FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

Data Protection in the European Union: the role of National Data Protection Authorities

Strengthening the fundamental rights architecture in the EU II

This report relates to article 8, protection of personal data, as enshrined in the Charter of Fundamental Rights of the European Union.

Europe Direct is a service to help you find answers to your questions about the European Union

Freephone number (*):
00 800 6 7 8 9 10 11

(*) Certain mobile telephone operators do not allow access to 00 800 numbers or these calls may be billed.

Cover picture: Comstock Images

More information on the European Union is available on the Internet (http://europa.eu).

Cataloguing data can be found at the end of this publication.

Luxembourg: Publications Office of the European Union, 2010

ISBN 978-92-9192-509-4
doi:10.2811/47216

Printed in Belgium

PRINTED ON WHITE CHLORINE-FREE PAPER

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

Data Protection in the European Union: the role of National Data Protection Authorities

Strengthening the fundamental rights architecture in the EU II

DISCLAIMER: The data and information used for this report were provided by the FRA research network FRALEX.
The responsibility for its conclusions and opinions lies with the European Union Agency for Fundamental Rights.

Contents

Foreword

The fundamental rights architecture in the European Union has developed over time and continues to evolve. This report is one of four by the European Union Agency for Fundamental Rights (FRA) that looks at three closely related issues, and institutions, which contribute to the overarching architecture of fundamental rights in the European Union: namely, equality bodies, data protection authorities, and national human rights institutions (NHRIs).

For the FRA, these three sets of monitoring bodies at the national level are highly relevant. The FRA is specifically mandated to cooperate with, for example, governmental organisations and public bodies competent in the field of fundamental rights in the Member States, including data protection authorities with the aim of improving 'joined up' cooperation between the national level and the EU level. It is the need for an ever more efficient protection and promotion of fundamental rights at the national level in particular, coupled with European and international mechanisms, which forms the basis for considering the fundamental rights architecture in the European Union.

The report at hand, on data protection authorities, is an analysis of their crucial role with respect to the fundamental right of data protection, and encompasses an assessment of their effectiveness, functioning and independence. This report is timely because data protection has acquired the status of a separate fundamental right in the EU, in the text of the Charter of Fundamental Rights (Article 8), and is now related to, but distinct from, the right to respect for private and family life. At the same time, data protection is also emerging as a key EU policy area, and the EU has been the key driving force for the development of legislation in many Member States.

The Commissioner for justice, fundamental rights and citizenship, Viviane Reding, recently stressed in a written statement to the European Parliament that data protection is an issue of particular importance for the EU. She said that it is her "firm belief that there can be no trust of citizens towards Europe if we do not remain vigilant in ensuring that personal data are protected against unauthorised use, and that citizens have the right to decide themselves whether or not their data are processed." It is in this spirit that the FRA presents this report.

Morten Kjaerum

Director

Executive Summary

EU plays globally pioneering role for fundamental right of data protection

Historically, the EU has played a key role in driving the development and introduction of national data protection law in a number of legal systems in the EU, which did not have such legislation previously. An important instrument in this respect was Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the "Data Protection Directive").

The EU Charter of Fundamental Rights – that, according to the new Article 6 of the Treaty of European Union, enjoys "the same legal value as the Treaties" – enshrines data protection as a fundamental right under Article 8, which is distinct from respect for private and family life under Article 7. This feature sets the EU Charter of Fundamental Rights apart from other key human rights documents which, for the most part, treat the protection of personal data as an extension of the right to privacy.

This inclusion of data protection as an autonomous fundamental right is a recognition by the EU of the importance of technological progress, and an attempt to make sure that fundamental rights take account of this progress. The undeniable fact that our lives are now becoming a continuous exchange of information, and that we live in a continuous stream of data, means that data protection is gaining importance and moving to the centre of the political and institutional system. This evolution is clearly visible when comparing the EU Charter with the 1950 European Convention of Human Rights of the Council of Europe (ECHR). Under Article 8 of the ECHR, "everyone has the right to respect for his private and family life, his home and his correspondence." The ECHR does not contain an explicit and autonomous right to data protection. Rather, data protection emerges from the jurisprudence of the European Court of Human Rights in Strasbourg as an aspect of privacy protection. In comparison, Article 8 of the EU's Charter of Fundamental Rights acknowledges the centrality and importance that the right to data protection has acquired in our society, as shaped by technological developments.

This comparative study analyses the current challenges and good practices related to the data protection system in the EU.

Challenges for the EU data protection system

The EU Agency for Fundamental Rights identified the following challenges for the data protection system in the EU:

Deficiencies of Data Protection Authorities:

At a structural level, the lack of independence of several Data Protection Authorities (DPAs) poses a major problem. In a number of Member States concerns are reported about the effectiveness and capability of the officers of Data Protection Authorities to perform their task with complete autonomy. At the functional level, understaffing and a lack of adequate financial resources among several Data Protection Authorities constitutes a major problem. At the operative level, a major problem is represented by the limited powers of several Data Protection Authorities. In certain Member States, they are not endowed with full powers to investigate, intervene in processing operations, offer legal advice and engage in legal proceedings.

Lack of enforcement of the data protection system:

In some Member States, prosecutions and sanctions for violations of data protection law are limited or non-existing. With regard to compensation, the legal system of various Member States effectively rules out the possibility of seeking compensation for a violation of data protection rights, due to the combination of several factors such as burden of proof, difficulties relating to quantification of the damage and a lack of support from the supervisory bodies, which are engaged principally in "soft" promotional activities like registration and awareness raising. There is a general tendency in the Member States to focus on 'soft' methods of securing compliance with data protection legislation, instead of applying and enforcing 'hard' instruments by which violators of data protection rights may be detected, punished and asked to compensate victims. Good practices in this respect regarding cooperation of Data Protection Authorities and other authorities to strengthen investigations were found in some Member States.

Rights awareness:

During the research for this report, the FRA was able to identify national surveys addressing data protection in 12 out of 27 EU Member States. These surveys have in some instances been commissioned by the national Data Protection Authorities. The questions posed, the number of participants, the methodology and the final results are diverse and do not always allow for comparison. Nevertheless, of itself the existence of these national surveys constitutes a good practice. In February 2008, two Eurobarometer surveys on data protection were published. The most important findings from these surveys were that a majority of EU citizens showed concern about data protection issues and that national Data Protection Authorities were relatively unknown to most EU citizens.

Lack of data protection in the former third pillar of the EU:

The main limitation currently faced by the EU to provide for effective and comprehensive data protection arises from the constitutional architecture of the former EU pillars. While data protection is highly developed in the former first pillar of the EU, the data protection regime in the former third pillar cannot be regarded as satisfactory. Yet the former third pillar of the EU comprises areas such as police cooperation, the fight against terrorism, and matters of criminal law where the need for data protection is especially important. The Lisbon Treaty facilitates the closing of this gap. Declaration No 21 to the Lisbon Treaty notes 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 may prove necessary because of the "specific nature" of these fields.

Exemptions from data protection for security and defence:

Article 13(1) of the Data Protection Directive provides for broad exemptions and restrictions concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters), and the activities of the State in areas of criminal law. There is a lack of clarity regarding the extent of these exemptions and restrictions. In various Member States, these areas are altogether excluded from the protection of data protection law. This leaves a considerably large area unprotected with potentially serious consequences for fundamental rights protection. Declaration No. 20 to the Lisbon Treaty says that whenever rules on protection of personal data are to be adopted which could have direct implications for national security, "due account" will have to be taken of the specific characteristics of the matter.

The challenge of technology:

Recent and ongoing technological developments pose challenges that urgently need to be addressed. Video surveillance in public space and in the employment environment is widespread, but the legislative framework is lagging behind. As an example, the report reveals that, in practice, CCTV cameras are often not registered and/or monitored in some Member States.

Good practices

Most of the good practices identified by the EU Agency for Fundamental Rights that contribute to effective data protection relate to awareness raising activities undertaken by national Data Protection Authorities in some Member States, whether they are organizing specific courses, seminars and lectures, providing educational programmes, issuing guidance and recommendations, or organizing informational and advisory campaigning. Some other good practices also relate to the institutional position of the supervisory bodies: namely, the degree of their independence, the enforcement of data protection legislation, active engagement in the preparation of proposals for and issuance of codes of conduct, and the degree of cooperation with national institutions, NGOs and Data Protection Authorities of other Member States.

Opinions

The European Union Agency for Fundamental Rights has formulated the following opinions based on the findings and comparative analysis contained in this report:

EU to widen its data protection regime

The Lisbon Treaty and its abolition of the pillar structure of the EU opens the opportunity for the EU to widen the its data protection regime, which currently only exists for the former first pillar, across all (former) pillars of the EU. Limitations on data protection for security or defence or other legitimate purposes remain possible according to Article 52 of the Charter of Fundamental Rights of the EU, but these limitations must be provided for by law and respect the essence of the right to protection of personal data and the requirements of necessity and proportionality. Complete and total exclusion of certain areas from the scope of data protection legislation is problematic from a fundamental rights perspective and must be avoided.

Ensuring effective enforcement

This report reveals a problem of understaffing and lack of adequate financial resources for several Data Protection Authorities. At the operative level, a major problem is represented by the limited powers of several DPAs. In certain Member States, they are not endowed with full powers to investigate, intervene, offer legal advice and engage in legal proceedings. DPAs need the necessary resources, powers and independence to contribute to the effective enforcement of the data protection system.

Guarantees for effective enforcement of data protection, and the investigation and detection of perpetrators, are crucial to achieve deterrence and to prevent data protection violations. Dedicating significantly more emphasis on enforcement would also help to convince the population that data protection issues are taken seriously. An exclusive focus on "soft" measures with no resort to "hard" measures undermines the credibility of the whole system. In this sense, effective enforcement would also contribute to enhanced rights awareness amongst the population. Data Protection Authorities should play an important role in the enforcement of the data protection system, either by directly having the power to issue sanctions or by having the power to initiate procedures that can lead to sanctions ex officio. This would strengthen their authority and credibility.

National Data Protection Authorities as independent guardians

At the structural level the lack of independence of several Data Protection Authorities poses a major problem. In several countries, however, normative or practical obstacles raise concern as to the effective independence of national DPAs from the political branches of government. The guarantee of independence is, in fact, primarily assured by the procedure of nomination and removal of the officers of the DPAs. The control over financial resources represents a second relevant element in ensuring the autonomy of supervisory authorities.

In various Member States, data protection officers are directly appointed by the Government with no involvement of the opposition in Parliament; in several cases this has raised serious concerns as to the effective independence of the data protection authority. Similar concerns may arise in those countries where the supervisory authority is attached to the Ministry of Justice. Finally, other Member States provide for a combined procedure to nominate the officers of the national Data Protection Authority, involving the executive, legislature and judiciary, or other organized societal groups at the same time. In some cases, however, it is essential to ensure that de facto the Government does not control directly or indirectly the majority of the appointees, thus depriving in effect the purpose of a pluralistic nomination procedure.

The Data Protection Directive 95/46/EC requires Data Protection Authorities to 'act with complete independence in exercising the functions entrusted to them' (Article 28(1) of the Data Protection Directive). However, the nature of this 'independence' is not elaborated upon. It would be advisable for the guarantees of independence in the directive to be specified in detail to guarantee effective independence of Data Protection Authorities in practice. It is thus advisable to include a reference to the so-called "Paris Principles" and other available standards in a future revision of the directive in order to offer a more comprehensive definition of independence.

National Data Protection Authorities as part of the emerging fundamental rights architecture of the EU

Data Protection Authorities should promote closer cooperation and synergy with other guardians of fundamental rights (such as national human rights institutions and equality bodies, etc.) in the emerging fundamental rights architecture of the EU. One possibility for the EU to contribute to better coordination and synergy could be to add a phrase to Article 28 of the Data Protection Directive 95/46/EC which would give the possibility to Member States to legislate to the effect that their Data Protection Authority effectively becomes a specialised section of their national human rights institution (an interesting example of a similar effect is Article 13 of Council Directive 2000/43/EC).

National Data Protection Authorities as efficient one-stop shops

The Data Protection Authorities are key actors for effective data protection. They serve as low threshold access points to effective data protection for citizens and other persons. They should not just deal with issues forming part of the former first pillar, as is currently the case in some Member States, but they should be designed to function as one-stop shops for all data protection concerns of citizens and other persons; including areas which were formerly part of the third pillar of the EU. A proliferation of data protection bodies and authorities is not conducive to raising the awareness of citizens of their existence. Also, a multitude of bodies creates confusion and unnecessary complexity.

Rights-awareness

In February 2008, two Eurobarometer surveys on data protection were published. The most important findings from these surveys were that a majority of EU citizens showed concern about data protection issues and that national Data Protection Authorities were relatively unknown to most EU citizens.

It is advisable that Data Protection Authorities pay particular attention to cultivating their public profile as independent guardians of the fundamental right to data protection and focus on raising awareness of their existence and role.

1. Introduction

The EU Charter of Fundamental Right enshrines the fundamental right to data protection in its Article 8. Data protection is also one of the key fundamental rights areas where the EU has the competence to legislate.

The Agency produced this report with the assistance of FRALEX, the legal expert group of the Agency. FRALEX national teams produced 27 national studies and one EU/international study (all publicly available on the website of the agency as background material via http://fra.europa.eu) based on common guidelines elaborated by the Agency. On the basis of these studies, the comparative report was developed. The national studies are dated February 2009. The "Article 29 Working Party" was consulted in connection with the draft comparative report and delivered comments.

This report is closely linked to the following projects and publications of the European Union Agency for Fundamental Rights:

- PNR opinion, October 2008[1]
- Contribution of the Agency to a consultation of the European Commission on body scanners, January 2009[2]
- Report on National Human Rights Institutions in the European Union Member States – Strengthening the Fundamental Rights Architecture I, 2010[3]
- EU-MIDIS Data in Focus III: Rights Awareness and Equality Bodies, 2010[4]

This report will first present the international law standards concerning data protection. It will then analyse data protection in EU law and the change brought about by the Lisbon Treaty. A comparative overview of data protection institutions and practices in the Member States follows. The report concludes with the identification of deficiencies and good practices.

1 Avalaible at http://fra.europa.eu/fraWebsite/attachments/FRA_opinion_PNR_en.pdf (accessed on 27.01.2010).
2 Unpublished contribution of the EU Agency for Fundamental Rights to a consultation of the European Commission.
3 Available at http://fra.europa.eu/ (24.02.2010).
4 Available at http://fra.europa.eu/eu-midis (24.02.2010).

2. Fundamental rights standards relating to data protection

The protection of personal data is recognized as a fundamental right in various European and international treaties and interpreted by the jurisprudence of international and regional courts.

