

**RISE Conference: "Ethics and Governance of Biometrics and Identification Technologies", Brussels, 9 December 2010**

*Peter Hustinx*

*European Data Protection Supervisor*

**"Recent developments in EU data protection: stepping up to more comprehensive and more effective protection"**

**Speaking points**

- It is a pleasure to speak at this conference on "Ethics and Governance of Biometrics and Identification Technologies". The aim of my remarks today is to inform you about the most recent developments in EU data protection, a subject that is extremely relevant for your work.
- Developments in biometrics and ID technologies are highly relevant to our work at EDPS, and the work conducted in the framework of the RISE project is therefore of great interest to us.
- The fundamental right to the protection of personal data is important for its own sake, but also as it has strong connections with other fundamental rights, apart from the right to privacy, such as non-discrimination or the freedom of movement. These rights will all be affected by large scale use of biometrics and other ID technologies.
- Your agenda - involving exchange of data by public authorities in different contexts, such as law enforcement (especially Prüm), border management, public services - shows how much public authorities in the EU - and in other parts of the world as well - now rely on the collection and use of personal data, and in particular biometrics.
- So it is important to promote a responsible use of biometrics, where the necessary safeguards are put in place at the right time. In other words, the data protection legal framework must fully and effectively apply to the use of biometrics and other ID technologies.
- The review of the data protection framework in the EU will keep us busy in the next few years. We must seize the opportunity to make data protection more effective and more relevant in practice, in an ever more ICT dependent society.
- We are facing great challenges, but also great opportunities: data protection enjoys a high profile in the political debate, be it about PNR, body scanners, social networks or large-scale IT systems for border management or law enforcement. The European Courts are also dealing with a growing number of data protection issues.

- Now, let me come to the main subject of my intervention today: the Commission is in the middle of a thorough review of the current EU framework for data protection.

### **The Commission's Communication**

- Only one month ago, the European Commission published a Communication on "a comprehensive approach to personal data protection in the European Union", as the final stage in the consultation process leading to a review of the 1995 Data Protection Directive.
- Based on its work on this subject, the Commission identified the need to address several key priorities. The first priority is to respond to the impact of new technologies. Three further priorities - enhancing the single market, providing stronger institutional arrangements and improving coherence - address a core problem that unites pretty much everybody concerned with the current framework: the lack of consistency and predictability in the implementation of the Directive. This consistency will be tested even further by the broader scope of the new legal framework as a result of the Lisbon Treaty.
- A further priority will be to strengthen international measures, to ensure protection of personal data on a global level. On today's agenda, we also see speakers from India and Israel. This is of course one more illustration that data protection is a global issue, which cannot possibly be dealt with by the EU in isolation from the rest of the world.
- The priorities of the Commission are translated into several specific objectives to which I will return shortly.

### **Reaction of EDPS**

- First of all, we welcome the Commission's Communication, we agree with its main lines and with the issues identified. But the next step will be even more important: a proposal for a new legal framework for an effective protection.
- In the future, this will also require the active involvement of the European Parliament and the Council, but at this stage our focus is still on the Commission.
- Let me be very clear at this point. There is no room for mistakes: the challenges are enormous. That is why the proposed solutions must be equally ambitious and actually enhance the effectiveness of the instruments of data protection.
- We will follow the work of the Commission closely, in a constructive way. Early next year, we will publish an opinion going into more details, but I want to share with you some main points today.

#### ***A. The need for strong and effective protection***

- Data protection is not an abstract thing. It relates to everybody's life, every moment of every day. It concerns our family, our work, our preferences, our lifestyle, our security, our health. It concerns us all directly! We must be aware of how information relating to us is used or abused, and we must be able to exercise our rights over it.
- Strong data protection supports and underpins other issues, such as the European economy, our security, and also accountability of governments. Data protection fosters trust, and trust is an essential component of economic development as well as of effective government.
- Economic development goes hand in hand with the introduction of new technologies and services. Data protection should be an integral part of digital services and technological developments such as social networks, ID technologies, road toll collecting, geo-localisation, etc.
- Governments also must be accountable for what they do with the personal data which they use for the different public interests they serve. This varies from the use of data as a support of policies in areas like public health, transport or taxation, to publication of some personal data on the internet for reasons of transparency, or to surveillance of certain individuals for law enforcement purposes.
- For all these reasons, a strong and effective protection of personal data is needed. And it is needed - today more than ever - in a technological society where the risks for privacy and protection of personal data have increased in ways we could not conceive in 1995, when the Data Protection Directive was adopted.

