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.
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 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 and electronic communications sectors. The main purpose of these is to guarantee the confidentiality of communications by prohibiting any unauthorised listening, tapping, 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, 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). Further, it needs to be underlined that in the EU context there is a European Data Protection Supervisor (EDPS) and a Working Party on the protection of individuals with regard to the processing of personal data, 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). 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.

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. 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, 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:

- 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).

---

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).
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/workingroup/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).
law-enforcement authorities. The quality of agencies seeking asylum in another country (or arrived irregularly), are checking whether an asylum applicant has already been rejected. Additionally, access to EURODAC is limited to officials who are responsible for making decisions on asylum applications, in accordance with the instrument that established the database. For instance, not all the population is entered into the database, which would lead to an indiscriminate gathering of data not only is not a guarantee of better security, but also a breach of the rights they enjoy in this regard. A 2008 Eurobarometer survey 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 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.


---

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).
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).

**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).
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).
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).

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