2.1. Data Protection in the Framework of the United Nations

The fundamental right to protection of personal data is recognized at the universal level in various human rights instruments adopted under the aegis of the United Nations, mostly as an extension of the right to privacy.[5]

In particular, in the International Covenant on Civil and Political Rights (ICCPR), which has been ratified by four fifths of the world's States, the right to the protection of privacy, family, home and correspondence is protected in Article 17, stating that "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks upon his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks". General Comment No. 16 on Article 17 ICCPR refers expressly to the right to the protection of personal data.[6] It provides, specifically that: "the gathering and holding of personal information on computers, databanks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination". In addition, the case law of the Human Rights Committee points out that the notion of private life in General Comment No. 16 should not be interpreted narrowly.[7]

Another instrument of particular significance is the United Nations Guidelines concerning Computerized Personal Data Files adopted by the General Assembly on 14 December 1990.[8] The Guidelines set out certain principles concerning the minimum guarantees that should be provided in national legislation for the protection of personal data. They provide for the principle of lawfulness and fairness of the collection and processing of personal data, accuracy, purpose-specification, interested-person access, non-discrimination and security of the data files. Departures from those principles "may be authorized only if they are necessary to protect national security, public order, public health or morality, as well as, inter alia, the rights and freedoms of others, especially persons being persecuted (humanitarian clause) provided that such departures are expressly specified in a law or equivalent regulation promulgated in accordance with the internal legal system which expressly states their limits and sets forth appropriate safeguards". Exceptions to the principle of non-discrimination, are even more limited, and "may be authorized only within the limits prescribed by the International Bill of Human Rights and the other relevant instruments in the field of protection of human rights and the prevention of discrimination". According to the Guidelines, the principles enshrined in them "should be made applicable, in the first instance, to all public and private computerized files as well as, by means of optional extension and subject to appropriate adjustments, to manual files. Special provision, also optional, might be made to extend all or part of the principles to files on legal persons particularly when they contain some information on individuals".

The fundamental right to protection of personal data is recognized also at the regional level in various regional human rights instruments outside Europe, mostly as an extension of the right to privacy.[9]

2.2. Data Protection in the Framework of the Council of Europe

At the regional level, the standard for the protection of personal data is established in several conventions adopted under the aegis of the Council of Europe. Most of these instruments have been ratified by all EU Member States and in some cases have been implemented in their domestic legal systems as supreme constitutional norms.

The most prominent legal document within the Council of Europe framework, the European Convention of Human Rights (ECHR) – which has been ratified by all EU Member States – does not explicitly mention the protection of personal data. However, extensive case law of the European Court of Human Rights (ECtHR) proves that the right to data protection is encompassed

5 Article 12 of the Universal Declaration of Human Rights protects the right to private life.

6 See Human Rights Committee, General Comment 16, (Twenty-third session, 1988), Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies, U.N. Doc. HRI/GEN/1/Rev.1 at 21 (1994), para 10.

7 See for instance case *Coeriel & Aurik v the Netherlands (1994)* Comm 453/1991.

8 Guidelines for the Regulation of Computerized Personal Data Files adopted by the General Assembly Resolution 45/95 of 14 December 1990.

9 The right to private life is found in Article V of the 1948 American Declaration of the Rights and Duties of Man, and in Article 11 of the American Convention on Human Rights of 1969. The African Charter on Human Right's and People's Rights of 1981 does not contain express recognition of the right to privacy.

in Article 8 ECHR, which expressly recognises the right to respect for private and family life, stating that "1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

Furthermore, within the Council of Europe framework, explicit recognition of the fundamental right to protection of personal data can be found in the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (also known as 'Convention 108')[10], which has been ratified by all EU Member States. The Convention imposes the obligation on the Contracting States to secure in their territory for every individual, whatever his/her nationality or residence, respect for his/her rights and fundamental freedoms, and in particular his/her right to privacy, with regard to automatic processing of personal data relating to him/her ('data protection'). The Convention applies to automated personal data files and automatic processing of personal data in the public and private sectors. It contains a number of principles concerning the processing of data, and, in addition, it refers to the quality of the data, in particular that they must be adequate, relevant and not excessive (principle of proportionality); their accuracy; the confidentiality of sensitive data; information of the data subject; and his/her right of access and rectification. However, the Convention generally relies on relatively vague and broad formulations, and it is not necessarily directly applicable, but requires that Contracting States parties adopt implementation measures: therefore it may not be invoked directly by individuals before courts. Moreover the Convention contains wide-ranging exceptions, including the possibility for the States parties to derogate from the rules concerning data protection when such derogation is provided for by the domestic law of the Party and constitutes a necessary measure in a democratic society.

Convention 108 also establishes a Consultative Committee (T-PD), consisting of representatives of Parties to the Convention complemented by observers from other States (members or non-members) and international organisations, which is responsible for interpreting the provisions and for improving the implementation of the Convention. This Committee adopted an Additional Protocol to the Convention, (which has not yet been ratified by all EU Member States), regarding supervisory authorities and Transborder Dataflow (2001), reinforcing the Supervisory Authorities and prohibiting the transfer of personal data to States or organizations that do not provide for an adequate level of protection.

Another important legislative instrument in the Council of Europe framework is the Convention on Human Rights and Biomedicine (1997),[11] (which has not yet been ratified by all EU Member States). Article 10 of this Convention reaffirms the principle protected in Article 8 ECHR and reiterated in Convention 108 by establishing that "1. Everyone has the right to respect for private life in relation to information about his or her health. 2. Everyone is entitled to know any information collected about his or her health. However, the wishes of individuals not to be so informed shall be observed. 3. In exceptional cases, restrictions may be placed by law on the exercise of the rights contained in paragraph 2 in the interests of the patient". Furthermore, under Article 6 of the Convention on Human Rights and Biomedicine, personal data concerning health constitute a special category of data and are as such subject to special rules. The Convention, nevertheless, allows for certain restrictions to the right to privacy, for example, when a judicial authority needs to identify the author of a crime (exception based on the prevention of a crime) or to determine paternity of maternity (exception based on the protection of the rights of others).

Finally, it should be mentioned that the Council of Europe has also used recommendations and resolutions to further elaborate the principles of the protection of personal data of individuals. These instruments are adopted unanimously by the Committee of Ministers and, although they are not legally binding, they contain standards of reference for all Member States. Since 1972, the Council of Europe has adopted a great number of recommendations and resolutions concerning data protection issues.[12]

In this respect, Recommendation No. R(87) 15 regulating the use of personal data in the police sectordeserves special mention as it goes even further than 'Convention 108' in ensuring the protection of sensitive personal data.[13] Under Principle 2.4 of the Basic Principles contained in the Appendix to this Recommendation, the collection of data on individuals solely on the basis that they have a particular racial origin, particular religious convictions, sexual behaviour or political opinions or belong to particular movements or organisations which are not proscribed by law should be prohibited. The collection of data concerning these factors may only be carried out if absolutely necessary for the purposes of the particular inquiry. The Appendix to this Recommendation also lays down a number of other principles designed to regulate the collection, storage, use, communication and conservation of personal data by the police. According to the preamble, the Recommendation recognises the need to strike a balance between, on the one hand, the interests of the individual and his right to privacy and, on the other hand, the interests of society in the prevention and suppression of criminal offences and the maintenance of public order. For this purpose, the relevant case law of the European Court of Human Rights is taken into account.

10 See http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm (24.02.2010).
11 See http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=164&CL=ENG (24.02.2010).
12 See Recommendation No.R(95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services (7 February 1995), Recommendation No.R(97) 5 on the protection of medical data (13 February 1997), Recommendation No.R(97) 18 on the protection of personal data collected and processed for statistical purposes (30 September 1997), Recommendation No.R(99) 5 for the protection of privacy on the Internet (23 February 1999) and Recommendation No.R(2002) 9 on the protection of personal data collected and processed for insurance purposes (18 September 2002).
13 Recommendation No.R(87) 15 regulating the use of personal data in the police sector (17 September 1987).

As far as the case law of the ECtHR on the protection of privacy and private life is concerned, there are a number of occasions in which the ECtHR has also referred to data protection issues. In this context, the ECtHR has found in Article 8 ECHR not only negative obligations for the Member States to abstain from interfering with the right to privacy, but also positive obligations, that entail 'the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals themselves.'[14]

In *M.S. v. Sweden*, for instance, the ECtHR made clear that 'the protection of personal data [...] is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention.'[15] In *Leander v Sweden*, the Court held that the storing of information relating to an individual's private life in a secret register and the release of such information amounted to an interference with his right to respect for private life as guaranteed by Article 8(1).[16] It stressed that 'in view of the risk that a system of secret surveillance for the protection of national security poses of undermining or even destroying democracy on the ground of defending it, the Court must be satisfied that there exist adequate and effective guarantees against abuse'. In *Z. v. Finland*, the ECtHR underlined that the protection of personal data, in particular the protection of medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the ECHR.[17] However, it accepted that the interests of a patient and the community as a whole in protecting the confidentiality of medical data may be outweighed by the interest in investigation and prosecution of crime and in the publicity of court proceedings where such interests are shown to be of even greater importance.

In *Rotaru v Romania*, the ECtHR expressly recognised that Article 8 ECHR should be interpreted in such a way as to encompass the guarantees concerning data protection enshrined in Convention 108.[18] It reiterated the principle held in *Leander* that the storing by a public authority of information relating to an individual's private life and the use of it amount to interference with the right to respect for private life and added that such an interference occurred also from the refusal to allow an opportunity for the personal data to be refuted. In *Amann v Switzerland*, the Court found that a card containing data relating to an individual's private life and stored by a public authority of itself amounted to an interference with the applicant's right to respect for his private life, without it being necessary for the Court to speculate as to whether the information gathered was sensitive or not.[19]

The ECtHR has recently recognized in *K.U. v. Finland* that national legislatures have a duty to provide a framework for reconciling the confidentiality of Internet services with the prevention of disorder or crime and the protection of the rights and freedoms of others. Since this framework had not been in place at the relevant time, Finland was held to have failed to protect the right to respect for the applicant's private life as the confidentiality requirement had been given precedence over his physical and moral welfare, and therefore the ECtHR concluded that a violation of Article 8 had taken place.[20] Furthermore, in *S. and Marper v. United Kingdom* the ECtHR ruled on the lawfulness of the retention by the British authorities of the applicants' fingerprints, cellular samples and DNA profiles after criminal proceedings against them were terminated by an acquittal or discharge and despite the fact that the applicants had requested their destruction. The ECtHR noted that cellular samples contained much sensitive information about an individual and thus held that the retention of both cellular samples and DNA profiles amounted to an interference with the applicants' right to respect for their private lives, within the meaning of Article 8(1) and observed that the protection afforded by Article 8 would be unacceptably weakened if the use of modern scientific techniques in the criminal justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests.[21]

In three French cases in 2009, while reaffirming the fundamental role of the protection of personal data subject to automatic processing, especially for police purposes, the Court concluded that the applicants' inclusion in the national police database of sex offenders, in the way in which it had been applied to them, was not contrary to Article 8.[22]

14 See *X and Y v Netherlands*, judgement of 26 march 1985, para 23.
15 See *M.S. v Sweden*, judgment of 27 August 1997.
16 See *Leander v. Sweden,* judgment of 26 March 1987, para. 48.
17 See *Z. v. Finland,* judgment of 25 February 1997, para 95.
18 See *Rotaru v Romania*, judgment of 4 May 2000, para 43.
19 See *Amann v Switzerland*, judgment of 16 February 2000, para 70.
20 See *K.U. v Finland*, judgment of 2 December 2008.
21 See *S and Marper v UK*, judgment of 4 December 2008.
22 See *Bouchacourt v. France*, *Gardel v. France*, and *M.B. v. France*, judgements of 17 December 2009 (not final).

3. Data protection in EU law

The protection of personal data is recognized in primary EU aw as an autonomous fundamental right, related to but distinct from the right to respect of private and family life. Article 8 of the EU Charter of Fundamental Rightsreads as follows: "1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority."[23] The EU Charter of Fundamental Rights has according to Article 6 of the Treaty on European Union (TEU), "the same legal value as the Treaties".

In the EU Data Protection Directive 95/46/EC, personal data are defined as "any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity".[24]

In the treatment of the protection of personal data as an autonomous right, the EU Charter of Fundamental Rights differs from other international human rights documents, which do not specifically mention a right to data protection, but mostly treat data protection as an extension of the right to privacy.

3.1. Data Protection in the former Community pillar

The EU data protection regime was profoundly affected by the former pillar division structure of the EU, which was abolished by the Lisbon Treaty. Data protection within each pillar was structured around separate sets of instruments. The former pillar division produced uncertainties as to which instruments applied to specific instances in the processing of data.

Insofar as the former first pillar of the EU was concerned, i.e. the former Community pillar, the main objective is to ensure the free flow of personal data between Member States in the process of the operation of the internal market, while at the same time protecting the fundamental rights of natural persons, and in particular their right to privacy with respect to the processing of personal data. The protection of personal data does not merely require that the EU institutions or the Member States' bodies abstain from illegal interferences in the personal data. There also exists a positive obligation to secure the protection of personal data.

Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter, the Data Protection Directive) constitutes the major EC instrument.[25] According to the ECJ, the Data Protection Directive adopted "at EU level, the general principles which already formed part of the law of the Member States in the area in question."[26] The EC data protection regime is based on the following fundamental principles enshrined in the Data Protection Directive: (i) processing of personal data must be lawful and fair to the individuals concerned; (ii) the purposes of the processing should be explicit and legitimate and must be determined at the time of the collection of the data; (iii) data must be relevant and not excessive in relation to the purpose for which they are processed. Data must also be accurate and where necessary, kept up to date; (iv) personal data can only be processed lawfully if certain criteria of processing defined in the directive are met (amongst other criteria, if the data subject has unambiguously given his or her consent). If the rights of data subjects fail to be respected, the individuals enjoy a judicial remedy that allows them to access and rectify personal data relating to them; (v) transfers of personal data to third countries are to be allowed only if those countries ensure an adequate level of protection; and (vi) the EU and its Member States must provide one or more independent authorities entrusted with the task of ensuring the correct application of the personal data rules.

The Data Protection Directive applies to "any operation or set of operations which is performed upon personal data", called "processing" of data. According to Article 3(1) it 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". Article 3(2) lays down the two areas where the Directive does not apply. First, processing of personal data "in the course of an activity which falls outside the scope of Community law, such as those provided for by former Titles V and VI TEU and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law". Second, processing of data "by a natural person in the course of a purely personal or household activity" also falls outside the scope of application of this Directive.

Another important EU legislative measure is Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications

23 For a commentary on Article 8 of the Charter see Commentary of the Charter of Fundamental Rights of the EU, EU Network of Independent Experts on Fundamental Rights, June 2006, available at http://ec.europa.eu/justice_home/doc_centre/rights/charter/docs/network_commentary_final%20_180706.pdf, 90. (21.01.2010)

24 Art. 2 (a) of the EU Data Protection Directive 95/46/EC.

25 OJ L 281 of 23.11.1995, p. 31.

26 See Case C- 369/98 *The Queen v Minister of Agriculture Fisheries and Food, ex parte Trevor Robert Fisher and Penny Fisher* [2000] ECR I-06751, para 34.

sector (the 'e-Privacy Directive').[27] It aims at harmonising the different national provisions on the protection of the right to privacy, with respect to the processing of personal data in the electronic communication sector while ensuring the free movement of such data and of electronic communication equipment and services. EU Directive 2002/58/EC particularises and complements Directive 95/46/EC with respect to the processing of personal data of natural persons in the electronic communications sector and provides for the protection of the legitimate interests of subscribers who are legal persons. The Directive does not apply to activities that fall outside the scope of the EC Treaty.

