CEPS Background Briefing

In preparation for the European Parliament Elections

Informing the Data Protection Debate

Elspeth Guild, Sergio Carrera and Alejandro Eggenschwiler

Many areas of EU policy will be the subject of critical debate and discussion in the campaigns leading up to the European Parliament elections on 4-7 June 2009. Although the broad themes and the relative importance attached to these themes will vary substantially from one member state to another, the issues that have become EU policy and law over the past ten years in the Area of Freedom, Security and Justice deserve informed and consistent analysis. These policies touch the core of every individual's right to liberty and security in an enlarged Europe.

This Background Briefing focuses on data protection. It first sets the scene by outlining the current state of play in EU data protection policy and the next steps that are expected to be taken in the near future. We then present key shortcomings and issues surrounding this policy domain. The concluding section highlights the main challenges in this field and puts forward key recommendations for the next five years.

This Briefing is one in a set of four dealing, respectively, with immigration, asylum, borders and data protection. They have been produced as part of a project: "Informing the Immigration Debate: Preparing for the European Parliament Elections 4-7 June" supported by the Barrow Cadbury Trust, an independent charitable foundation that funds and promotes social justice initiatives (for more information, see http://www.bctrust.org.uk). The Background Briefings aim to inform the debate about these controversial and often technical issues for the political parties as they prepare for the EP elections and address the voting public.

Elspeth Guild is a Professor at the Centre for Migration Law of the Radboud University of Nijmegen (the Netherlands) and a Senior Research Fellow in the Justice and Home Affairs Section at CEPS. Sergio Carrera is a Research Fellow and Head of the Justice and Home Affairs Section at CEPS. Alejandro Eggenschwiler is Research Assistant at CEPS. An earlier version of this Background Briefing was presented at a lunch on April 15th in the European Parliament, organised in cooperation with the office of Baroness Sarah Ludford, Member of the European Parliament, Member of the Committee on Civil Liberties, Justice and Home Affairs and Vice-Chairwoman of the Subcommittee on Human Rights.

CENTRE FOR EUROPEAN POLICY STUDIES

Thinking ahead for Europe

BARROW CADBURY

1. State of Play of the EU Data Protection Legal Framework

The right to data protection in the EU is based upon a set of legal acts belonging to both international and EU law (for a full list of measures adopted in the field of data protection, see Annex). The 1995 Directive on Data Protection[1] is the key piece of legislation as it lays down the general principles that member states must follow in order to guarantee the individual's right to privacy, while ensuring that no restrictions are imposed on the circulation of data between them. The directive applies to the collection, storage, disclosure and dissemination of personal data, both by automatic (electronic databases) and non-automatic means (traditional filing systems), in relation to which it grants the 'data subject' a set of rights, including the right to be informed if data relating to him/her are being processed; the right to obtain the rectification, erasure or blocking of data that have not been lawfully processed; and the right to judicial recourse in the event of any breach of rights conferred during the processing of personal data. In order to address the threats posed by developments in technology to an individual's right to data protection, the directive has been supplemented by two further instruments dealing with privacy in the telecommunications[2] and electronic communications[3] sectors. The main purpose of these is to guarantee the confidentiality of communications by prohibiting any unauthorised listening, taping, storage or other kinds of interception or surveillance.

Privacy and data protection rules are also enshrined in the European Convention for the Protection of Human Rights and Fundamental Freedoms (Art. 8) and Convention 108,[4] both adopted under the auspices of the Council of Europe, as well as in the Charter of Fundamental Rights of the European Union (Arts. 7 and 8).[5] Further, it needs to be underlined that in the EU context there is a European Data Protection Supervisor (EDPS)[6] and a Working Party on the protection of individuals with regard to the processing of personal data,[7] which have been established as independent bodies with supervisory and advisory powers. In particular, the EDPS ensures that EU institutions and bodies process individuals' personal data lawfully; advises the EU decision-making bodies on new legislative proposals and on any issue having an impact on data protection. It also cooperates with national data protection authorities to promote a homogeneous level of data protection in the EU (for a selection of a list of EDPS Opinions, see Annex).[8] The Working Party provides the platform for such cooperation by bringing together the representatives of the national data protection authorities, the EDPS and the European Commission.[9]

The legal framework outlined above applies only to the AFSJ policy domains that are grouped under the Title IV of the TEC (visas, asylum and immigration) – the First Pillar. Data protection issues might also arise in the AFSJ domains, falling under Title VI of the TEU (police and judicial cooperation in criminal matters) – Third Pillar – which are regulated by the recently adopted Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.[10] Such a divide is a consequence of the AFSJ cross-pillar structure that risks lowering the standard and undermining the consistency of data protection in the EU, especially in light of the fact that the Framework Decision does not apply to the processing of a wide range of personal data, including domestic data, data exchanged between member states and third countries and data processed by Europol, Eurojust, the Schengen Information System (SIS) and the Customs Information System (CIS).

