Data protection in a transatlantic perspective : future EU-US data protection agreement in the framework of police and judicial cooperation in criminal matters

Gayrel, Claire

Publication date:
2010

Document Version
Publisher's PDF, also known as Version of record

LIBE HEARING

DATA PROTECTION IN A TRANSATLANTIC PERSPECTIVE

FUTURE EU-US DATA PROTECTION AGREEMENT IN THE FRAMEWORK OF POLICE AND JUDICIAL COOPERATION IN CRIMINAL MATTERS

Monday 25 October 2010
Brussels

CLAIRE GAYREL
Researcher at CRID (Research Centre on IT and Law)
University of Namur (FUNDP)
Namur – Belgium
claire.gayrel@fundp.ac.be

Ensuring Effective Enforcement Mechanisms of Data Protection in the Future EU-US Agreement on Data Protection

Thank you for the invitation to this public hearing. It is for me an honour and of great interest to discuss the complex matter of the future EU-US data protection agreement in criminal matters. The perspective of a General Data Protection Transatlantic Agreement aiming at strengthening the EU-US cooperation in criminal matters raises many issues, from an external observer point of view. These can unfortunately not extensively be all dealt with today. Let's however discuss them.

If the EU-US High Level Contact Group (HLCG) Final Report on information sharing and privacy and personal data protection appears to constitute a basis for future negotiations, it must be said that it does not address a range of crucial issues (many of which have been identified by the European Data Protection Supervisor in its opinion of 11 November 2008). Whether these issues have been the object of informal debates have not been made public. This makes it difficult for observers to build useful comments on what has or has not already been done. **In order to have a proper public debate on such a sensitive issue, documents must be made publicly available.**

The Study[1] conducted by Rocco Bellanova and Paul De Hert on request of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs, addresses in further detail important incompatibility points between the EU and the US data protection regimes.

Among the main concerns raised by experts is application of the **purpose limitation principle**, which entails different implications in particular with respect of the concept of further use for "compatible purpose". In the US, the application of the so-called "routine use" allowing inter-agencies transfers of data has shown strong discrepancies with the European conception of "compatible" purposes. However, it must be highlighted that even on the European side, there is a trend to extend the meaning of compatible purposes. The principle of interoperability, along with the increasing use of personal data primary collected for commercial purposes and further used for law enforcement (Data retention Directive, future PNR European system) are some of the illustrations that the purpose limitation principle is also highly under pressure in the European data protection system[2].

A second major issue relates to **the retention periods** in the US. At worst, these are not regulated at all. At best, these are extensively long. This matter should be addressed in the specific agreements on the exchange of personal data.

I would now address some of other issues that have insufficiently been dealt with by the EU-US HLCG, focussing mainly on the enforcement mechanisms of data protection principles.

I. The adequacy, a European requirement, but also a method, entailing core data protection principles and objectives

My first point is that, though the EU is not bound by the *adequacy requirement* in the framework of such an agreement on the protection of personal data, the EU should nevertheless be consistent with the *adequacy as a method.*

I share the view of the EDPS that strongly recommends that adequacy should be the grid analysis to follow when assessing the level of protection of personal data provided in the general Agreement. The adequacy requirement is a core principle of European data protection in the matter of trans-border data flows. It is provided in the Additional Protocol 181 to the European Convention 108 – to which 19 Member States are nowadays bound –, in the European Data Protection Directive 95/46, in the Europol and Eurojust conventions and in the Framework decision on the protection of personal data in the former third pillar matters. Though none of these instruments legally require an adequacy assessment in the framework of a EU-third country agreement on the protection of personal data, adequacy should nevertheless be referred to as the assessment tool, since it allows ensuring consistency in the

[1] BELLANOVA, Rocco, DE HERT, Paul, "Data Protection From a Transatlantic Perspective: the EU and US Move Toward a EU-US Data Protection Agreement?", *Study Requested by the LIBE Committee*, European Parliament, Brussels, 2008

[2] See DUMORTIER, F., GAYREL, C., JOURET, J., MOREAU, D., POULLET., Y., "La protection des données personnelles dans l'Espace européen de liberté, de sécurité et de justice", *Journal de Droit Européen*, n°166, February 2010

European trans-border data flow policy. Rather than a requirement, adequacy should be used here as a method, entailing core principles and objectives. The grid provided by the Working Party 29 in its Working Paper 12, has now been well experienced in the first pillar. It is mostly inspired from the European Convention 108, which provides the core data protection principles applicable in every member States. A similar grid analysis must be adapted with respect to trans-border data flows and the protection of personal data in criminal matters in order to delineate the standards of protection that the EU is expecting from its partners.