Directives 95/46/EC and 2002/58/EC are addressed to the Member States. Accordingly, they do not apply as such to the EU institutions and bodies. Protection of personal data is also a 'treaty-given' right to the extent that Article 16 of the Treaty on the Functioning of the European Union sets out the rules on the protection of individuals with regard to the processing of personal data and on the free movement of such data applicable to the European Union institutions themselves. On the basis of the former Article 286 of the EC Treaty, which was replaced by Article 16 of the Treaty on the Functioning of the European Union, Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 has been enacted on the protection of individuals with regard to the processing of personal data by the EU institutions and bodies and on the free movement of such data.[28] The Regulation aims at protecting the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data. It applies to the processing of such data by all EU institutions and bodies insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of EU law. This Regulation established the European Data Protection Supervisor (EDPS) in 2004.

The EDPS is an independent supervisory authority devoted to protecting personal data and privacy and promoting good practice in the EU institutions and bodies. The EDPS monitors the EU administration's processing of personal data, advises on policies and legislation that affect privacy and cooperates with similar authorities to ensure consistent data protection. The supervisory task is to ensure that the EU institutions and bodies process personal data of EU staff and others lawfully. Every institution or body should have an internal Data Protection Officer (DPO). The DPO keeps a register of processing operations and notifies systems with specific risks to the EDPS. The EDPS conducts a prior check as to whether or not those systems comply with data protection requirements. The EDPS also deals with complaints and conducts inquiries. Thus, the EDPS oversees Regulation (EC) 45/2001 on data protection. The EDPS advises the European Commission, the European Parliament and the Council on proposals for new legislation and a wide range of other issues with relevance to data protection. The EDPS cooperates with other Data Protection Authorities in order to promote consistent data protection throughout Europe. A central platform for the cooperation of the EDPS with national supervisory authorities is the so-called "Article 29 Working Party".[29]

Directive 2006/24/EC is a recent measure on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (the 'Data Retention Directive')[30]. This Directive aims at harmonizing Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data that are generated or processed by them. This ensures that the data are available for the purposes of the investigation, detection and prosecution of serious crimes, as defined by each Member State in its national law.

The ECJ has interpreted Directive 95/46/EC in numerous rulings. A first set of questions that the Court was called upon to answer concerned the scope of application of this Directive. In *Österreichischer Rundfunk,* the Court was asked to rule whether the Data Protection Directive was applicable at all to the control activity exercised by the Austrian court of Audit about the salaries of the employees of certain entities.[31] The ECJ found that it was applicable. According to the Court, "since any personal data can move between Member States, Directive 95/46 requires in principle compliance with the rules for protection of such data with respect to any processing of data as defined by Article 3". Similarly, in *Satakunnan Markkinapörssi and Satamedia,* the Court held that the processing of personal data files which contain solely, and in unaltered form, material that has already been published in the media, falls within the scope of application of Directive 95/46.[32]

A second set of legal issues concerned the interpretation of specific provisions of the Data Protection Directive. In *Lindqvist*, the ECJ ruled on the issue of processing of personal data carried out through the medium of the Internet.[33] Placing of this information in the Internet constituted 'processing of personal data wholly or partly by automatic means'. However, it held that loading personal data onto an internet site could not be regarded as 'transfer to a third country' under the provision of Article 25 of Directive 95/46. Finally, the Court has delivered a very important decision regarding the principle of non-discrimination in the protection of personal data within the

27 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L201 of 31.07.2002, p. 37.

28 Regulation (EC) No.45/2001 of the European Parliament and of the Council of 18 December 2000 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 L 8 of 12.1.2001, p. 1-22.

29 This Working Party is based on Article 29 of the EU Data Protection Directive 95/46/EC. See http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm (24.02.2010).

30 Directive 2006/24/EC of the European Parliament and the Council of 15 March 2006 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 L 105 of 13.4.2006, p. 54.

31 See Joined Cases C-465/00, C-138/01 and C-139/01, *Österreichischer Rundfunk,* Judgment of 20 May 2003, Full Court, [2003] ECR I-4989.

32 See Case C-73/07 *Satakunnan Markkinapörssi and Satamedia*, judgment of 16 December 2008.

33 See Case C-101/01 *Bodil Lindqvist* [2003] ECR I-12971.

context of Union citizenship.[34] The ECJ held that the difference in treatment between Member State nationals and other Union citizens which arises by virtue of the systematic processing of personal data relating only to the latter for the purposes of fighting crime, constitutes discrimination which is prohibited by Article 12(1) EC.

The Court has engaged in a balancing exercise between the right to privacy and data protection, and other fundamental rights and freedoms protected within the EC legal order. It has shown itself to be very sensitive in cases that concern freedom of expression, and more particularly, journalism, where it seems ready to accept an exemption from data protection for this purpose. In contrast, the Court has chosen not to provide a clear answer in the case of tension between the right to data protection and the protection of intellectual property.

In *Lindqvist*[35], the ECJ had to strike the balance between the right to data protection and freedom of expression enshrined, *inter alia*, in Article 10 ECHR and protected within the EC legal order as a general principle of EU law. The Court noted that "fundamental rights have a particular importance, as demonstrated by the case in the main proceedings, in which, in essence, Mrs Lindqvist's freedom of expression in her work preparing people for Communion and her freedom to carry out activities contributing to religious life have to be weighed against the protection of the private life of the individuals about whom Mrs Lindqvist has placed data on her internet site". In *Satakunnan Markkinapörssi and Satamedia*[36], the ECJ was asked to interpret Article 9 of the Data Protection Directive, which allows the Member States to provide for exemptions and derogations for the processing of personal data "carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression". More particularly, Markkinapörssi collected public data from the Finnish tax authorities for the purposes of publishing extracts from them in the regional editions of the Veropörssi newspaper, and transferred the same data to Satamedia with a view to those being disseminated by a text-messaging system. The ECJ noted the importance of the right to freedom of expression in a democratic society and held that notions relating to that freedom, such as journalism, should be interpreted broadly. It then clarified that activities which involve the processing of data from documents which are in the public domain under national legislation, may be classified as 'journalistic activities' if their object is "the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them". Furthermore, the Court ruled that those activities are not limited to media undertakings but cover every person engaged in journalism, and may be undertaken for profit-making purposes.

The ECJ dealt with similar issues in *Promusicae*.[37] It found that "Directive 2002/58 does not preclude the possibility for the Member States of laying down an obligation to disclose personal data in the context of civil proceedings", and the intellectual property protection legislation does not "require the Member States to lay down, in order to ensure effective protection of copyright, an obligation to communicate personal data in the context of civil proceedings". It concluded that there was a "need to reconcile the requirements of the protection of different fundamental rights, namely the right to respect for private life on the one hand and the rights to protection of property and to an effective remedy on the other".

3.2. Data Protection in the former second and third Pillars of the EU

There are still serious uncertainties and deficiencies with regard to the protection of personal data in the framework of activities beyond the scope of the former first pillar. Although the fundamental rules pertaining to the protection of personal data must be observed in the processing of personal data within the former second and third pillar, there is a lack of a general legal framework on the protection of personal data in the former second and the third pillar. Instead, data protection is scattered in a series of *ad hoc* sets of rules on data protection in various instruments on the processing of personal data in the framework of, for instance, police and judicial cooperation in criminal matters.[38] The former second and third pillars also faced a number of structural problems and inadequacies that limited even further the possibilities for effective protection of fundamental rights. The former third pillar suffered, firstly, from inadequacies in terms of democratic control. The role of the European Parliament was substantively limited only to consultation, and the Council was free to ignore its opinion, if it chose to do so. Furthermore, the right of initiative was shared between the Commission and the Member States and the rule of unanimity applied to this formerly intergovernmental pillar. Secondly, judicial control by the Court of Justice within the former third pillar was also limited. According to former Article 35(1) TEU, the Court had jurisdiction to give preliminary rulings on the validity and interpretation of framework decisions and decisions on the interpretation of conventions, and on the validity and interpretation of the measures implementing them. This jurisdiction was subject to prior acceptance by Member States that may further limit the possibility of requesting a preliminary ruling to certain national courts and tribunals.

34 Case C-524/06 *Huber v Bundesrepublic Deutschland* , judgment of 16 December 2008.

35 See Case C-101/01 *Bodil Lindqvist* [2003] ECR I-12971.

36 See Case C-73/07 *Satakunnan Markkinapörssi and Satamedia*, judgment of 16 December 2008.

37 Case C-275/06, *Productores de Música de España (Promusicae) v Telefónica de España SAU*, judgment of 29 January 2008.

38 For the protection of personal data in the context of Title VI TEU (the so-called III pillar), see for instance, the Convention implementing the Schengen Agreement of 1990 including specific data protection provisions applicable to the Schengen Information System, OJ L 239 , 22.9.2000, p. 19; the Europol Convention of 1995 and, inter alia, the Rules governing the transmission of personal data by Europol to third States and third bodies, OJ C 316, 27.11.1995, p. 2; the Decision setting up Eurojust of 2002, OJ L 63, 6.3.2002, p. 1 and the Rules of procedure on the processing and protection of personal data at Eurojust, OJ C 68, 19.3.2005, p. 1.; the Convention on the use of information technology for customs purposes of 1995, including personal data protection provisions applicable to the Customs Information System, OJ C 316, 27.11.1995, p. 34; and the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union of 2000, in particular Article 23, OJ C 197, 12.7.2000, p. 1, 15.

Thirdly, the advisory role of Data Protection Authorities, such as the Data Protection Supervisor was also limited compared to the first pillar. For instance, even though the European Commission confirms that it feels bound to consult the European Data Protection Supervisor when it adopts a proposal for legislation which may have an impact on the protection of personal data (as it has the obligation under Article 28(2) of Regulation 45/2001), its right of initiative in the third pillar was shared with the Member States that were not bound by such an obligation. The situation under the second pillar was more problematic, as no possibility for judicial review existed within the Common Foreign and Security Policy framework.

In recent years the exchange of personal data between law enforcement authorities in the different Member States has become a common scenario in the framework of Police and Judicial Cooperation. In this respect, the "Hague Programme", adopted on 5 November 2004 in response to the 'war on terrorism' has included the "principle of availability", which means that information that is available to certain authorities in a Member State must also be provided to equivalent authorities in other Member States. The "principle of availability" has serious implications on the protection of personal data, and adequate safeguards were and still are needed.

Against this setting, Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters was welcomed.[39] The Decision is the first horizontal data protection instrument in the field of personal data used by police and judicial authorities. The Framework Decision is applicable to cross-border exchanges of personal data within the framework of police and judicial cooperation. The instrument contains rules applicable to onward transfers of personal data to third countries and to the transmission to private parties in Member States. The decision also allows EU Member States to have higher-level safeguards for protecting personal data than those established in this instrument. However, the Framework Decision cannot ensure of itself that the guarantees of the right to respect for private life and of personal data protection are fully complied with in the processing of personal data in the framework of the second and third pillars. As its scope of application only covers *transborder flows of data between law enforcement authorities of the Member States,* it does not apply to the processing of data by law enforcement agencies within each Member State. The Framework Decision needs to be implemented by EU Member States by 27 November 2010, by taking the necessary measures, including designating one or more public authorities that should be responsible for advising and monitoring the application within its territory.

The protection of personal data was also one of the fields in which the former pillar structure of the EU continuously gave rise to divergent views of which processing falls under which pillar. The ECJ judgment in the Passenger Name Record (*PNR*) cases illustrated the problems arising from the former pillar division for the EU Data Protection regime.[40] The cases concerned the agreement concluded between the US and the EU for the transfer of data contained in the reservation and departure control systems of airlines operating flights to and from the United States, referred to as "Passenger Name Records" ('*PNR* data'). Upon a Decision on Adequacy adopted by the Commission on 14 May 2004 pursuant to Article 25 of the Data Protection Directive, the Council adopted on 17 May 2004 a Decision allowing for the conclusion of the Agreement with the US. The European Parliament brought an action before the Court seeking the annulment of both the Commission's Decision on adequacy and the Council's Decision on the conclusion of the agreement, on grounds, *inter alia*, of breaching the fundamental principles of the Data Protection Directive and the right to privacy. The Court annulled the Adequacy Decision on the sole ground that its subject matter was outside the material scope of the Data Protection Directive. It held that the transfer of *PNR* data constituted processing operations concerning "public security and the activities of the State in areas of criminal law" as referred to in Article 3(2) of Directive 95/46, and thus the Adequacy Decision could not be adopted under this Directive. Similarly, the ECJ annulled the Council's Decision on the conclusion of the Agreement, on the basis that it could not be adopted on the legal basis of Article 95 EC, because it related to "the same transfer of data as the decision on adequacy and therefore to data processing operations which, are excluded from the scope of the Directive", and thus the EU did not have competence to conclude the Agreement. By resulting in the transferral of the *PNR* Agreement from the former first to the former third pillar, with significant consequences regarding the judicial review and the democratic control arising thereof, the Court's ruling created "a loophole in the right of data protection" of the individual.[41] More importantly, as a result of the ECJ decision, the EU had to negotiate and conclude a new agreement with the USA, based this time on the correct legal basis. In 2007, the Commission introduced a proposal for a Council framework decision on the use of Passenger Name Record (PNR) data for law enforcement purposes.[42] The FRA was requested by the French Presidency to deliver an opinion on this proposal, which it delivered on 28 October 2008.[43] The Agency was of the opinion that the added value and necessity of the proposal on the use of PNR should be explained, that vague terms should be avoided and that there was a need for sufficient procedural safeguards. The Agency also suggested explicit prohibition of discriminatory ethnic profiling.

In the case of *Ireland v European Parliament and Council* the ECJ was asked once again to pronounce on the pillar division problem of the EU Data Protection regime.[44] More specifically, Ireland challenged Directive 2006/24/EC on the retention of telecommunications data, on the ground that Article 95 EC

39 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters OJ L 350, 30.12.2008 , p. 60.

40 Joined Cases C-317/04 and C-318/04, *European Parliament* v. *Council and Commission*, Judgment of the Grand Chamber of 30 May 2006, [2006] ECR I-4721.

41 See E. Guild and E. Brouwer, The Political Life of Data – The ECJ decision on the PNR Agreement between the EU and the US, (2006) Centre for European Policy Studies No. 109.