2. Shortcomings and Issues

The AFSJ is driven by a firm belief in technology as the solution to every security threat, without consideration for the fact that it could engender more insecurity in terms of fundamental rights and liberties of the individual, especially as regards the right to the protection of personal data as enshrined in Art. 8 of the Charter of Fundamental Rights. The EU has so far developed a number of databases and systems of information exchange, which include, for instance:[11]

- EURODAC, a database containing the fingerprints of all asylum applicants and all persons apprehended while irregularly crossing an EU external border. By the end of 2007, EURODAC had 1,086,246 fingerprint sets, and over the first five years of its operation had cost the EU €8.1 million. After a drop between 2005 and 2006, the 2007 EURODAC statistics show a 19% rise of 197,284 compared to 165,958 in 2006, in the number of data transactions regarding asylum-seekers. Further, the number of persons apprehended in connection with an irregular crossing of EU external border saw a drop of 8% in 2007 (38.173).[12]

1 Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data (OJ 1995 L 281/31).

2 Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector (OJ 1998 L 24/1).

3 Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201/37), amended by Directive 2006/24/EC (OJ 2006 L 105/54).

4 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.
OJ 2000 C 364/1.

5 OJ 2000 C 364/1.

6 Art. 41 of Regulation 45/2001/EC on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ 2001 L 8/1).

7 Art. 29 of Directive 95/46/EC.

8 http://www.edps.europa.eu/EDPSWEB

9 http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm

10 Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ 2008 L 350/60).

11 For a full overview of EU databases and systems of information exchange, see F. Geyer (2008), "Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice", CHALLENGE Research Paper No. 9, May 2008, Centre for European Policy Studies.

12 European Commission, Communication, Annual Report on the activities of EURODAC Central Unit in 2007, COM(2009) 13, 26.1.2009, Brussels.

• The Schengen Information System (SIS), a database used by the authorities of the Schengen member states to exchange data on certain categories of people and goods, which has primarily been used as a database of third-country nationals to be refused entry into the EU, and which has developed into the SIS + to include the 2004 member states. The latter will be transformed (with new capabilities and information) into the second generation of the SIS (SIS II).[13]

• The Visa Information System (VIS), which will contain information on all persons who apply for short stay visas to the EU.

• In addition, the creation of three new EU large-scale databases has been proposed by the European Commission, as a part of its 2008 Border Package: an EU entry/exit system that registers the movement of specific categories of third-country nationals at the external borders of the EU; an Automated Border Control System for the verification of a traveller's identity (for both EU and non-EU citizens alike) based on biometric technology; and an Electronic Travel Authorisation System that would oblige non-EU travellers to provide personal data for pre-departure online check (see the Background Briefing on Borders).

The content and way in which these tools are used give rise to a number of concerns.

Firstly, data mining is one of the most sensitive issues in the data protection debate. The outcome of database searches by law-enforcement authorities can be problematic depending on how they are carried out. For instance, not all the population is entered into the databases and, as a result, suspicion tends to fall only on those who match the profile the authorities are looking for and are already in the database. Different types of searches raise different problems. One or multiple searches by law enforcement authorities on individuals are often most common. Searches based on profiles, when the law enforcement agents do not know who they are looking for, raise many more issues of concern. The use of commercially gathered data for law enforcement purposes can also lead to problems. In order to avoid the risk of unnecessary harm to individuals, personal data collected for law-enforcement purposes need to be accurate. Problems arise when original data are integrated with more recent information, usually when the individual comes to the attention of authorities, providing a completely arbitrary picture of the person. Furthermore, personal data gathered for security purposes need to be adequate and proportional to the purpose for which they are being collected, as an indiscriminate gathering of data not only is not a guarantee of better security, it is also a breach of the individual's right to privacy.

Second, ensuring that access to sensitive data is strictly limited to those who should have it is an issue of major concern. Access to EU databases depends on the instrument that established the database. For example, access to EURODAC is limited to officials who are checking whether an asylum applicant has already sought asylum in another country (or arrived irregularly), but there have been moves afoot to widen it to all law-enforcement authorities. The quality of agencies collecting, processing and exchanging data, as well as the implications of giving third-countries' authorities access to EU databases, therefore need to be carefully assessed to ensure that the individuals' personal data are lawfully and adequately dealt with.

Lastly, individuals must be adequately protected against the consequences of data inaccuracies or of lax data exchange, and they must be properly informed of the rights they enjoy in this regard. A 2008 Eurobarometer survey[14] showed that, while the majority of EU citizens (64%) are concerned about data protection issues, only about a quarter of them (27%) are aware of the rights they enjoy in case of misuse of their personal data, and that not even one-third (29%) know that sensitive data like racial or ethnic origins receive special legal protection. The rights of the data subject, along with effective information about them, need therefore to be addressed as another key issue in the data protection debate so as to eliminate the inconsistencies that currently undermine the EU legal framework on data protection, especially with regard to its application to the AFSJ. The degree of protection granted at the EU level, indeed, is far from homogeneous, as the rights of the data subject depend very much on the database under consideration, and the gap between the standards attained in the policy domains belonging respectively to the First and Third Pillars is still significant.

