EUROPEAN PARLIAMENT 2009 - 2014

Committee on Civil Liberties, Justice and Home Affairs

10.9.2010

WORKING DOCUMENT 1

Future European Union (EU) - United States of America (US) international agreement on the protection of personal data when transferred and processed for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police and judicial cooperation in criminal matters.

Committee on Civil Liberties, Justice and Home Affairs

Rapporteur: Jan Philipp Albrecht

A discussion on the future EU-US data protection agreement requires some preliminary considerations concerning the approach towards data protection on the two sides of the Atlantic. This is the main aim of the first two working documents which set out to map the main developments and evolutions of the two systems. A third working document will provide comments pertaining to the future data protection agreement.

The EU approach in the field

It has been argued that privacy and data protection have been conceived as 'legal "proxies" for the moral and political ideals of individual and political autonomy. Privacy (self-development) has been seen as freedom from unreasonable constraints (from state or from others) in the construction of one's personality while data protection (seen as 'informational self-determination') has been interpreted as control over some aspects of one's personality one projects on the world.'[1]

Privacy is a cornerstone concept enshrined in Article 8 of the European Convention of Human Rights (ECHR) and Article 7 of the Charter of Fundamental Rights (hereinafter referred to as the Charter).

The **fundamental right to protection of personal data** is enshrined in Article 8 of the Charter, covered under Article 8 of the ECHR and again provided for in the Lisbon Treaty in Article 16 TFEU.

Currently several pieces of legislation have been enacted in the EU and within the context of other international organisations in respect to protection of personal data. In this respect one should recall:

- Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data[2]
- Directive 2002/58/EC on privacy and electronic communications (E-privacy Directive)[3]
- Regulation (EC) Nr. 45/2001 applicable to data processing by EU institutions and bodies[4]
- Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (CFDDP)[5]
- 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CoE 108) together with its 2001 Protocol[6]

In line with the report 'The Future of Privacy' of the Working Party 29 and of the Working Party on Police and Justice (hereinafter referred to as WP PJ), it must be underlined that

1 A Rouvroy and Y Poullet, Self-determination as "the key" concept and A Rouvroy and Y Poullet, 'The right to informational self-determination and the value of self-development Reassessing the importance of privacy for democracy' p. 24.

2 OJ L 281, 23.11.1995, p. 31.

3 OJ L 201, 31.7.2002, p. 37; Revised by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.

4 OJ L 8, 12.1.2001, p. 1.

5 OJ L 350, 30.12.2008, p. 60.

6 ETS No. 108, 28.01.1981 and http://conventions.coe.int/treaty/en/treaties/html/181.htm.

'Directive 95/46/EC is meant as a general legal framework, which could be complemented by specific regimes for data protection for specific sectors.' Such a specific regime is the one imposed by the ePrivacy Directive. Moreover, the Data Protection Directive does not apply to processing by EU institutions (governed by Regulation (EC) Nr. 45/2001) nor to 'the processing of personal data in the course of an activity which falls outside the scope of Community law, such as those provided for by Title V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, Sate security […] and the activities of the State in areas of criminal law' (Art. 3(2)).[7]

Current rules on Data Protection for Police and Judicial Cooperation

The 2008/977/JHA CFDDP is currently the instrument that applies to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means, of personal data which form part of a filing system or are intended to form part of a filing system. The CFDDP is 'without prejudice to essential national security interests and specific intelligence activities in the field of national security.'

The 'Future of Privacy' report sees the CFDDP as 'a first step towards a general framework in the former third pillar but is far from complete. It is only applicable in cross border situations. It seems to lack essential elements and tools to effectively deal with working methods in the area of law enforcement.'[8]

Article 6 of the CFDDP foresees that the processing of special categories of data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership and the processing of data concerning health or sex life) shall be permitted only when this is strictly necessary and when the national law provides adequate safeguards. In contrast, Article 6 CoE 108 in its Article 6 establishes that such personal data *may not be processed automatically unless domestic law provides appropriate safeguards.*

The CFDDP also provides as regards transfers to competent authorities in third States or to international bodies a mechanism whereby transfer can be allowed under a series of conditions (purpose, receiving body, consent of the Member State) including the requirement of adequacy of the third State or international body concerned (Article 13).