42 COM (2007) 654.

43 See http://fra.europa.eu/fraWebsite/attachments/FRA_opinion_PNR_en.pdf (22.01.2010).

44 Case C-301/06 *Ireland v. European Parliament and Council*, Judgment of the Grand Chamber of 10 February 2009.

was not the appropriate legal basis for this legislative measure, because its main objective is to facilitate the investigation, detention and prosecution of serious crime, including terrorism, and thus it should have been adopted under the third pillar. The Court did not share this view and held that the Directive was adopted on the appropriate legal basis, since both its aim and its content fall under Article 95 EC. The ECJ distinguished *Ireland v European Parliament and Council* from the *PNR* judgment on the ground that Directive 2006/24 covers the activities of service providers in the internal market and does not contain any rules governing the activities of public authorities for law-enforcement purposes as was the case in *PNR*. However, the Court stated expressly that the action brought by Ireland (and therefore its judgment) related "solely to the choice of legal basis and not to any possible infringement of fundamental rights arising from interference with the exercise of the right to privacy contained in Directive 2006/24".[45] Doubts about the conformity of this directive with fundamental rights have been raised in some Member States. In Romania for instance, a tribunal seized the Constitutional Court about the alleged unconstitutionality of the Romanian Data Retention Law, in the context of a case filed by an NGO against a telecommunications company on privacy grounds.[46] The Constitutional Court in Romania declared the law implementing the data retention directive unconstitutional and in violation of fundamental rights of privacy on 8 October 2009.[47] The reasoning of the court does not just relate to the implementing legislation in Romania, but questions the fundamental rights compatibility of the directive itself. In Germany, a case challenging the fundamental rights compatibility of the German legislation implementing the data retention directive is currently pending before the Federal Constitutional Court. The court did issue a temporary injunction, which provides for partial suspension of the implementing legislation until the final decision is reached.[48] On 2 March 2010, the German Federal Constitutional Court declared the German legislation implementing the EU Data Retention Directive unconstitutional.[49] In this context, it might be advisable that the European Union reviews the fundamental rights conformity of the EU Data Retention Directive 2006/24/EC proactively in the light of the new fundamental rights standards of the Lisbon Treaty (see below). A further ruling of the European Court of Justice on the fundamental rights conformity of the data retention directive would be desirable in this context to ensure legal certainty across all EU Member States.

45 *Ireland v. European Parliament and Council*, para 57.

46 http://www.mondonews.ro/Legea-298-de-stocare-a-datelor-telefonice-ajunge-la-CCR+id-5439.html (07.09.2009).

47 Romania/Curtea Constituțională, Decision nr. 1258 of 8 October 2009 of the Romanian Constitutional Court, available at: http://www.legi-internet.ro/fileadmin/editor_folder/pdf/Decizie_curtea_constitutionala_pastrarea_datelor_de_trafic.pdf (24.02.2010).

48 German Constitutional Court, press release Nr 37/2008 of 19 March 2008.

49 In its decision of 2 March 2010 the German Constitutional Court (1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, Urteil vom 2. März 2010) found unconstitutional the law transposing the Data Retention Directive in Germany on the ground that the obligations it imposes are disproportionate. In particular, the Court held that Section 113 of the Telecommunications Act does not guarantee the security of the stored data; lacks in transparency because it imposes a direct use of the data for the investigation, detection and prosecution of a number of criminal offences that are not specified clearly; and the legal protection that it affords to the data subject is not compatible with the requirements of the German Constitution, http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011.html (04.02.2010).

The main limitation currently faced by the EU to provide for effective and comprehensive data protection arises from the former constitutional architecture of the EU pillars. While data protection is highly developed in the former first pillar of the EU, the data protection regime in the former third pillar cannot be regarded as satisfactory. Yet the former third pillar of the EU comprises areas such as police cooperation, the fight against terrorism and matters of criminal law where data protection is especially important and crucial.

3.3. The Lisbon Treaty

In the context of the fundamental right to data protection, the Lisbon Treaty constitutes a significant step forward for the EU since it contains a number of important improvements concerning data protection at EU level. A first major improvement is that the Lisbon Treaty confers binding legal status on the Charter of Fundamental Rights. Article 8 of the Charter on the protection of personal data will be in a position to play a role which goes far beyond its formal and symbolic proclamation as a fundamental right. The recognition of data protection as an autonomous fundamental right with full legal validity as part of primary EU law means that data protection will play a more important role when balanced with other values and interests (e.g. security or market interests), and when priorities are being defined by the EU legislator and by the ECJ. A second major improvement is the abolition of the former 'pillars structure' This means that under the Lisbon Treaty, the structural problems previously faced by the former third pillar, concerning the decision making process and judicial review, are remedied. Thus, qualified majority voting is introduced in the area of Freedom, Security and Justice, the European Parliament's role was strengthened and the ECJ has full jurisdiction in the area. However, it is to be noted that special arrangements will apply to the United Kingdom and Poland due to the Protocol Nr. 30 to the Lisbon Treaty, which seeks to limit the effects of the EU Charter of Fundamental Rights in British and Polish law. A similar intention to limit the effects of the EU Charter in Czech law was the purpose of point 2 of the Presidency Conclusions of 29/30 October 2009 where it is agreed that a protocol will be attached to the EU treaties to the effect that Protocol Nr. 30 "shall be modified in order to refer to the Czech Republic in the same terms as they refer to Poland and to the United Kingdom".[50] Declaration No. 20 to the Lisbon Treaty says that whenever roles on protection of personal data are to be adopted which could have direct implications for national security, "due account" will have to be taken of the specific characteristics of the matter. Declaration No 21 notes 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 may prove necessary because of the "specific nature" of these fields. The question of the concrete effects of these protocols and declarations for the protection of personal data remains debatable, and will not be clarified until case law by the Court of Justice starts to emerge.

50 http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/ec/110889.pdf (24.02.2010).

4. Comparative Overview

This core section of the report will present a comparative overview of the national Data Protection Authorities, domestic practices implementing the requirements of data protection legislation, the remedies available in the Member States to sanction and compensate the violations of the data protection legislation and awareness of data protection rights among EU citizens. The information presented here is based on the 27 national studies produced by the FRALEX teams (all publicly available on the website of the agency as background material: http://fra.europa.eu) based on common guidelines elaborated by the Agency. This comparative report was developed on the basis of these studies. The national studies are dated February 2009.

4.1. Data Protection Authorities

All EU Member States, in compliance with the requirements of Article 28(1)(1) of the Data Protection Directive, have conferred one national supervisory Authority with the wide remit of monitoring the application of and ensuring respect for data protection legislation within their territories. Several Member States (e.g. Austria, Netherlands) have designated one Data Protection Authority of general competence and several other sector-specific supervisory bodies (for instance, in health, post or telecommunications). Some of those States organised along federal lines or with significant powers held at the regional level (e.g. Germany, Spain) are endowed, in turn, with one national supervisory body and several sub-state agencies entrusted with the same function at the regional or federal level.[51] Furthermore, whereas in many countries (e.g. Romania), prior to the establishment of Data Protection Authorities, the duty to monitor the respect for privacy rights was entrusted to Ombudsman institutions, in some Member States (e.g. Finland), the Ombudsman still maintains a relevant function in protecting personal data.

In this section, a comparative overview is presented. Good practices in this context are presented later in section 6.1.

4.1.1. Independence

EU Member States have made positive efforts to comply with Article 28(1)(2) of the Data Protection Directive, which requires Member States to ensure that their national Data Protection Authorities act in complete independence while exercising the functions entrusted to them. The interpretation of this provision of the Data Protection Directive was the subject of an Opinion of Advocate General Mazák. In this Opinion, the term "independence" is qualified as relative in nature, since it is necessary to specify in relation to whom and at what level such independence must exist. Concerning data protection authorities, it is stated that the purpose of such authorities needs to be taken into account when assessing their independence.[52]

In several countries, however, normative or practical obstacles raise concern as to the effective independence of the national supervisory bodies from the political branches of government. The guarantee of independence is, in fact, primarily assured by the procedure of nomination and removal of the officers of the Data Protection Authorities. The control over financial resources represents a second relevant element in ensuring the autonomy of the supervisory authorities.

In a number of Member States (e.g. Germany, Slovenia) officials of Data Protection Authorities are elected by the legislative assemblies, sometimes even through procedures which require consensus between the majority and the opposition (e.g. Greece). With some exceptions (such as Hungary, where a constitutional practice allows parliamentary parties to distribute available positions amongst each other according to that party's choice of candidate), this ensures a high level of independence of the elected officials. In other Member States, in contrast, data protection officers are directly appointed by the Government (e.g. Ireland, Luxembourg), with no involvement of the opposition in Parliament. In several cases (e.g. United Kingdom,[53] Lithuania, Estonia) this has raised severe concerns as to the effective independence of the Data Protection Authority. Similar concerns may arise in those countries where the supervisory authority is attached to the Ministry of Justice (e.g. Denmark, Latvia). Finally, other Member States (e.g. France, Spain, Portugal, Belgium) provide for a combined procedure to nominate the officers of the national Data Protection Authority, involving the executive, the legislature and the judiciary or other organized societal groups (e.g. the Supreme Council of the Universities in Spain) at the same time. In similar cases, however, it is essential to ensure that the

51 For comparative purposes, however, this report will only analyze the Data Protection Authorities established at the State level. Note that in Germany similar data protection authorities exist at the level of the Länder with supervisory powers over the public and private sphere, over the broadcasting institutions or the churches. In addition, in some Länder there are supervisory authorities only competent for the supervision of the private sphere. This report does not cover these supervisory authorities at Länder level.

52 Opion of Adovocate General Mazák, Case C-518/07, *Commission of the European Communities v Germany*, delivered on 22 October 2009. The Commission launched this infringement procedure against Germany for incorrect implementation of the EU Data Protection Directive for data protection authorities in the private sector (lack of independence). The European Court of Justice (Grand Chamber) delivered the judgement in the case C-518/07, Commission of the European Communities v Germany, on 9 March 2010 and stated under points 18 and 19 of the judgement: "With regard, in the first place, to the wording of the second subparagraph of Article 28(1) of Directive 95/46, because the words 'with complete independence' are not defined by that directive, it is necessary to take their usual meaning into account. In relation to a public body, the term 'independence' normally means a status which ensures that the body concerned can act completely freely, without taking any instructions or being put under any pressure. Contrary to the position taken by the Federal Republic of Germany, there is nothing to indicate that the requirement of independence concerns exclusively the relationship between the supervisory authorities and the bodies subject to that supervision. On the contrary, the concept of 'independence' is complemented by the adjective 'complete', which implies a decision-making power independent of any direct or indirect external influence on the supervisory authority."

53 In the UK, as of 2009, the Parliament has an advisory role and a public hearing of the chosen candidate takes place before the Justice Select Committee before appointment. The views of the committee are non-binding, but generally taken into account before appointment.

Government does not, in practice, control directly or indirectly the majority of the appointees, thus effectively frustrating the purpose of a pluralistic nomination procedure.

In a number of Member States (e.g. Italy), officers of Data Protection Authorities have a tenure of seven years with a prohibition of recall or reappointment for a second term. In some countries (e.g. Slovenia, Poland) officers of Data Protection Authorities may be subject to early dismissal from office only on specified grounds of misconduct and only after following the same procedure used for their appointment. These technical solutions ensure a high level of independence of the supervisory bodies, by reducing political influence and pressure. In other Member States (e.g. Ireland), on the contrary, the Government can directly remove the data protection commissioners from office, raising concerns as to the genuine independence of the supervisory body especially in monitoring governmental authorities' compliance with data protection legislation.

The autonomy of the supervisory body is particularly enhanced where, as in Portugal and Greece, the existence and remit of an independent authority, tasked to oversee the respect of data protection legislation, is explicitly established in the Constitution. Other significant guarantees of institutional independence, then, are provided by the attribution of distinct legal personality to the Data Protection Authority (e.g. Spain, Malta) and by the possibility for it to commence legal proceeding before the national Constitutional Court (e.g. Slovenia).

4.1.2. Resources

In most EU Member States Data Protection Authorities receive the resources necessary for their functioning from the State's budget (e.g. Italy, France, Netherlands, Estonia), and often from the budget allocated to the Ministry of Justice. In some Member States, however, the supervisory authorities are able to significantly increase their financial resources through the revenues obtained from the notifications of the data processors and/or the monetary sanctions imposed as a penalty for the infringement of data protection legislation (e.g. Luxembourg, Malta). In the United Kingdom, notification fees are the only source of income for the data protection work of the supervisory authority.

In a large number of Member States (e.g. Austria, Italy, Romania, France, Portugal) the lack of adequate funding of supervisory authorities was highlighted as a problem in the national studies. In other countries where the Data Protection Authority is currently relatively well funded, budget cuts have been set for the coming years (e.g. Ireland, Denmark). Given the tasks entrusted to the Data Protection Agencies by both EU and national law, the absence of sufficient human and financial resources represents a significant challenge to the effectiveness of the national supervisory systems that might jeopardize the protection of the fundamental rights of data subjects. As such, Member States should ensure that national Data Protection Authorities are provided with enough resources to function properly.

4.1.3. Powers

EU Member States were bound to endow their national supervisory Authorities with the general powers specified in the Data Protection Directive, Articles 28(2) (power to advise legislative or administrative authorities in the process of drafting legislation or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data), 28(3) (power of investigation, of intervention and of engagement in legal proceedings) and 28(4) (power to hear claims). As will be apparent from the overview below, these provisions of the Data Protection Directive, however, have not been fully implemented in all Member States, creating a situation where some national authorities are entrusted with only limited instruments to fulfil their supervisory tasks. As such, this is a problem that has to be addressed by the affected countries.

In general terms, in analyzing the powers of the various national Data Protection Authorities, it is possible to distinguish between two general tendencies, reflecting the approaches followed by the Member States in implementing the Data Protection Directive. Whereas several countries (e.g. Finland, Sweden, Ireland, United Kingdom) have stressed the preventive and proactive role of the supervisory agencies, emphasizing their *ex-ante* role in ensuring the protection of personal data, other Member States (e.g. Latvia, Czech Republic, Greece) have given priority to the *ex-post facto* enforcement and control function of the Data Protection Authorities, and charged them with a reactive duty to monitor compliance with data protection legislation. The nature of the powers entrusted to the supervisory bodies has, therefore, varied accordingly, with a preference for 'soft' preventive instruments in the first cases and for 'harder' measures in the second cases. It is important, nonetheless, not to overemphasize these differences: there are indeed countries (e.g. Denmark, Netherlands, Slovenia, and Italy) who have adopted a median stand, entrusting their national Data Protection Authorities with powers designed to help and ensure active compliance with data protection legislation, while at the same time empowering them to pursue and punish breaches. Moreover, there are several common features that cut across these distinctions between countries, as will become apparent in the next four sub-sections.

4.1.3.1. Powers of investigation

According to Article 28(3)(1) of the Data Protection Directive supervisory bodies should be endowed with powers of investigation, such as the power of access to data forming the subject-matter of processing operations and the power to collect all the information necessary for the performance of their supervisory duties. The following Table No. 1 indicates the degree of implementation of the above mentioned provisions in national legislation instituting the Data Protection Authorities, highlighting whether the supervisory authority is empowered to: a) request the data processor/controller/subject to provide information or produce documents; b) request access to data banks and filing systems from the data processor/controller; c) carry out searches and seizures in the premises of the data processor/controller without warrant; d) carry out searches and seizures in the premises of the data processor/controller after obtaining a warrant; e) conduct audits to control compliance by the data processors/controller and to ensure that data processing is carried out in conformity with the relevant legislation.

