive 95/46, applying to the commercial areas and the public sector, other than law enforcement.

This architecture in itself signals that there is a problem with the comprehensiveness of the package. And indeed, if you look more closely, this is where the main weaknesses of the package can be found. The level of protection in the proposed Directive is substantially lower than in the proposed Regulation.

This can be analysed on its own merits, but exchange of data between public and private entities, e.g. law enforcement and banks, telephone, travelling etc is increasing, and a lack of balance will have practical consequences in a wider field.

Continuity and change

But if we now focus on the Regulation, there are some main messages which need to be kept in mind.

The first one is that – in spite of all innovation – there is a lot of continuity. All basic concepts and principles that we have now will continue to exist, subject to some

clarification and some innovation. An example of innovation is that there is now a stronger emphasis on data minimisation: i.e. not more data than strictly necessary. Another example is the recognition of "Privacy by Design" as a general principle.

Where the innovation comes in, it is mainly about "making data protection more effective in practice". This implies, as we will see, a strong emphasis on implementation of principles, and on enforcement of rights and obligations, to ensure that protection is delivered in practice.

At the same time, the Regulation provides for simplification and reduction of costs. A clear example is that prior notification of processing operations has been eliminated. This is only required in situations of specific risks. The Regulation also provides for a one-stop-shop for companies with establishments in different member states. This involves the introduction of a lead DPA.

A directly binding Regulation will of course also bring much greater harmonisation – in principle: one single applicable law in all Member States – and greater consistency. In itself, this will also bring an important simplification and reduction of costs for companies operating in different member states.

General scope

Let me also emphasize that the proposed Regulation has a general scope: it will apply both in the private and in the public sector. This is completely consistent with the situation under the present Directive 95/46. The possibility of a systematic distinction in this Directive between the public and the private sector was explicitly considered and rejected.

This comprehensive approach of the present Directive has been feasible, because of the fact that some of its provisions – referring to public tasks – are more relevant for public bodies and other provisions – referring to contracts or legitimate interests – are more relevant for private actors.

The ECJ has clearly explained in its judgment in the *Rechnungshof* case (May 2003) that the present Directive also applies in the public sector of a member state.

However, it also emphasized that national law can only serve as a legitimate ground for processing if it complies with fundamental rights.

This position is only reinforced by the fact that Article 8 of the EU Charter now also provides for an explicit recognition of the right to the protection of personal data, and that Article 16 TFEU provides an explicit horizontal legal basis for the adoption of rules on the protection of personal data, both at EU level and in the member states, when they are acting within the scope of EU law.

At the same time, a much closer analysis of the relationship between EU law and national law on the basis of the proposed Regulation is needed. The impression that the Regulation will simply replace all relevant national law is not correct. There are at least four different ways in which national law and EU law will co-exist and interact. Among them also the fact that the Regulation will build on national law in much the same way as happened in the *Rechnungshof* case. It may well be that more space is needed for an even better interaction between EU law and national law.

If we come to the substance of the Regulation, it strengthens the roles of the key players: the data subject, the responsible organisation, and the regulatory authorities.

User control

The first perspective could also be seen as enhancing user control. The current rights of the data subject have all been confirmed, but strengthened and extended.

The requirement of consent has been clarified: *when* you need it, it needs to be real and robust consent. There is also a stronger right to object. There are stronger means to ensure that the rights of the data subject are respected in practice. There is more emphasis on transparency. There is a provision introducing a collective action, not a class action in US style, but still organisations acting on behalf of their members or constituencies.

There is also much talk about the "right to be forgotten", but at further analysis, it is basically an emphasis on deleting data when there is not a good enough reason to

keep them. The right to data portability is basically also a specification of the present right to require a copy of personal data, in a particular format.

Responsibility

The biggest emphasis is on real responsibility of responsible organisations. Responsibility is not a concept that only comes at the end, when something has gone wrong. Instead, it comes as an obligation to develop good data management in practice. This appears in language such as *taking all appropriate measures to ensure compliance*, and *verifying and demonstrating that these measures continue to be effective*.

This is one of the major shifts. It also implies that the burden of proof is in many cases on the responsible organisation, i.e. to demonstrate that there is an adequate legal basis, that consent is real consent, and that measures continue to be effective.

The Regulation also provides for a number of specific requirements, such as the need for a privacy impact assessment, the keeping of documentation, and the appointment of a data protection officer. Some of those provisions, especially on documentation, are in my view overly detailed and would require some modification to make them more appropriate. Some exceptions in the same provisions may not be fully justified. A better balance in this part of the proposal may in fact solve both problems.

A general provision on security breach notification is also included. EU law now provides for such a notification only in the case of telecommunication providers.

Supervision and enforcement

A third main emphasis in the Regulation is on the need for more effective supervision and enforcement. The safeguards for complete independence of data protection authorities have been strengthened fully in line with the ECJ judgment in the case *Commission vs Germany*.

The Regulation also provides for regulators with strong enforcement powers in all Member States. Administrative fines of millions of euros - competition size fines – catch a lot of attention, but the message is: if this is important, it should be dealt with

accordingly. This will therefore drive "data protection" higher on the agenda of corporate boardrooms, which is welcome.

If we look more closely, we see a practice of more vigorous enforcement, with various means: remedial sanctions, administrative fines, and also some increased civil liabilities.

International cooperation among data protection authorities is also strongly encouraged and facilitated. The introduction of a lead authority for companies with multiple establishments is welcome, but this lead authority will not be acting on its own, but in fact be part of a network of close cooperation with other competent authorities.

Very important is the introduction of a consistency mechanism in the context of a European Data Protection Board, which is to be built on the basis of the present group of data protection authorities ("Article 29 Working Party"). This mechanism will ensure consistent outcomes of supervision and enforcement in all member states. Its secretariat will be provided by the EDPS.

Global Privacy

A final element is the wider international dimension of the Regulation, in two ways. The scope of the Regulation has been clarified and extended. These provisions now apply not only to all processing in the context of an establishment in the EU, but also when from a third country, goods or services are delivered on the European market, or when the behaviour of Europeans is being monitored online.

This is a reality on the Internet nowadays. At the same time, it is a realistic approach that builds on an increasing synergy of thinking on data protection around the world.

As to other international aspects, also provisions on trans-border data flows have been extended and in some ways streamlined and simplified. There is a specific provision now on Binding Corporate Rules, with also a number of simplifications.

Let me also mention here that international cooperation is developing among data protection authorities in a wider context – e.g. between the Federal Trade Commission in the US and DPAs in the EU – in a global network (GPEN). This will make it better possible to deal with global actors on the Internet. This is also based on a growing convergence of data protection principles and practices around the world.

Final remarks

In conclusion, my view is that this is a very welcome proposal, but subject to certain improvements of some important elements.

Apart from the current lack of balance between the Regulation and the Directive for law enforcement, this applies to the possible need for more space for interaction between EU law and national law, and the need to reconsider some of the present exceptions, including those for small and medium enterprise. In my view, it is *essential* that general provisions are inherently *scalable*. Inappropriate specifications may only call for unnecessary exceptions.

Finally, a word on procedure: discussions are now taking place in Council and Parliament. This will not take a few months. My guess is that we will see some conclusions in the course of next year, probably under the Irish presidency.

So, in any case by 2014, I would think, the main proposal has a good chance of being adopted. I would expect that the Regulation will make it to the end, with some necessary improvements obviously.