### ***B. The need for reviewing legislation***

- Since 1995, our society has undergone fundamental changes due to rapid technological developments and globalisation. Nevertheless, we are convinced that general principles of data protection remain valid today. But, there is an imperative need to ensure full and effective protection in the future.
- Today's technology has allowed the exchange of data on an unprecedented scale. At the same time, data flows have become more subtle and less detectable. Biometrics, social networks, cloud computing, behavioural advertising, data surveillance - they all pose enormous challenges for data protection!
- Data protection is a fundamental right - as clearly stated in the EU Charter - and governments are accountable for ensuring effective protection of this fundamental right. The Lisbon Treaty confirms this. It mandates the Council and the European Parliament to adopt consistent legislation on data protection.
- For data protection, the Lisbon Treaty really makes a difference. The same level of protection must be given, also in the area of law enforcement. The abolition of the pillar structure is a major step for data protection.

- And last but not least, the EU Charter of Fundamental Rights became binding. Last month, for the first time, the Court of Justice used the Charter to decide on the lawfulness of data processing. This was in the German *Schecke*-case.
- The review is also a great opportunity for improving other aspects of the current framework, such as ensuring a better harmonisation of national laws, clarifying the existing rules and strengthening the enforcement. Let me say a few words about each of these points.

### ***C. Main points for the new framework***

- Harmonisation/internal market: we support the Commission's objective to further harmonise national legislation of EU Member States: less margin of manoeuvre and more precise provisions in the new framework will bring more legal certainty, to the benefit of data controllers as well as individuals. These are essential conditions in a digital market where data flow without borders. Harmonisation can also significantly reduce administrative burdens.
- To achieve full harmonisation we must not be afraid to reconsider the type of legal instrument for data protection: a directly applicable European regulation may be the most effective means to protect fundamental rights while ensuring the internal market objectives.
- Technologically neutral. The new legal framework must be effective for a large number of years, and at the same time not hamper technological developments. On the other hand, the framework must bring more certainty for companies and for individuals.
- To be more precise, it must address some issues which are typically linked with some new technologies, like IP addresses and RFID, but also remain technology neutral. Whether it will address biometrics (including fingerprints and DNA) as a category of data deserving particular protection is still an open question.
- At the same time, there is an opportunity for new rights in an electronic environment, like the 'right to be forgotten'. It could be attractive to include such a right - subject to conditions - in the new legal framework.
- Privacy by design and accountability. We strongly support the inclusion of these two new principles in the revised data protection framework. Because we firmly believe that both will contribute effectively to real compliance with data protection rules.
- The *accountability* principle will require organisations - in public and private sector - to put in place measures to ensure the protection of data. Data protection should be a concern for top management. In doing so, they will have to consider the risks, types of data, and other relevant aspects of data processing.

- Obviously such measures should be scalable: small SMEs with negligible processing of personal data should not be subject to the same requirements as bigger corporations that manage large amounts of data.
- The *privacy by design* principle means embedding privacy as the default into the design, operation and management of ICT and systems, across the entire information life cycle. Therefore, *privacy by design* will require organisations to roll out products and services with privacy embedded features.
- Taking privacy and data protection into account in the earliest stages of the design of ICT is crucial because of the difficulty in doing so at later stages, when the products or services are already in the market.
- At this point, a few more words about *biometrics*. Biometrics (e.g. fingerprints) has many advantages, but also weaknesses. For example, not everyone can enrol - an issue you have discussed in previous RISE events. Moreover, there is an inevitable error rate in large-scale biometric systems.
- Biometric systems are inherently based on probability. This is why one needs to apply false-rejection and false-acceptance rates. In this respect, I have always emphasised that those who are responsible for data processing must proceed on the assumption that a biometric system is not perfect. False-rejection and false-acceptance rates should be matched to the ultimate purpose of the system.
- This is particularly important with regard to large-scale applications. The necessary organisational and legal arrangements need to be taken to provide for rapid and effective appeal procedures for victims of erroneous rejection.
- Security breaches. We also support a wider scope for security breach notifications, which currently only apply to ISPs and network operators. This should eventually apply to all data controllers, also in the public sector. We think that security breach notifications will be a good tool to make people more aware of data protection and it will also enhance security in companies.
- Globalisation. The increasingly globalised world economy relies on the free flow of information, including personal data. Data protection is not meant to unduly restrict such flows.
- However, the protection of individuals' privacy would be jeopardised if controllers could freely move the data outside the EU borders, to jurisdictions affording none or little protection. If global data protection standards were developed and applied across the globe, the rationale behind cross border rules would be minimised.
- We support the development of international standards on data protection. A lot of energy is invested in the development of such standards by the data protection community. One of the most prominent initiatives was headed by the Spanish DPA with input from different stakeholders and resulted in the presentation of "International Standards on the Protection of Personal Data and Privacy" at the

International Conference of Data Protection Commissioners in Madrid in November 2009.