Table No. 1 Powers of investigation

Member State	Request information and documents	Access data banks and filing systems	Search of premises and seizure without judicial warrant	Search of premises and seizure premises with judicial warrant	Conduct audits
Bulgaria	●	●	●		●
Belgium	●	●	●		●
Czech Republic	●	●	●		●
Denmark	●	●	●		●
Germany	●	●	●	● [54]	●
Estonia	●	●	●		●
Greece	●	●	●		●
Spain	●	●	●		●
France	●	●		●	●
Ireland	●	●	●		●
Italy	●	●	● [55]	●	●
Cyprus	●	●	●		●
Latvia	●	●	●		●
Lithuania	●	●	●		●
Luxembourg	●	●	●		●
Hungary	●	●	●		●
Malta	●	●		●	●
Netherlands	●	●	●		●
Austria	●	●	●		●
Poland	●	●	●		●
Portugal	●	●	●		●
Romania	●	●			●
Slovenia	●	●	●		●
Slovakia	●	●	●		●
Finland	●	●	●		●
Sweden	●	●	●		●
United Kingdom	●			●	● [56]

54 This observation is limited to the Federal Data Protection Commissioner. It does not concern the data protection commissioners at the Länder level and the supervisory authorities over the private sphere.

55 Normally a judicial warrant is not required in Italy, if a search is carried out at a person's home or in another private dwelling with that person's consent. Alternatively an authorisation from the judge shall be required.

56 The UK data protection authority can only carry out an audit at the request of the controller, not against the wishes of a controller. The power therefore cannot be used to control compliance with the law.

As Table No. 1 illustrates, the vast majority of Member States allow their Data Protection Agencies to monitor the respect of data protection legislation by private and public operators involved in data processing, and more specifically to audit the interested parties; conduct examinations; order the delivery of information; order the grant of access to business data and documents; and copying data and documents. These powers can be exercised *proprio motu* or upon request or application by a data subject who alleges violations of his personal data rights. In the vast majority of Member States, supervisory authorities can, in the exercise of their functions and in order to detect violations of the data protection legislation, enter (if necessary with help of the police) premises and any other place where data processing is performed, seize the necessary equipment, investigate and take evidence (even against the data controllers' consent), without the need to request a prior judicial warrant.

4.1.3.2. Powers of intervention

According to Article 28(3)(1), second indent of the Data Protection Directive supervisory bodies should be endowed with powers of intervention, such as that of delivering opinions before processing operations of sensitive data are carried out and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller. The following Table No. 2 gives information of the degree of implementation of the above mentioned provision in the various domestic legislation, highlighting where, supervisory authorities are empowered to: a) register the processing operations that are notified by the data controllers; b) authorize the processing operations likely to present specific risks to the rights and freedoms of data subjects after a prior check of their compatibility with the requirements of the data protection legislation; c) halt the processing of personal data; d) order the erasure or destruction of data; e) issue a warning to and reprimand the controller (i.e. by ordering the implementation of specific technical and organizational measures to prevent infringements of relevant legislation).

Table No. 2 Powers of intervention

Member State	Register processing operations	Authorize processing operations likely to present specific risks	Halt processing operations	Order the erasure or destruction of data	Issue a warning or reprimand the controller
Bulgaria	●	●	●	●	●
Belgium	●	●			
Czech Republic	●	●	●	●	●
Denmark	●	●	●	●	●
Germany	●	●	● [57]		●
Estonia	●	●	●	●	●
Greece	●	●	●	●	●
Spain	●		●	●	●
France	●	●	●	●	●
Ireland	●	●	●	●	●
Italy	●	●	●	●	●
Cyprus	●		●	●	●
Latvia	●		●	●	●
Lithuania	●	●	●	●	●
Luxembourg	●	●	●	●	●
Hungary	●	●	●	●	●
Malta	●	●	●	●	●
Netherlands	●	●	●	●	●
Austria	●	●	●	●	●
Poland	●	●	●	●	●
Portugal	●	●	●	●	●
Romania	●	●	●	●	●
Slovenia	●	●	●	●	●
Slovakia	●	●	●	●	●
Finland	●	●	●	●	●
Sweden	●	●	●		●
United Kingdom	●		●	●	●

57 From 1 September 2009 it has been open to supervisory authorities to halt processing operations if certain conditions are met.

Table No. 2 underscores a certain convergence between the Data Protection Authorities of the EU Member States as far as the power of intervention is concerned. With the limited exception of prior checking of sensitive data processing operations, which is not provided *de jure* or *de facto* in certain countries, all supervisory bodies are requested to maintain a register for the notifications of the data processing operation. Except in Belgium and partially in Germany, moreover, they may: order a private data controller to discontinue a processing operation which is in violation of the act and to rectify, erase or block specific data undergoing such processing; ban private data controllers' use of a specified procedure in connection with the processing of data if there is a considerable risk that data is processed in violation of the relevant legislation; order private controllers to implement specific technical and organizational security measures to prevent illegal processing of data, accidental or unlawful destruction or alteration of data, disclosure of data to unauthorized persons, abuse of data or other unlawful forms of processing; and finally issue a prohibition notice or a mandatory injunction against data processors that are violating the relevant legislation.[58]

4.1.3.3. Powers to hear claims and engage in legal proceedings

According to Article 28(4)(1) of the Data Protection Directive supervisory bodies should be endowed with powers to hear claims lodged by any person, or by an association representing that person, concerning the protection of his/her rights and freedoms in regard to the processing of personal data and to inform the person concerned of the outcome of the claim. According to Article 28(3)(1) third indent, Data Protection Authorities must be able to engage in legal proceedings where the national data protection legislation has been violated or to bring these violations to the attention of the judicial authorities. Finally, Article 28(3)(1), second indent, allows supervisory bodies to refer cases to national parliaments or other political institutions. The following Table No. 3 illustrates the degree of implementation of the above-mentioned provision in the Member States, highlighting whether the supervisory authority is empowered to: a) hear and reviews claims or complaints from data subjects, b) refer the case to the attention of the police or the judicial authorities, c) bring the case directly before judicial authorities, acting as a party to a claim (i.e. engage in legal proceedings *stricto sensu*), d) make a determination in its own right as to the existence or not of a violation (with the possibility of issuing a sanction) thus performing a quasi-judicial function, and e) referring the matter to national parliaments or political institutions, especially by proposing legislative and regulatory measures for the modification of the relevant data protection legislation to address the most compelling problems arising from its application and to reflect the evolution of computer processing techniques.

58 The observation is limited to the competence of the Länder Data Protection Commissioners and/or the supervisory authorities in relation to the private sphere. It does not concern the Federal Commissioner for Data Protection.

Table No. 3 Powers to hear claims and engage in legal proceedings

Member State	Hear and review claims or complaints	Refer the case to the police or judicial authorities	Bring the case directly before judicial authorities	Make a determination itself as to the merits of a claim	Refer the matter to national Parliaments
Bulgaria	●	●	●	●	
Belgium	●	●	●	●	●
Czech Republic	●	●	●	●	
Denmark	●	●		●	
Germany	●	●	● [59]	● [60]	●
Estonia	●			●	●
Greece	●	●		●	●
Spain	●	●		●	
France	●	●		●	●
Ireland	●		●		
Italy	●	●		●	●
Cyprus	●	●		●	
Latvia	●		●	●	
Lithuania	●	●		●	●
Luxembourg	●	●	●	●	
Hungary	●	●			●
Malta	●	●	●	●	●
Netherlands	●	●		●	
Austria	●		●	●	
Poland	●	●		●	
Portugal	●	●		●	
Romania	●	●	●	●	
Slovenia	●	●	●	●	
Slovakia	●	●		●	●
Finland	●	●	●	●	●
Sweden	●	●	●		
United Kingdom	●	●			

59 This observation does not concern the Federal Commissioner for Data Protection in Germany, but the data protection authorities at Länder level.
60 This observation does not concern the Federal Commissioner for Data Protection in Germany, but the data protection authorities at Länder level.

The Table underscores some divergences between the Data Protection Authorities of the EU Member States. All supervisory bodies are endowed with the authority to hear complaints lodged by interested parties who allege a violation of their personal data rights and have a corresponding duty to provide an answer within a fixed time to the petitioners. Nevertheless, if at the end of an investigation the claim appears well founded, only some of national Data Protection Authorities can autonomously commence legal proceedings before a competent tribunal (notably, in the case of Slovenia, even before the Constitutional Court) or themselves exercise a quasi-judicial function by deciding on the merits of the case brought by the claimant (as an alternative forum to judicial authorities). Decisions of the administrative supervisory bodies entrusted with quasi-judicial powers are in any case always reviewable by ordinary courts: a necessary corollary of the rule of law required by Article 28(3)(2) of the Data Protection Directive.

4.1.3.4. Advisory powers

According to Article 28(2) of the Data Protection Directive, supervisory bodies should be consulted by national legislatures and administrations when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data. A general power of the Data Protection Authorities to provide advice and information to private parties involved in data processing operations and to issue general sector-specific recommendations may then be inferred from the purposes of the Data Protection Directive. Finally, Article 25 of the Data Protection Directive sets specific rules regulating the transfer of personal data to non-EU countries (i.e. third countries), possibly leaving room for the intervention of national supervisory bodies. The following Table No. 4 provides information on the advisory powers of the national Data Protection Authorities, highlighting whether supervisory bodies a) are *de jure* or *de facto* always consulted by the legislature and/or administrative offices prior to the enactment of legislation or regulations affecting individual rights to data protection; b) may be consulted at the legislature's and administrative offices' discretion, prior to the enactment of legislation or regulation affecting individual rights to data protection; c) provide advice and information for to the parties (e.g. informing them of their rights and obligations); d) issue general recommendations and opinions on how to enhance the implementation of and compliance with data protection legislation in specific sectors (e.g. promoting the drafting of codes of conduct); e) authorise the transfer of personal data to third countries.

Table No. 4 Advisory powers

Member State	Must be consulted by the legislature or adm. offices	May be consulted by the legislature or adm. offices	Provide advice and information to parties involved in data processing	Issue general recommendations and opinions	Authorize the transfer of data to third countries
Bulgaria	●		●	●	
Belgium	●	●	●	●	
Czech Republic		●	●	●	
Denmark		●	●	●	●
Germany	●	●	●	●	● [61]
Estonia	●		●	●	
Greece	●	●	●	●	●
Spain	●		●	●	●
France	●	●	●	●	●
Ireland		●	●	●	●
Italy	●	●	●	●	●
Cyprus	● [62]		●	●	●
Latvia	●		●	●	
Lithuania		●	●	●	●
Luxembourg	●		●	●	●
Hungary		●	●	●	● [63]
Malta		●	●	●	●
Netherlands	●		●	●	●
Austria	●		●	●	●
Poland		●	●	●	
Portugal	●		●	●	●
Romania		●	●	●	●
Slovenia		● [64]	●	●	●
Slovakia		●	●	●	●
Finland	●	●	●	●	
Sweden	●	●	●	●	●
United Kingdom		●	●	●	● [65]

61 German supervisory bodies can give authorisation, but it is not in all cases compulsory or necessary.

62 Section 23(i) of Law 138(I)/2001is interpreted by the Data Protection Authority in Cyprus as granting a right to be consulted whenever a regulation is under discussion. In practice, the Commissioner is invariably consulted by the legislature and by the administration whenever issues of personal data protection arise.

63 There are indications that this power is undermined by a lack of effective enforcement.

64 In SK, the data protection authority is de facto always consulted prior to enactment of legislation affecting data protection, even though this is not mandatory by law.

65 In practice, this power seems to be used rarely, if ever. See national thematic study on assessment of data protection measures and relevant institutions, UK, available on http://fra.europa.eu (24.02.2010).

As Table No. 4 highlights, all Member States have entrusted their domestic supervisory agencies with the authority to advise private parties on the application of data protection legislation. Data Protection Authorities have also a quasi-legislative power to produce general regulations for specific sectors, promote the drafting of private codes of conduct and provide opinions and recommendations for the public and private actors operating in the field of data processing. Most of these measures are, however, not legally binding. At the same time, many Member States accord only a consultative function to supervisory bodies in the context of advising the executive and legislature on draft legislation relating to personal data protection. Thus, their advice on draft bills and regulations is optional, or (as in France, Italy, Germany, Austria, Greece) only strictly legally required in the elaboration of executive regulations. This is regrettable considering that advice given during the drafting process may avoid problems in future. The absence of opinions issued by Data Protection Authorities prior to the enactment of legislation or guidelines that have a potentially negative impact on personal data protection, may signal that there is a failure to fully appreciate the importance of the protection of privacy when making political choices. As such, it may be recommended that Member States ensure a more consistent involvement of supervisory bodies in the policy-making process.

4.1.4. Activities

The supervisory bodies of the EU Member States are commonly involved in a series of activities directed at assessing the status of national privacy legislation as well as spreading the culture of personal data protection. To begin with, Data Protection Authorities perform the function of informing the general public and the State's institutions about challenges to privacy rights, the measures taken by the supervisory body to address them, and the steps necessary for improving their defence. Article 28(5) of the Data Protection Directive, indeed, requires supervisory bodies to draw up a report of their activities at regular intervals and to make it publicly available. All Data Protection Authorities, therefore, publish annual reports on the status of the protection of privacy rights in the domestic legal system, and some of them (e.g. Italy) even had monthly bulletins with the most up-to-date decisions or regulations adopted. In some countries (e.g. Spain, United Kingdom, France, Italy) the annual report is presented publicly, sometimes before the legislature, giving the mass media the opportunity to cover the event.

National supervisory authorities have a special duty to raise the awareness of privacy and personal data rights among EU citizens. This venture is particularly important since the effectiveness of data protection legislation can be ensured only when individuals are aware of their fundamental rights and actively involved in securing them. As will be analyzed below, in several Member States the general public is either largely unaware of its rights (e.g. Poland, Malta), or believes that privacy rights are well protected with limited need to improve the system (e.g. Denmark, Finland), or considers other rights, such as the right to information (e.g. Sweden) hold greater weight than data protection rights. Data Protection Authorities are therefore directly engaged in awareness-raising. With few exceptions (e.g. Lithuania, Bulgaria, Slovakia), they run specialized user-friendly web sites where all relevant legislation, opinions and decisions of the agency are available and constantly updated. Conferences, initiatives and special programs are then financed by the supervisory bodies in many countries (e.g. Slovenia, Netherlands) to target specific sectors of the population, such as students and employees.

At the EU level, the national supervisory authorities cooperate and work jointly with each other under the framework of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data, established by Article 29(1)(1) of the Data Protection Directive (also known as the "Article 29 Working Party"). According to Article 29(2) the Working Party is composed of the European Data Protection Supervisor, one representative of each of the national supervisory authorities, and a representative of the European Commission. The Working Party has an advisory status and acts independently. Article 30(1) specifies that it shall: examine any question covering the application of the national measures adopted under the Directive in order to contribute to the uniform application of such measures; gives the Commission an opinion on the level of protection in the EU and in third countries; advises the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed EU measures affecting such rights and freedoms; and offer an opinion on codes of conduct drawn up at EU level. The opinions and recommendations of the Working Party are generally taken into account and referred to by the national Data Protection Authorities, and are particularly helpful in the development of a common EU standard of personal data protection, shared by all national supervisory bodies.[66]

4.2. Compliance

In this section, a comparative overview is presented. Good practices in this context are presented in section 6.2 below.