Relations to other instruments

With respect to the relationship of the CFDDP with agreements with third States it is indicated that *it is without prejudice to any obligations and commitments incumbent upon Member States or upon the Union by virtue of bilateral and/or multilateral agreements* with third States *existing at the time of adoption of the CFDDDP. However, it is foreseen that in the application of these agreements, the transfer to a third State of personal data obtained from another Member State, shall be carried out while respecting Article 13(1)(c) or (2), as appropriate* (Article 26).

7 The report also indicates that 'several pieces of sectoral legislation also contain specific rules relating to the processing of personal data (on money laundering, customs legislation or VIS, EURODAC or SIS II legislations).' 02356/09/EN WP 168, adopted on 1 December 2009.

8 (n7) p.25.

The CFDDP also sets out the interaction with acts adopted prior to its entry into force under Title VI TEU and which regulate the exchange of personal data between Member States or the access of designated authorities of Member States to information systems established pursuant to the Treaty establishing the European Community. It indicates that where such acts prescribe specific conditions as regards the use of such data by the receiving Member State they shall take precedence over the provisions of the CFDDP on the use of data received from or made available by another Member State.

Such examples are Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (the so-called Prüm Decision) or Council Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union (the Swedish initiative). These texts make reference to different data protection standards. As regards processing of personal data which is supplied pursuant to the above-mentioned texts it is foreseen that the level of protection that should be guaranteed should be at least equal to that resulting from CoE 108 and its 2001 Additional Protocol[9].

The Europol Decision also sets out its own data protection rules which draw back to the CoE 108 Convention.[10] It must also be mentioned that there exists a supplemental agreement between Europol and US on the exchange of personal data and related information, which provides specific data protection provisions.[11]

From this brief overview it appears that a patchwork of data protection rules is currently at works within the former third pillar setting. The differences can account, as argued by the joint report of WP 29 and WP PJ for 'the specificities of the area covered,' or simply are 'the consequence of a different legislative history'.[12]

Recent developments

Article 16 TFEU of the Lisbon Treaty which entered into force on 1 December 2009 provides for the *adoption under the ordinary legislative procedure (co-decision) of rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data*. Furthermore, the treaty requires that compliance with these rules be subject to the control of independent authorities. This entails that the new legal basis for data protection is to be applicable to all processing taking place in the private and in the public sector, including the processing in the area of police and judicial cooperation and common foreign and security policy. Nevertheless, Declaration 21 attached to the Lisbon Treaty indicates that '*specific rules* on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 TFEU

9 The convention defines a number of principles for the fair and lawful collection and use of data. Notably, data can only be collected for a specific purpose and should not be used for any other reason. Data must be accurate, adequate for this purpose and stored only for as long as is necessary. The convention also establishes the right of access to and rectification of data for the person concerned (data subject), and requires special protection for data of a sensitive nature, for example on religion, political beliefs, genetics or medical information.

10 OJ L 121, 15.5.2009, p.37.

11 http://www.europol.europa.eu/legal/agreements/Agreements/16268-1.pdf

12 (n7) p.7.

may prove necessary because of the specific nature of these fields.'

As regards oversight, a recent ruling of the Court of Justice has clearly indicated that the supervisory authorities 'must enjoy an independence allowing them to perform their duties free from external influence. *That independence precludes not only any influence exercised by the supervised bodies, but also any directions or any other external influence, whether direct or indirect*, which could call into question the performance by those authorities of their task consisting of establishing a fair balance between the protection of the right to private life and the free movement of personal data.'(emphasis added)[13]

In this sense it must also be stressed that reflection has been engaged as regards the review of the data protection framework (having as a benchmark Directive 95/46/EC) with an emphasis on the enforcement of the role of data protection authorities, the need to have one legal framework on data protection at EU level, for the private and the public sectors, including police and judicial cooperation with a high level of protection for individuals, regardless of where their data are being processed and by whom.[14]

13 Commission v. Federal Republic of Germany C-518/07 [30].

14 For further information see http://ec.europa.eu/justice/policies/privacy/news/docs/pr_15_07_10_en.pdf. See also the Opinion on the Principle of accountability of the Working Party 29, 00062/10/EN WP 173 Adopted on 13 July 2010.