3. Future Challenges and Recommendations

The following major future challenges can be identified in relation to data protection in the EU's AFSJ:

First, privacy rules must be built into the programmes that run EU databases and information systems. These programmes should include the automatic deletion of data at the end of the permitted period; prevent all unauthorised access to the system and any duplication of images on computer screens; and prohibit the indiscriminate searching of databases.

Second, databases should not be set up without prior impact assessment studies being carried out by objective and independent organisations. Any EU strategy on data exchange needs to start with the evaluation and inventory of current policies, tools and institutional structures involved in data exchange in the field of security at the EU level. Any new databases should only be set up, and subsequently used, for specific and lawful purposes – avoiding vague, open definitions and aimless data collection.

Third, data collection systems should not reveal sensitive data about ethnic origin, religion or other aspects prohibited in EU non-discrimination law. Hidden criteria indicating ethnic or religious distinctions, such as the birthplace of parents or the individual, or the former nationality, should be forbidden.

13 Report from the Commission on the Development of the Second Generation Schengen Information System (SIS II) Progress Report – July 2008 – December 2008, COM(2009) 133, 24.3.2009, Brussels.

14 The Gallup Organisation (2008), "Data Protection in the European Union. Citizens'perceptions", Eurobarometer, p. 5.

ANNEX

Adopted measures

1. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data (OJ 1995 L 281/31).
2. Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector (OJ 1998 L 24/1).
3. Regulation 45/2001/EC on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ 2001 L 8/1).
4. Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201/37).
5. Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105/54).
6. Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ 2008 L 350/60).

Opinions adopted by the European Data Protection Supervisor in 2009

Supervision

1. Opinion of 29 April 2009 on a notification for prior checking on Voice Logging at the Joint Research Centre Institute for Energy (JRC-IE) in Petten (Case 2008-014).
2. Avis du 1er avril 2009 sur la notification d'un contrôle préable à propos du dossier "Exercice annuel de retraite anticipée sans réduction des droits à pension" (Dossier 2008-719).
3. Avis du 30 mars 2009 sur la notification d'un contrôle préalable concernant le dossier "stagiaires structurels" (Dossier 2008-760).
4. Avis du 25 mars 2009 sur la notification d'un contrôle préalable à propos du dossier "traitement des demandes de levée de l'immunité de juridiction et d'inviolabilité des locaux et archives de la Commission" (Dossier 2008-645).
5. Avis du 23 mars 2009 sur la notification de contrôle préalable à propos de la gestion des informations transmises par l'OLAF dans le cadre du Memorandum of Understanding (Dossier 2009-011).
6. Avis du 10 mars 2009 sur la notification d'un contrôle préalable à propos du dossier Procédure de fin de stage (Dossier 2008-720).
7. Opinion of 26 February 2009 on a notification for prior checking regarding ETF - Flexitime procedure (Case 2008-697).
8. Avis du 23 février 2009 sur la notification d'un contrôle préalable à propos du dossier "Groupe de réintégration et de réorientation professionnelle" (Dossier 2008-746).
9. Opinion of 20 February 2009 on a notification for prior checking regarding the engagement and use of temporary agents (Case 2008-315).
10. Opinion of 18 February 2009 on a notification for prior checking on the procedure for early retirement without reduction of pension rights (Case 2008-748).
11. Opinion of 9 February 2009 on a notification for prior checking regarding "ART: Audit Reconciliation Tool" (Case 2008-239).
12. Avis du 26 janvier 2009 sur la notification de contrôlé préalable à propos du dossier "Menaces vis-à-vis des intérêts de la Commission dans les domaines contre intelligence, contre terrorisme" (Dossier 2008-440).
13. Opinion of 21 January 2009 on a notification for prior checking on the assessment of staff's capacity to work in a third language before first promotion (Case 2008-690).
14. Opinion of 21 January 2009 on a notification for prior checking concerning the report on probation period (Case 2008-604)
15. Opinion of 16 January 2009 on a notification for prior checking on the management of Central and Local Training SYSLOG Formation (Case 2008-481).
16. Avis du 16 janvier 2009 sur la notification d'un contrôle préalable à propos du dossier "Procédure relative aux commissions d'invalidité" (Dossier 2008-626).
17. Avis du 15 janvier 2009 sur la notification d'un contrôle préalable à propos du dossier "gestion et facturation de la crèche du Secrétariat Général du Conseil" (Dossier 2007-441).
18. Avis du 9 janvier 2009 sur la notification d'un contrôle préalable à propos du dossier "Exercice annuel de retraite anticipée sans réductions des droits à pension" (Dossier 2008-552).

Opinions adopted by the Working Party on the protection of individuals with regard to the processing of personal data in 2008

1. Opinion 3/2008 of the Article 29 Working Party on the World Anti-Doping Code draft International Standard for the Protection of Privacy.
2. Opinion 2/2007 on information to passengers about the transfer of PNR data to US authorities, Adopted on 15 February 2007 and revised and updated on 24 June 2008.
3. Opinion 2/2008 on the review of the Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive).
4. Opinion 1/2008 on data protection issues related to search engines.