4.2.1. Data Protection Registrations and Approval Procedures

Article 2 of the Data Protection Directive provides that 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. Furthermore, Articles 5 to 8 of the Data Protection Directive set out the general rules and principles on the lawfulness of the processing of personal data, the criteria for making data processing legitimate and special categories of processing such data.

66 In UK, opinions and recommendations of the Working Party are not considered binding by the UK data protection authority, even though they are sometimes referred to as informal guidance.

In relation to these, Articles 18 to 20 refer to the obligation to notify the supervisory authority and the prior checking of processing operations likely to present specific risks to the rights and freedoms of data subjects.

The national thematic studies have been heavily relied on in assessing compliance with data protection standards, such as the rules relating to data protection registrations and data protection approval procedures. The vast majority of these included data on the number of registrations and approvals for the years 2000-2007. Several contained analysis and qualitative assessments based both on these figures as well as from contacts with the respective national authorities. These figures have served as indicators for assessing compliance. Other indicators include practices of national authorities, the degree of compliance with national legislation and typified instances of non-compliance with the Directive.

The majority of EU Member States (Bulgaria, Lithuania, Austria, Ireland, Finland, Denmark, Sweden, Luxembourg, Czech Republic, Spain, Italy, Malta, Netherlands, Poland, Romania, Slovenia, Cyprus, Estonia, Greece, Portugal, Latvia, and Germany) have elaborated a legal framework that transposes the stipulations of the Data Protection Directive in an effective manner. By effective transposition it is meant that the national legislation is *prima facie* in compliance with the requirements of the Directive. The effectiveness of the actual implementation of national legislation varies between Member States and is the object of the analysis found in the following paragraphs. On the other hand, 5 Member States (France, Hungary, Slovakia, United Kingdom, and Belgium) exhibit deficiencies in their laws which create inconsistencies between the overall system created by the Data Protection Directive and the national provisions. The assessment of compliance represents, however, a rather problematic area. In many instances understaffing in the national DPAs has meant that they have been unable to provide a systematic and statistical account of the situation in the field. Even when such statistical data exist they are not always consistent and sufficient to provide a proper account of the situation. It has, therefore, been impossible to arrive at an aggregate, EU-wide and overall assessment of the degree of compliance and/or of problematic areas in law and in practice. From this extremely incoherent picture, examples of manifest failures to comply with the directive are taken from the national thematic studies to illustrate some of the problems encountered.

Bulgaria has transposed the relevant provisions of the Data Protection Directive, but the practice personal data controllers relating to registrations shows that the national authority was not prepared, from its creation, to develop its administrative capacity sufficiently to allow for the implementation of its duties.[67] The national authority cannot yet deal effectively with the large number of applications for registration. The ratio of applications to registrations is disproportionate, in the sense that registrations remain disproportionately low in comparison to the number of applications for registration.[68]

In Poland, according to national legislation, every entity engaged in the processing of data is obliged to register a data filing system with the National Data Authority, which has limited investigatory powers on data processed by special state services (e.g. intelligence services). Even when an entity processing data is not obliged to register the processing of data, it remains obliged to fulfil the requirements enabling the processing of data. The processing of sensitive data is prohibited as a general rule, with exceptions falling largely within the provisions of the Data Protection Directive. The main problem which is identified is the lack of awareness of entities processing data about the obligation to register. In numerous cases these entities failed to register the data filing systems, while further mistakes are numerous at the registration stage. Processing of sensitive data has raised problems in two significant cases. Firstly, relating to collecting data of Roma children. In this instance the national authority ordered the deletion of the data concerning Roma children which was processed without their knowledge and consent.[69] The second case concerned the processing of data of election candidates from different national and ethnic minorities. The national authority ordered the suspension of the processing of data acquired from unofficial sources without the data subject's consent.[70] The 2007 report of the national authority revealed lack of compliance with data protection standards in certain sectors of the public administration.[71] The public security sector does not reveal any particular deficiencies in the field of data protection and the institutions seem to comply with the legislation. Entities processing data in different commercial fields, public health institutions, banks and financial institutions were found not to fully comply with the legislation.

Greece's legislation initially introduced a system of universal notification, thus avoiding the possibility of exceptions and simplifications to registration and notification procedures offered by the Data Protection Directive. A subsequent amendment of the law introduced the possibility of exemptions, which led to a drastic decrease in notification numbers. The Greek legislature has not adopted the option provided by the Data Protection Directive, allowing the appointment of an internal privacy/data protection officer. Due to the inherent asymmetry of power that characterizes the employer–employee relationship, the national authority rejects consent of the individual as a ground that legitimises of itself, processing of personal data.[72] As far as compliance with the decisions of the national Data Protection Authority is concerned, in the vast

67 By December 2003, four employees of the national authority were confronted with 227, 251 applications. Annual Report of Commission for Personal Data Protection of the Republic of Bulgaria 2002-2003, pp. 11-12, available in Bulgarian at: http://www.cpdp.bg/godishniotcheti.html (10.01.2009).

68 For example, in 2006 applications reached 274,446 and the registrations 31,970. Annual Report of Commission for Personal Data Protection of the Republic of Bulgaria 2006, p.17, available in Bulgarian at: http://www.cpdp.bg/godishniotcheti.html (10.01.2009).

69 Decision issued on 12 October 2007, reference: GI-DEC-DOLiS-218/07/5787, 5788.

70 Decision issued on 23 November 2007, reference: GI-DOLiS-430/103/07/6592.

71 This included: the storage of data in inappropriate conditions, such as on shelves and in drawers without locks; the use of IT systems that often did not meet the technical requirements prescribed by law; in isolated cases, the use of IT systems that allowed access to data filling to non-authorized persons; the use of data collected during administration proceedings for a goal other than the stated purpose; in isolated cases, publishing data of persons, via a website, without prior consent.

72 An approach adopted also by the European Commission in the Report: Possible content of a European framework on protection of workers' personal data, Brussels 2002.

majority of cases the controllers comply. A prominent case of non-compliance, which gave rise to serious concerns and a public outcry, was the use by the Greek Police of CCTV systems for filming political demonstrations despite binding decisions to the contrary issued by the national authority regarding the use of cameras in public places[73] while the ruling of the DPA was pending before the Plenary of Council of State.[74] Additionally, the auditors of the authority were not allowed to access the premises of the police in order to control compliance with the authority's decisions. The Chairman and most of the members of the authority subsequently tendered their resignations.

Regarding the United Kingdom, it has been reported that the European Commission is investigating alleged failures to implement eleven of the Directive's thirty-four articles properly – almost a third of its provisions.[75] Although the United Kingdom Government still claims that it has implemented the Directive fully, many deficiencies have been pointed out.[76] Even more problematic, the national Data Protection Authority has made it clear that it feels that it is not its task to ensure that the national law is interpreted in a way consistent with the EC Directive, or to point out where national law might fail to meet the requirements of the Data Protection Directive.[77]

Germany has transposed the Data Protection Directive both in federal and the *Länder* data protection laws. Non-public bodies have a duty to notify automated data processing operations prior to their implementation to the supervisory authority or the competent Commissioner for Data Protection. Public bodies of the Federation have to announce such operations to the national authority. Obligatory registration does not apply if the controller has appointed an internal data protection officer. It appears that a significant number of private companies that are by law obliged to appoint data protection officers do not comply with this obligation and that those companies that do comply with the general obligation to appoint data protection officers very often do not facilitate the efficient and effective work of those appointed. Also, it cannot be ignored that the majority of medium-sized enterprises still display a range of problems with data protection. This is due to the fact that the appointed data protection officers – should they be appointed at all – cannot initiate changes to practice that may be required due to a lack of time either for relevant training to enable them to do this or time to discharge of their responsibilities adequately. Recent scandals, which have involved both private and public institutions, highlight extensive and serious cases of data and privacy violations on a large scale.[78] These cases involve, amongst others, severe violations of privacy rights through spying on or secretly observing employees by video, or by computerized profile searches against employees in the work place. Others relate to data trading in unprecedented amounts without the prior approval of data subjects.[79] The failure to take appropriate measures such criminal prosecution often exacerbates the problem.

4.2.2. Appointment of internal Data Protection Officers

Regarding the appointment of internal data protection officers, most of the national laws provide for general requirements with no specific knowledge or expertise in the field being required. In Denmark, Italy and Greece, the legislation does not provide for the appointment of data protection officers. In Belgium, the relevant royal decree is silent on the policy of appointment of internal data protection officers. In the explanatory statement relating to the royal decree of 13 February 2001 executing the Data Protection Act, the government explicitly states that the idea of appointing such a person did not receive support in Belgium. In Austria, the legislation does not create any obligation to appoint internal data protection officers, but in the public sector trade unions have promoted the appointment of such internal data protection officers. In relation to the remaining Member States these fall largely into two categories: a) those whose national legislation provides for certain requirements to be met and b) those that do not do so. The national legislation of some Member States (Cyprus,[80] Bulgaria,

73 Decision 58/2005 of the national data protection authority (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα),http://www.dpa.gr/portal/page?_pageid=33,15453&_dad=portal&_schema=PORTAL (19.02.2008).

74 The Greek Ministry for Public Order made an application to the Council of State seeking to overturn the Authority's decisions.

75 'Europe claims UK botched one third of Data Protection Directive', *Out-Law News*, 17 September 2007, available at: http://www.out-law.com/page-8472 (26.01.2009). Although this is, as such, a media article, it is based on information obtained directly from the authorities concerned under freedom of information law, and both the UK Government and the Commission confirmed that various issues were being discussed, without being specific. However, the information obtained by Out-Law showed that "the articles of the Directive which the Commission claims have not been implemented properly are articles 2, 3, 8, 10, 11, 12, 13, 22, 23, 25 and 28 ... These Articles relate to: the definitions used in the Directive (e.g. the meaning of personal data); the scope of the Directive's application to manual files; the conditions when sensitive personal data can be processed; the fair processing notices give to individuals; the rights granted to data subjects; the application of exemptions from these rights; the ability of individuals to seek a remedy when there is a breach; the liability of organisations for breaches of data protection law; the transfer of personal data outside European Union; and the powers of the Information Commissioner.'

76 E.g., D. Korff (2008) 'UK Data Sharing: European Conflict', in: *Data Protection Law & Policy*, p.12ff. Other issues were raised in the enquiry mentioned in the next footnote, and in R. Thomas and M. Walport (2008) *Data Sharing Review Report*, available at: http://www.justice.gov.uk/docs/data-sharing-review-report.pdf (26.01.2009).

77 As it was put by the Assistant Information Commissioner, Jonathan Bamford, in answer to a question by a House of Commons Select Committee during hearings on the Electronic Patient Record being introduced in the National Health Service, in a session in May 2007: 'If there is any issue to do with whether the UK Data Protection Act correctly implements the EU Data Protection Directive that is a matter for the Ministry of Justice, as it is now, because that is the body which is responsible for ensuring that we implement the Directive in UK law. If there is a concern about a difference it is for the Ministry of Justice to answer that point. The Information Commissioner is charged with implementing the UK Data Protection Act...If you have a real concern [about any failure of the Act to properly implement the Directive], I believe it is important that you speak to the Ministry of Justice as part of this inquiry.' Answer to Question 176 at the Select Committee hearing on 10 May 2007. Full transcript available at: http://www.parliament.the-stationery-office.co.uk/pa/cm200607/cmselect/cmhealth/422/7051002.htm (26.01.2009).

78 http://www.heise.de/tp/r4/artikel/28/28579/1.html (29.01.09), http://www.dorstenerzeitung.de/nachrichten/politik/blickpunkt/art302,350317 (29.01.09), http://www.tagesschau.de/inland/datenschutz110.html (29.01.09), http://www.sol.de/news/welt/tagesthema/Datenschutz;art7325,2705543 (29.01.09), http://www.ruhrnachrichten.de/nachrichten/politik/blickpunkt/art302,433610 (29.01.09), http://ez.omg.de/?id=20&nid=29923 (29.01.09), http://www.handelsblatt.com/unternehmen/handel-dienstleister/rasterfahndung-bei-der-bahn;2136145 (29.01.09).

79 See http://www.aufrecht.de/news/view/article/illegaler-handel-mit-adress-und-kontodaten-sprengt-alle-grenzen.html (29.01.09).

80 The data protection legislation in Cyprus contains a provision that the personnel of the office of the national data protection authority in Cyprus shall possess the qualifications to be prescribed by regulations. Such regulations have not up to now been passed.

Estonia, Lithuania, Ireland, Sweden, Slovenia, Romania, Finland,[81] Portugal, and the United Kingdom) does not include any provisions concerning the requirements of appointment of data protection officers. For the remaining Member States (France, Luxembourg, Latvia, Czech Republic, Malta, Netherlands, Poland, Hungary, Slovakia, Germany), national legislation contains explicit provisions on the officers' independence or adequate knowledge of/expertise in the field. It must be noted that these requirements are not further qualified. The only exceptions are Hungary and Latvia where an internal data protection officer must hold a higher education degree in law, public administration or information technology, or a qualification equivalent thereto, in order to be appointed or commissioned within the organisation of the data controller or of the technical data processor.

In assessing the appointment requirements of data protection officers, it must be borne in mind that EU legislation does not provide for specific standards to be attained. However, it is obvious that appointing persons with special expertise and/or special awareness-raising roles contributes positively to ensuring that the applicable legislation is respected and implemented in full. Irrespective of the capacities and level of knowledge of data protection officers, it must be pointed out that the practice of their recruitment by a branch of the Executive is not conducive to the independence of the national data authorities. Furthermore, one Member State (Ireland) has opted for the adoption of guidelines and two others (Sweden and Slovakia) for special training for data protection officers. Finally, no evidence is available regarding compliance in this area.

4.3. Sanctions, Compensation and Legal Consequences

All EU Member States have implemented Chapter III of the Data Protection Directive, on "Judicial Remedies, Liability and Sanctions" in their legal systems. This requires national authorities to set up adequate and effective remedies to ensure respect for the rights guaranteed in personal data legislation; the adoption of suitable and proportionate sanctions to be imposed in cases of breaches of data protection legislation; and provision of means to ensure compensatory damages for those adversely affected by unlawful processing of their personal data. Since, however, the provisions of the Data Protection Directive concerning remedies, sanctions and liability only set the objective to be pursued by Member States, without specifying detailed criteria to be followed, a number of differences exist among the national laws on data protection. These relate both to the possibility of obtaining justice and receiving damages, and of having violators sentenced and punished for breaches of personal data rights.

4.3.1. Remedies

Article 22 of the Data Protection Directive codifies the general obligation for Member States to provide, "without prejudice to any administrative remedy… for the right of every person to a judicial remedy for any breach of the rights guaranteed him". The following Table No.5 details the various methods through which the national legal systems to ensure compliance with EU law. These are: a) administrative remedies before the Data Protection Authority; b) non-judicial remedies before the supervisory body (as an alternative to legal action which, once commenced, preclude a claim before a judicial authority); c) judicial remedies available before the ordinary courts or tribunals.