- The standards published in Madrid take into account core data protection principles, including fairness, necessity, proportionality and transparency, and crucial safeguards such as accountability obligations for data controllers. They also include innovative obligations like the need to integrate *privacy by design* in the development of new technological tools. Finally, they provide for access and rectification rights to the data subjects, and for judicial and administrative redress.
- However, although a lot has been achieved, we have to deal with the reality of still rather patchy data protection standards across the world.
- Therefore, there is a need to maintain some provisions on data transfers. However, we fully agree with the Commission on the need to clarify and simplify them and to bring them more up to date. Binding corporate rules is one of the mechanisms for data transfer that needs to be streamlined in order to constitute an effective mechanism to legitimise such transfers.
- Data transfers involving public sector bodies also deserve attention. We fully support the need to define the minimum principles guaranteeing a high level of protection for personal data as a condition to the exchange of such data. Such principles should be used as a benchmark for subsequent bilateral or multilateral agreements to be concluded by the EU and by its Member States with third countries.
- Data protection for police and justice. In the area of police and justice, there is a growing exchange of data between EU countries, between the EU and the rest of the world, and, by and large, between public authorities and the private sector such as the telecom sector, airlines or banks.
- Systems or programmes for exchange of information are planned and developed at a rapid pace: e.g. Prüm, Visa Information System or a possible EU Entry-Exit system. Let me also mention the discussions concerning the interoperability between these systems and the - in our view quite problematic - key role for biometrics in that context.
- These exchanges are presented as necessary in the fight against crime and terrorism, but also to manage immigration better. Of course, we need to consider and verify to which extent they are really necessary.
- However, 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 a Council Framework Decision from 2008. This Framework Decision is by far not sufficient; the Communication of the Commission clearly highlights its deficiencies.
- In our view, it is evident that police and justice should 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.

- Including police and justice in the general framework would offer more guarantees to citizens but also make the task of police authorities easier. Having to apply different sets of rules is unduly cumbersome, needlessly time-consuming, and stands in the way of meaningful international cooperation.
- Roles of data protection authorities: There is a need for strengthening the independence, resources and enforcement powers of the data protection authorities and for strong and consistent enforcement actions throughout the EU, because we often deal with multinational or even global players.
- The existence of data protection authorities endowed with strong powers and competences is also important for the individual. In particular, since the most vulnerable people in society (e.g. asylum seekers, beneficiaries of social help) are highly dependent on government, protective legislation and effective data protection authorities are a vital equaliser in this relationship.
- We support the objective of the Commission to improve not only collaboration and coordination between DPAs but especially the enforcement of common positions taken at the level of the Article 29 Working Party. There should also be one effective answer to data issues raised by multinational companies active within the EU.
- The need for effective enforcement also requires the possibility of collective actions to facilitate redress for data subjects and reinforce compliance by data controllers.

#### ***D. And in the meantime....***

- In the meantime, we must ensure the effectiveness of existing arrangements. How can this be done?
- First, we should concentrate on enforcement, at national and at EU level. The existing legal framework must be applied effectively, also when we deal with technological phenomena and global players. At EU level, the Commission will have to continue to be vigilant and open infringement proceedings where necessary, as it did recently in connection with the requirement of “complete independence” of DPAs in a case against Germany. Member States are obliged to ensure the correct implementation of existing legal instruments.
- Second, it is important to ensure that data protection principles are "built-in" in new regulations which may have an impact, directly or indirectly, on data protection. Data protection authorities should make full use of their advisory powers to ensure such a proactive approach.
- Third, ensuring cooperation between the various actors - both at European and at international level - is essential. The Article 29 Working Party plays an important role with a view to promoting uniform application in Europe.

- However, data processing has now acquired an increasingly global dimension. Hence, it is important to reinforce the international instruments of cooperation, and work together with third countries, international organisations and international networks. It is very positive that the US Federal Trade Commission has now joined the family of Privacy and Data Protection Commissioners. The FTC is also quite active in setting up a Global Privacy Enforcement Network.

### *Conclusion*

- My key message today is that the reform of the EU legal framework for data protection is **very relevant and timely**, that the focus should be on providing more **effective protection** in a European information society of 2015 and beyond, and that the Commission now needs to be truly **ambitious** to come up with adequate proposals by mid next year.
- In the meantime, it is important that we at EDPS continue to do our work in **supervision, consultation and cooperation**, and that all EU institutions and bodies continue to improve the way in which they comply with current data protection requirements in practice, when they process personal data and develop legislation or policies with an impact on data protection.
- This also applies - without any doubt - to the use of biometrics and ID technologies. Let me therefore wish you a very productive conference.