The perspective of a general EU-US data protection Agreement in the new constitutional context of the Lisbon Treaty provides the opportunity for the EU to break with the current presumption of adequacy surrounding every EU-US Agreements in criminal matters. Indeed, neither Europol, nor Eurojust has found relevant to assess the protection offered by the US, though these agencies are required to do so and have done so in their other agreements with third states. The Mutual Legal Assistance Agreement has also put aside the adequacy method. It is time to break with EU-US custom-made Agreements in this matter. **The progressive development of an adequacy presumption with regard to the US Data protection system in criminal matters undermines the EU's data protection policy aiming at building adequacy bridges with other third countries**. It is even more important since the adequacy experience in the first pillar has shown that third states aiming at being considered as providing an adequate level of protection often take inspiration from legislations of other third states that have been considered adequate by the EU. An inadequate level of protection in the EU-US Agreement could be considered by other third states as a precedent, which would in turn puts in difficulty the EU when requiring a higher level of protection from other states. Consistency in this matter is fundamental and adequacy is the relevant tool.

II. The adequacy method: the relevant and necessary tool as to the assessment of enforcement mechanisms

This previous recommendation leads me to the second point of my presentation: the adequacy method is the relevant tool as to the assessment of enforcement mechanisms which are at the heart of the objectives of any data protection legislations.

These objectives have been identified by the Working Party 29 as follows: a) to deliver a high level of compliance with the rules (implying the existence of systems of verification by independent authorities); b) to provide support and help to data subjects in the exercise of their rights and; c) to provide appropriate redress to the injured party when rules are not complied with.[3]

a) Providing a high level of compliance with the rules

As has been underscored by the Working Party 29, "*no system can guarantee a hundred percent compliance, but some are better than others. A good system is*

[3] Working Document 12 of the Working Party 29 relating to "*Transfers of Personal Data to Third Countries: Applying Article 25 and 26 of the EU Data Protection Directive*" of 24 July 1998.

generally characterised by ***a high degree of awareness*** *among data controllers of their obligations, and among data subjects of their rights and the means of exercising them. The existence of* ***effective and dissuasive sanctions*** *can play an important role in ensuring respect for rules, as of course can* ***systems of direct verification by authorities, auditors, or independent data protection officials***".

As far as the first objective is concerned, issues are raised as to the difference of approaches of independent data protection authorities in the US and in the EU. It appears that US Privacy agencies (Department of Homeland Security Office, the President's Civil Liberties and Privacy Oversight Board among others) are actually advisory bodies and cannot be considered as structurally independent when compared to EU Data Protection Authorities. However, structural independence, with the exception of the judiciary power, is rarely admissible and/or constitutionally possible in many legal systems. The experience of the adequacy requirement on this point in first pillar decisions shows that some countries have been considered as providing an adequate level of protection, though the Data Protection Authorities established in such countries were not "structurally" independent[4]. Instead, **independence requires an assessment as a whole** and must be sought in a wide range of guarantees: the financial resources of the DPA, mode of allocation of these financial resources (is there a financial independence?), guarantees as to the independence of the members (rules applying to the nomination and termination members' mandate, incompatibility regimes, professional secrecy rules), assessment of the functional independence (is there an effective staff? Are the right competences gathered?), and of course in the normative, investigation and sanctions powers of the DPA. These are examples of guarantees that may counterbalance, if rightly applied, the lack of structural independence. US proposals aiming at satisfy the independence criterion must therefore cover all these aspects in order to reach a reasonable compromise.

b) Providing support and help to data subjects in the exercise of their rights

As far as the second objective is concerned, the Working Party 29 has stated that "*The individual must be able to enforce his/her rights rapidly and effectively, and without prohibitive cost. To do so there must be some sort of institutional mechanism allowing independent investigation of complaints."*

This objective must be at the heart of the EU-US debates and the means to achieve it should be clearly delineated in the Agreement – notably with respect to the effectiveness of the exercise of one's rights and the means of assistance to provide to data subjects. This objective is even more important in the context of cooperation in criminal matters, since the rights of the data subjects are more limited. In practice, National Data Protection Authorities should be involved, being the interfaces between the data subjects and the foreign authority requested to provide access, rectification