81 Specific provisions concerning appointment of data protection officers can only be found in the Act on the Electric Processing of Client Data within the Social- and Healthcare Services as well as in the Act on the Electronic Medical Prescriptions (*Laki sähköisestä lääkemääräyksestä, Lag om elektroniska recept*, Act no. 61/2007). These Acts require that social and healthcare service providers, pharmacies, The Social Insurance Institution of Finland (KELA) and The National Authority for Medicolegal Affairs (TEO) designate Data Protection Officers.

Table No. 5 Remedies

Member State	Administrative remedies before the DPA	Non-judicial remedies before the DPA	Judicial remedies before the ordinary courts or tribunals.
Bulgaria	●		●
Belgium		●	●
Czech Republic	●		●
Denmark	●		●
Germany	●		●
Estonia	●		●
Greece	●	●	●
Spain	●		●
France	●		●
Ireland	●		●
Italy	●	●	●
Cyprus	●		●
Latvia	●		●
Lithuania	●		●
Luxembourg	●		●
Hungary	● [82]		●
Malta	●		●
Netherlands	●		●
Austria	●		●
Poland	●		●
Portugal	●		●
Romania	●		●
Slovenia	●		●
Slovakia	●		●
Finland	●		●
Sweden	●		●
United Kingdom	●		●

82 In Hungary the Data Protection Authority has limited powers to provide administrative remedies, but lacks the ability to enforce these.

Individuals in all Member States can lodge a claim relating to a specific violation or a more general complaint before the national Data Protection Authorities, alleging an infringement. A fundamental principle of the Rule of Law is the right, also recognized in all Member States, to initiate legal proceedings before ordinary courts of justice to obtain a judicial decision on the dispute. Often this can be via simplified procedures (e.g. Italy, Belgium).. As a matter of fact, however, in several Member States (e.g. Finland, Austria, Latvia, Estonia), judicial remedies, while available in theory, are not pursued by complainants in practice. Only Belgium, Italy and Greece, allow data subjects the option of settling disputes, either through the courts or by lodging a complaint with the Data Protection Authorities which may offer a swift and cost-effective remedy via a quasi-judicial procedure.

4.3.2. Sanctions

According to Article 24 of the Data Protection Directive Member States are compelled to "lay down the sanctions to be imposed in case of infringement" of the data protection legislation. The implementation of this general provision at the national level, nonetheless, has given rise to significant variations. The influence of domestic legislation and practice in the field of criminal and administrative law indeed is particularly relevant in this field and has shaped both the approach followed initially by the legislatures of the Member States in drafting the relevant legislation and the subsequent approach of the administrative and judicial authorities in its interpretation and enforcement. As it is not possible to provide a comprehensive comparison of the national (administrative and criminal) law relating to sanctions (and punishments) against data protection violations, the analysis will focus here on the institutions entrusted with the power to adopt sanctions, and on the main sanctions that they may adopt.

A variety of sanctions may be imposed by the Data Protection Authorities. As well as those presented above in section 3.1.3.2 (issuing a warning or reprimand to the data processor/controller, ordering the suspension of the processing of personal data, blocking and erasure of specific data), supervisory bodies are also empowered to order pecuniary sanctions. Courts may also order pecuniary sanctions as well as imprisonment or its alternatives such as a suspended prison sentence or community service. The following Table No. 6 illustrates the range of consequences that may flow from the failure to comply with data protection legislation in each legal system: a) administrative fines imposed by the Data Protection Authorities; b) criminal fines imposed by courts; c) imprisonment or its alternatives imposed by courts. Note that the duty to compensate loss and damages will be analyzed separately below.

Table No. 6 Sanctions

Member State	Administrative fines imposed by the DPA	Criminal fines imposed by the judicial authorities	Detention imposed by judicial authorities
Bulgaria	●		
Belgium		●	
Czech Republic	●		
Denmark		●	●
Germany	● [83]	●	●
Estonia	●	●	●
Greece	●	●	●
Spain	●		
France	●	●	●
Ireland	●	●	
Italy	●	●	●
Cyprus	●	●	
Latvia	●		
Lithuania		●	
Luxembourg	●	●	
Hungary		●	●
Malta	●	●	●
Netherlands	●	●	●
Austria		●	●
Poland		●	●
Portugal	●		●
Romania	●	●	
Slovenia	●	●	●
Slovakia	●	●	●
Finland	●	●	●
Sweden		●	●
United Kingdom		●	●

83 In 2008, for instance, administrative fines amounting to 1.4 million euros were imposed on and accepted by the commercial enterprise LIDL.

As Table No. 6 illustrates, Data Protection Authorities are empowered to levy economic sanctions only in some Member States (and their decisions are anyhow always subject to appeal before administrative courts). In other Member States (e.g. Belgium, United Kingdom) DPAs may only negotiate amicable solutions with those found in violation. The effectiveness of administrative sanctions ordered by supervisory bodies, however, has raised concern in a number of Member States, because the level of fines is seen as too low or fines are imposed too infrequently to have a dissuasive effect. In other Member States (e.g. Austria, United Kingdom, Denmark, France), it is rather the practice of judicial authorities that has proved to lack a dissuasive effect. Thus in some Member States (e.g. Estonia) criminal sanctions have never actually been issued by judicial authorities.

4.3.3. Compensation

According to Article 23(1) of the Data Protection Directive Member States are to "provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered". National legislation on civil liability however, differs, depending on whether Member States have decided to specifically regulate the duty to compensate damage suffered in a data protection case, or have simply provided an extension of the ordinary framework of civil liability in the field of personal data protection. The following Table No. 7 presents the main solutions chosen by the Member States in implementing the provision of the Data Protection Directive: a) an extension of the ordinary framework of civil liability (with the plaintiff carrying both the burden of proof of the damage suffered and the risk of the costs of litigation); b) an extension of the existing framework of civil liability but with reversal of the burden of proof (allowing the controller to be exempt from liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage); c) the implementation of a special framework of civil liability.

Table No. 7 Compensation

Member State	Extension of the existing framework of civil liability	Existing framework of civil liability with the reversal of the burden of proof	Special framework of civil liability
Bulgaria	●		
Belgium	●		
Czech Republic	●		
Denmark		●	
Germany		●	●
Estonia	●		
Greece			●
Spain	●		
France	●		
Ireland	●		
Italy		●	
Cyprus	●		
Latvia	●		
Lithuania	●		
Luxembourg	●		
Hungary			●
Malta	●		
Netherlands	●		
Austria	●		
Poland	●		
Portugal	●		
Romania	●		
Slovenia	●		
Slovakia	●		
Finland	●		
Sweden		● [84]	●
United Kingdom	●		

84 In the Swedish Personal Data Act there are special rules on compensation, but the procedure falls within the existing framework of civil cases.

As illustrated by Table No. 7 compensation is due wherever damage is caused by the failure to process personal data in compliance with data protection legislation. In most Member States compensation may, in theory, be obtained via standard judicial proceedings regulated by general provisions relating to civil liability, even though in a number of States awards of compensation in data protection cases were not detected (e.g. Cyprus, Malta, Portugal, Latvia), or very few lawsuits for damages brought before judicial authorities were found (e.g. Finland, Estonia). In several Member States the general rules on civil liability apply to data protection cases, with the exception of the reversal of the burden of proof, which is shifted from the claimant to the respondent (the data processor/controller). Finally, in some countries a special framework for obtaining damages has been created. In particular, a rule of strict liability applies to data processors/controllers in Greece and Germany (but only with regard to public data processors/controllers). Thus, responsibility is not dependent either on intent or negligence but simply follows from the existence of damage caused by a breach of the legislation. In Belgium it is reported that some courts may award damages following an expedited procedure before the president of the court of first instance. In Sweden, the Ministry of Justice may award compensation without judicial proceedings for violations by governmental or administrative organs. In Hungary, judicial procedures relating to data protection are not subject to court levies and duties and a rule similar to that of strict liability applies for the purposes of assessing the responsibility of the data controller/processor.

The procedural and substantive quantification of the damages to be awarded against the data processors/controllers liable for violating personal data rights varies in the Member States on the basis of the legislation and judicial practice concerning civil liability, and as a consequence cannot be analyzed within the context of this comparative report. The range of compensation payments awarded in data protection cases, moreover, is unknown in most Member States (Hungary, Sweden, Slovenia, Romania, Czech Republic, United Kingdom, Portugal, Poland, Netherlands, Malta, Luxembourg, Lithuania, Latvia, Italy, Ireland, Greece, Germany, France, Finland, Estonia, Denmark, Cyprus, Bulgaria, Belgium, and Austria). It is worth underlining, however, that in the legislation or in the judicial practice of a number of Member States (Italy, Slovenia, Germany, Greece, United Kingdom, Lithuania, Sweden, and Hungary) damages for intangible harm, such as distress, can also be awarded, either as such or together with damages for material loss.

4.3.4. Specialised data protection legislation in the context of the employment relationship

The necessity to ensure respect for the fundamental rights and dignity of the data subject is particularly pressing in the context of employer-employee relationships. On the one hand the protection of the privacy and of the personal data of employees is essential and a pre-requisite guaranteeing the fundamental right to participate in trade unions and to collective action. On the other hand, some of the most advanced technologies for monitoring and controlling the behaviour of individuals (such as camera surveillance, and remote e-mail control) are used predominantly in working life. As such, Member States should adopt additional legislation addressing data protection in the context of employment relationships in order to compensate for the inherent inequality of the parties to the employment contract by requiring stricter obligations for the employer to comply with data protection law.

While the Data Protection Directive, in Article 8(1) prohibits the processing of personal data revealing trade-union membership, a number of Member States (Italy, Hungary, Spain, Slovenia, Slovakia, Czech Republic, Portugal, Poland, Netherlands, Luxembourg, Latvia, Ireland, Greece, Finland, Belgium) have also introduced special provisions (either through employment legislation or in general data protection laws) to guarantee a higher standard of compliance with the right to privacy and personal data in the context of the employment relationship. These provisions specify a role for the Data Protection Authorities, which are authorized to draw up general regulations and guidelines, especially for private companies. Trade unions, then, besides providing consultation to the workers in questions regarding data protection, are often directly involved both beforehand in negotiating agreements with employers to establish a personnel records system and subsequently in monitoring compliance therewith.

Various deficiencies are, nonetheless, evident concerning data protection in the context of employment. To begin with, in several Member States (Sweden, Romania, United Kingdom, Bulgaria, Malta, Lithuania, Cyprus, France, Estonia, Denmark, Austria and Germany concerning private employment) special legislation to enhance the protection of employees is still lacking. Moreover, even where such legislation does exist, concerns arise out of the lack of a monitoring role for trade unions (e.g. Czech Republic, Latvia, Ireland), the discretionary powers of the employer to decide the goal of processing of personal data (e.g. Poland), the exemption for small companies from compliance with strict standards for data processing in the context of employment (e.g. Netherlands). Finally, in other countries (e.g. Finland), while protection of personal data in the context of the employment relationship has been satisfactory to date, recent legislative reforms are pending that would significantly lower the existing standards by allowing employers to monitor, under certain conditions, the addresses of e-mails sent and received by employees, as well as the type of attachments linked to messages, but not the content of the message itself.[85] According to the Finnish Bill, companies will be given a right to process identification data in their communications networks to detect, prevent and investigate violations of business secrets, unauthorised use, espionage as well as certain other crimes.

4.4. Rights-Awareness

In this sub-section results from Eurobarometer surveys and other studies/surveys carried out in the Member States will be presented to provide an overview of rights-awareness among

85 See, Finnish Government Bill HE 48/2008 vp.

the public with regard to data protection. Further, links will be examined between rights-awareness and the following:

- data protection authorities, their powers, remit, resources and activities
- practices indicating compliance with data protection law
- practices regarding sanctions, compensation and legal consequences in data protection cases

In section 5.1.4 below, deficiencies related to rights awareness will be discussed, and in section 6.3 good practices related to rights-awareness will be identified.

In February 2008, two Flash Eurobarometer surveys were published: No 225 – "Data Protection in the European Union: Citizens' perceptions"[86] and No 226 – "Data Protection in the European Union: Data controllers' perceptions".[87]

The topics of the first survey included: the public's general feelings and concerns about data privacy; the trust that they placed in different types of organisations that held their personal data; awareness of their data protection rights and of the national protection authorities; perceived security of data transmission over the Internet and the usage of tools that improved the data security; and attitudes on the restriction of their data protection rights in the light of international terrorism. The survey interviewed 27,000 respondents in the EU-27 (1,000 interviews per country) mainly through telephone interviews using fixed-line telephone numbers (however, in nine Member States the fixed-line telephone coverage was deemed inadequate, and so the sample consists of a mix of telephone and face-to-face interviews).

The survey reached the following findings:

- A majority of respondents across EU said that they were very or fairly concerned about how their personal data is handled. However, the level of concern is the same as what was found in an earlier Eurobarometer survey in 1991.
- The respondents had the highest confidence in medical services, doctors and public institutions in protecting personal data.
- The majority of respondents questioned whether the national legislation in their countries is able to cope with the use of personal information on the Internet.
- While most respondents seemed to be aware of their rights regarding the use of personal data and the existence of relevant legislation, on average only 28% of the respondents in the EU-27 were aware of the existence of a national data protection authority.

The task of the second survey was to measure perceptions about data protection among data controllers in the 27 EU Member States. The topics of that survey included perceptions about national data protection legislation; in-house practices relating to data protection and personal data transfer; recent experiences with privacy policy and data protection; the future of the legal framework on data protection; and data protection in the light of international terrorism.

This survey made the following findings:

- A majority of people who are responsible for data protection issues within their company said that they were very or somewhat familiar with the provisions of the national data protection law (56%).
- An equal share of the respondents (56%) considered that the national data protection laws offered citizens medium-level protection, while 28% described the level of protection as 'high' and 11% as 'low'.
- 50% of the respondents were of the opinion that existing legislation is rather unsuited or not suited at all to cope with the increasing amount of personal information that is being exchanged.
- An overwhelming majority (91%) considered the requirements of the data protection law as necessary. One third of the respondents (35%) said that, in some respects, the requirements are too strict.
- Opinions were divided over the adequacy of harmonisation of national laws to allow for free movement of personal data and the existence of differences in the way Member States interpret data protection laws across the EU (on both accounts, a large number of respondents did not have a clear opinion).
- Thirteen percent of interviewees in the EU-27 said that they were in regular contact with the national data protection authority – however, the results ranged from 41% of the respondents in Italy to 1% in Austria.
- The most often-quoted reason for contacting the national data protection authority was asking for guidance (60% of respondents who were in regular contact with the data protection authority gave this reason) or making a notification (56%).
- In assessing the statistical data which are available from the Member States, one has to note at the outset that national surveys are available only in 12 of the 27 Member States. These surveys have in some instances been commissioned by the national data protection authorities. The questions posed, the number of respondents, the methodology, the sampling and the final results are diverse and do not always allow for linking the results to the issues covered by this comparative study.

National surveys on rights awareness are available for some Member States (Sweden, Denmark, Finland, France, Austria, Spain, Ireland, Latvia, Netherlands, Slovenia, Hungary, Slovakia, United Kingdom) but not for the remainder (Luxembourg, Lithuania, Bulgaria, Germany, Czech Republic, Italy, Malta, Poland, Romania, Cyprus, Estonia, Greece, Belgium, Portugal).