[4] To quote one, in the Uruguayan data protection system, the Data Protection Authority has been created as a body dependent on AGESIC (Agencia para el Desarollo del Gobierno de Gestion Electronica y la Societad de la Informacion y del conocimiento) which in turn depends on the Presidency of the Republic. When applying the WP12 requirement of independence, the Working Party 29 have taken in consideration a series of other guarantees and concluded that these last came to satisfy the independence requirement and this, in spite of the structural link between AGESIC (and the Presidency) and the DPA. See Opinion 6/2010 of the Working Party 29 on the level of protection of personal data in the Eastern Republic of Uruguay, 12 October 2010.

or opposition. This would allow "indirect" access/rectifications rights when necessary. The possibility to request assistance from the DPA of a data subject (meaning the DPA on the basis of one's nationality or place of residence) in the exercise of his/her rights should reduce the practical barriers involved by transfers toward the other side of the Atlantic. I mainly refer to problems such as language skills, lack of knowledge of the foreign system, prohibitive cost in case of recourse to a lawyer…
In brief, **strengthening cooperation between Data protection supervisory bodies of both sides of the Atlantic is the necessary corollary to the strengthening of police and judicial cooperation of national authorities for law enforcement purposes.**

c) Providing appropriate redress

In this respect, the Working Party 29 states that "*This is a key element which must involve a system of independent adjudication or arbitration which allows compensation to be paid and sanctions imposed where appropriate."*

The EU-US HLCG Report has duly raised attention to the discrepancies between the European and American legal systems in providing redress, especially as regards the non-availability of civil remedies for non-US persons. The right to redress, under the US system, is limited at two levels. First, only "*US persons*" are entitled to launch a redress action under the US Privacy Act[5], excluding by thus aliens. Second, the admissibility of a civil action is subject to two conditions: the agency's behaviour must prove to have produced an adverse effect on the individual[6], and the agency must have acted "*in a manner which was intentional or wilful*"[7]. The current limitations to redress actions cannot be considered to comply with the European enforcement mechanisms objectives.

It is quite surprising that the EU-US HLCG foremost focussed on the redress mechanisms as an "*outstanding issue*", and that it did not in the same way on the scope of protection of the Privacy Act in itself. The applicability of the Act is limited to information pertaining to US persons and hold by government agencies. Beyond the limitations to the right to redress**, it is the lack of protection of personal data regarding non-US persons and the lack of subsequent judicial review of violations of this Act as a whole, which are at stake.**

Actually, EU and US have developed different approaches concerning supervision. Els De Busser's insightful analysis of data protection in EU and US criminal cooperation has found that "*where the EU ensures a supervision that is organized prior to the gathering of data, the US emphasizes the excluding of evidence after it has been gathered*."[8] On the European side, the exceptions to the data protection principles need to be legal and necessary, as it is the case for the exceptions to the right to private life of Article 8 of the ECHR. This implies that, on a national level, supervision should be organized in order to ensure the legitimacy of gathering personal data or breaching privacy. The independence of this supervision has been

---

[5] Privacy Act of 1974, (a)(2): "*the term "individual" means a citizen of the United States or an alien lawfully admitted for permanent residence*"
[6] Privacy Act of 1974, (g)(1)(D)
[7] Privacy Act of 1974, (g)(4)
[8] DE BUSSER Els, *Data Protection in EU and US Criminal Cooperation*, Maklu, Antwerpen, 2009, p. 302

highlighted as a requirement in ECHR's case law. On the contrary, in the US data protection regime, the many exceptions to the warrant requirement (mainly deriving form the US Patriot Act and the Foreign Intelligence Surveillance Act) and the increasing competences of administrative authorities make the judiciary the ultimate guarantor of privacy rights. In criminal proceedings especially, it appears that "*the supervision of the data protection rules is first and foremost awarded to the exclusionary rule*"[9], which consists in the suppression of evidence gathered in violation of the requirements of data protection by means of pre-trial motion. Since supervision mostly rests on the courts, it is even more important to ensure that the right to judicial review, as firmly laid down in the ECHR and the Charter of Fundamental Rights, is guaranteed to anyone under the US system.

These discrepancies supports the need to put in place strong assistance mechanisms at the level of the DPAs, since the effective exercise of one's rights could primarily be guaranteed at this level, the judiciary being the ultimate level of protection. Proposals from the US concerning this aspect cannot be overlooked.

25 October 2010

[9] *Ibidem*, p. 292