There are regular public surveys concerning the protection of personal data in Slovakia. Their outcomes are reflected in the

86 Data Protection in the European Union: Citizens' perceptions. Flash Eurobarometer No 225 (http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf) (21.02.2009).

87 Data Protection in the European Union: Data controllers' perceptions. Flash Eurobarometer No 226 (http://ec.europa.eu/public_opinion/flash/fl_226_en.pdf) (21.02.2009).

reports issued by the national data protection authority. Two of the surveys (conducted in 2005[88] and 2007[89]) are published on its web site.[90] Both surveys consist of a nationally representative random sample of respondents of at least 18 years of age (in the 2005 survey the net sample size was 1,283 respondents, and in the 2007 survey 1,131 respondents). Based on the findings of the 2007 survey, 51% of the respondents declared their awareness concerning the right to data protection and almost 50% of them recognised the Office for Personal Data Protection as the relevant national authority (which is 5% higher than in the previous survey of 2005). Based on the outcomes of the surveys, it can be stated that the public continues to lack a full appreciation of the issues surrounding the protection of personal data and that these are not debated broadly.

In Latvia, two surveys were conducted in 2003 and 2005 (both were based on a stratified random sample of approximately 1,000 respondents permanently resident in Latvia). The results which are relevant to the present comparative study are as follows: 29.5% (23.3% in 2003) were aware about the existence of the national data protection authority; 19.5% of respondents (14.5% in 2003) reported having been in a situation where their data have been processed incorrectly, thus allegedly creating financial or moral damages; 13.5% of respondents (6.4% in 2003) report having faced a situation where they have been requested to provide more data about themselves than necessary; 22.9% of respondents have tried to obtain information about themselves from institutions or companies. Most of the latter (66.2%) were successful in doing so, although 32.5% were refused the information. The results of the survey show that awareness about data protection should be raised among State institutions, as well as for the public in general.

In Sweden, the national Data Protection Authority carries out research on the public and private sectors, as well as groups in society, on a regular basis. Three recent studies are available. The first relates to provincial health authorities' levels of awareness of data protection rules relating to accessibility to patients' data.[91] The second study analysed the questionnaires sent to 103 companies and public authorities, chosen randomly, regarding employers' attitudes towards employees use of the Internet and e-mail and the monitoring that exists by means of processing of biometric data and surveillance cameras.[92] The third study on awareness of, and attitudes towards, data protection law and rights focused on young people aged 14-18 years (533 respondents, sampling with quotas for selected respondent groups), who completed an on-line questionnaire.[93] The results of these surveys have neither been presented nor analysed in the national studies and therefore no comment may be made on them.

In Denmark two studies are available. A recent study emerging from the project *Privacy enhancing shaping of security research and Technology*, conducted by Privacy and Security Technology (PRISE) identifies the need for a public debate on questions about implementing new security technologies. A second one, which is a survey from 2005 on CCTV-surveillance by *Det Kriminalpræventive Råd* [the Council for the Prevention of Crime] based on interviews with 994 respondents, finds that "generally the Danes are positive toward TV-surveillance. Women seem to be more concerned with criminality than men. Citizens with a higher level of education seem to be more concerned with the interference with privacy".[94] In general, the survey suggests that the Danish population does not particularly worry about the issue of privacy. The Danish population has in general a fundamental trust in the Government's and the authorities' handling of data protection and maintains that the issue of crime prevention and security is more important than the intangible and abstract notion of privacy.

The national Data Protection Authority of Ireland conducted a survey in 2008 (a follow-up to similar research carried out in 1997, 2002 and 2005), with a sample of 1,000 respondents who were interviewed face-to-face as a part of an omnibus study.[95] One of the key findings of the survey was that almost two thirds of the population (65%) believe they have experienced some type of invasion of privacy – most often quoted categories dealt with receiving unsolicited commercial messages.[96] Out of a range of issues a good health service (mentioned by 89% of the respondents) and crime prevention (87%) were seen as most important affecting the respondents, followed by privacy of personal information (84%). While half of the respondents felt that adequate controls were in place both in the public and private sectors to prevent employers from accessing personal information records for inappropriate purposes, approximately one in five had doubts about the effectiveness of such controls. Respondents attach the highest levels of importance to medical records, financial history and credit card details in terms of keeping this information private. Fifty-eight percent of respondents were aware of the national Data Protection Authority. The national DPA stated that the results of the survey would be used to shape the future work of his Office.[97]

In France, the Commission Nationale de l'Informatique et des Libertés (CNIL) commissions survey research on an annual basis to monitor people's awareness of the organisation and of their rights. These surveys use a representative sample of 1,000 respondents of at least 18 years of age. According to this survey, in 2007 61% of French people think that

88 http://www.dataprotection.gov.sk/buxus/docs/sprava_5_2005_prieskum_vm1.pdf (23.01.2009).
89 http://www.dataprotection.gov.sk/buxus/docs/zaverecna_sprava_07.pdf (23.01.2009).
90 http://www.dataprotection.gov.sk/buxus/generate_page.php?page_id=421 (22.01.2009).
91 Summary in English available at Report 2005:1 http://www.datainspektionen.se/Documents/rapport-accessibility-to-patients-data.pdf (29.01. 2009).
92 Monitoring in Working Life Report 2005:3, English summary available at http://www.datainspektionen.se/-Documents/rapport-monworklife-summary.pdf (27.01.2009).
93 http://www.datainspektionen.se/Documents/rapport-ungdom-2009.pdf (27.01.2009).
94 TV-overvågning – Fakta om TV-overvågning i Danmark. Det Kriminalpræventive Råd, Februar 2005. Available in Dannish at: http://www.dkr.dk/ftp_files/WEBDOX/PDF/dkr_mat_083.pdf (03.02.2009).
95 Full survey available at http://www.dataprotection.ie/docs/Public_Awareness_Survey_2008/794.htm (10.01.09).
96 Report presenting the findings of survey available at http://www.dataprotection.ie/docs/Public_Awareness_Survey_2008_Report/821.htm (24.02.2010).
97 Press Release of 12.08.08, available at http://www.dataprotection.ie/viewdoc.asp?DocID=815 (10.01.09).

collecting data is a violation of their right to privacy, and they consequently desire more protection.[98] Moreover, 32% claimed to know about the national Data Protection Authority in a similar survey in June 2004, 37% in December 2005, 39% in December 2006, and 50 % in November 2007.[99] One person out of two knows about tasks that it performs. However, only 26% said that they felt sufficiently informed about their rights with regard to the protection of personal data, while 72% of the respondents felt they were not adequately informed.[100]

In July 2008, a survey based on face-to-face street interviews with 1,213 respondents (using respondent quotas) on the confidence of the population of Austria in data protection was published.[101] According to this, issues such as data protection or surveillance are to a large extent unknown among Austrians: 77% of the respondents admitted to being more or less oblivious with regard to such topics; 92% stated not knowing whether (personal) data are being collected about them and if so, by whom; 76% of respondents were of the opinion that the Austrian population was not sufficiently informed about data protection, the risks of data abuse or the legal conditions in question. Regarding video surveillance, 55% of the respondents declared that they were used to the fact that video cameras monitor and record events and the behaviour of practically every person, regarding it as a part of modern life, rather than a threat to fundamental rights. In another study, concerning video surveillance of public space (1,237 respondents, using the same methodology as in the above-mentioned study), up to 81% of the respondents declared that they accepted video cameras directed towards passers-by and 90% admitted that they had become accustomed to surveillance cameras being ever-present.[102]

Two studies are available for Spain. The first bears the title "Study on the Level of Compliance of Small and Medium Sized Spanish Companies with the Organic Law on Personal Data Protection and with the new Statutory Regulation".[103] It affirms that 96% of the small and medium size Spanish companies have files containing personal data, and 78% are in the medium of electronic files, so that all of them fall under the scope of data protection legislation (the results are based on telephone interviews with a stratified sample of 250 small and medium sized companies (companies with under 50 employees)). Small and medium size Spanish companies show a positive attitude towards data protection: 82% of the studied companies affirmed that they were aware of the need for compliance with the relevant legislation, whereas 79% confirmed their intention to assign economic and/or human resources to comply with the legislation on data protection. There is also an important study by the local Basque Agency on Personal Data Protection conducted in June 2008, which deals with the social perception of data protection in the País Vasco (based on a stratified random sample of 600 respondents, interviewed over the telephone).[104] This study states that 37% of the population of this Autonomous Community are very or quite concerned about how public bodies and private companies are using citizens' personal data.

Various surveys have investigated perceptions of privacy and privacy-awareness in the Netherlands.[105] In a 1989 survey, citizens seemed to be of the opinion that privacy is as important as good health care, a clean environment, and the fight against unemployment and crime.[106] A 1999 survey distinguished three groups of citizens: 1) citizens who think that information technology is necessary and who do not see a problem with regards to privacy (19%); 2) citizens who think that the increasing use of information technologies creates more privacy problems (35%); and 3) citizens who think that information technologies are a threat to privacy (47%).[107] A 2007 survey focusing on freedom and solidarity found that 51% of the respondents considered that the Dutch government sufficiently protects the fundamental right to privacy, while 43% thought the government should protect their privacy better (the results from the 2007 survey are based on a random sample of households from an Internet household panel, and the survey was administered through computer-assisted self-interviewing (CASI). Respondents were 13 years old or older, with a net sample size of 967 interviewees).[108] In January 2009, results were published of a survey commissioned by the national data protection authority (this is based on an on-line survey of 2,016 respondents). The report, *Nothing to hide but frightened nonetheless*, evaluates the attitude of Dutch citizens with regard to the collection and processing of their personal data.[109] In general most citizens are rather willing to disclose their personal data – however, this does not mean that citizens are unaware of their privacy. Most citizens are aware, but their willingness to provide data can better be seen as a result of inevitability and a resigned attitude than in terms of trust that the data are used in a correct manner. In particular in the group discussions, respondents showed themselves frightened when confronted with the risks of personal data processing. Nevertheless, altering practices was seen to be too burdensome a task. Control and transparency seemed important for the acceptance of data processing and citizens expressed interest in having overviews

98 CNIL, 25/01/2008, « 61% of French people believe that the creation of computerized data files infringes upon their right to privacy », in: http://www.cnil.fr (19.11.2008).
99 CNIL, *Annual Report 2007*, p. 39.
100 CNIL, *Annual Report 2007*, p. 39.
101 Vertrauen der ÖsterreicherInnen in den Datenschutz, available under: http://www.oekonsult.eu/datensicherheit2008.pdf (04.01.2009).
102 Big Brother. Gefahr oder Normalität, available under: http://www.oekonsult.at/bigBrother_gesamtergebnisse_final.pdf (15.01.2009).
103 *Estudio sobre el grado de adaptación de las Pequeñas y Medianas Empresas españolas a la Ley Orgánica de Protección de Datos y el nuevo Reglamento de Desarrollo*, Instituto Nacional de Tecnologías de la Comunicación [National Institute of Communication Technologies], July 2008, available at: http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Estudios_e_Informes_1/estudio_lopd_pymes (08.01.2009).
104 *La protección de datos personales*. This study is available at: http://www.avpd.euskadi.net/s04- 5249/es/contenidos/informacion/estudio/es_cuali/adjuntos/informe.pdf (08.01.2009).
105 See also Sjaak Nouwt (2005), *Privacy voor doe-het-zelvers*, The Hague: Sdu, ITeR Series Vol. 73. http://arno.uvt.nl/show.cgi?fid=41691 (27.01.2010).
106 Holvast, Jan, Henny van Dijk and Gerrit Jan Schep (1989), *Privacy Doorgelicht*, Den Haag: SWOKA.
107 Smink, G.C.J., A.M. Hamstra and H.M.L. van Dijk (1999), *Privacybeleving van burgers in de informatiemaatschappij*, Den Haag: Rathenau Instituut, Werkdocument 68.
108 Dieter Verhue, Harmen Binnema & Rogier van Kalmthout (2008), *Nationaal Vrijheidsonderzoek. Meting 2008. Opiniedeel*, April 2008, p. 36. http://www.4en5mei.nl/mmbase/attachments/158819/p4751_vrijheidsonderzoek_opiniedeel_v4_read_only.doc (27.01.2010).
109 J. Koffijberg et al. (2009), *Niets te verbergen en toch bang; Nederlandse burgers over het gebruik van hun gegevens in de glazen samenleving*, Amsterdam: Regioplan, publication number 1774. http://www.cbpweb.nl/downloads_rapporten/rap_2009_niets_te_verbergen_en_toch_bang.pdf (27.01.2010).

of their registered personal data on a regular basis. Furthermore, information on technological-societal developments is seen as important and helpful in the formation of privacy-aware attitudes. Finally, there is considerably more trust for the correct use and processing of personal data by the government than by private companies and institutions.

According to the Public Opinion Poll of Slovenia the national Data Protection Authority is ranked as the most trustworthy state institution.[110] No other surveys were available on matters related to this comparative study.

In Hungary, a survey on the awareness and knowledge of the constitution was conducted in 2005 (representative sample of 1,000 respondents).[111] Eight point one percent of the respondents believed that "under the current constitution the right to privacy cannot be exercised at all; according to 56.5% it can be exercised to a small degree; and according to 33.5% it can be exercised to the highest degree". As to the question whether or not the level of the protection of private life should be changed, 38.9% of the respondents were of the opinion that the level of protection was adequate, 58.3% called for a higher level of protection.[112] In 2008, a survey was commissioned by the Ombudspersons' Office on the recognition and appreciation of the ombudspersons.[113] According to the survey (sample of 1,000 respondents): the proportion of citizens actively knowing the ombudsmen had grown from 15% in 1998 to 32% in 2007; 59% of respondents knew about national DPA; 11% of the respondents were certain and another 28% believed they would seek a remedy from the ombudsmen in case their rights had been violated. In relation to public trust the ombudsmen ranked third among major public institutions with 52% of respondents saying that they trusted the ombudsmen.

The Information Commissioner's Office in the United Kingdom has used surveys in monitoring public awareness on data protection. The latest public awareness findings show a decrease of ten percentage points (from 49% in 2006 to 39 % in 2007) in the share of respondents who believe that existing laws provide sufficient protection for personal details. The survey in 2007 interviewed 1,223 respondents by telephone. The sample design used respondent quotas to ensure the representation of specific groups in terms of gender, age, ethnicity and other variables. Looking at surveys carried out from 2004 to 2007, the respondents' awareness of their right to see information (when prompted with the topic) has increased from 74% in 2004 to 90% saying it is their right to see information that organisations keep on them. Seventeen percent of the respondents had, in fact, exercised this right by making a request to an organisation to see their personal information. When the respondents were asked to evaluate a list of typical concerns that people might have regarding the handling of their personal data, in each case 83-94% of the respondents said they were very or fairly concerned. Most concern was attached to organisations passing or selling personal details to other organisations, and the security issues in storing personal details.[114]

Complementing the above research findings, an important finding from the Eurobarometer surveys is that the national authorities remain relatively unknown to most EU citizens. This can be seen as a fundamental problem and largely explains the lack of knowledge of the powers conferred on them. Accordingly, this knowledge deficit yields to lack of rights' awareness and lack of knowledge on data protection authorities' powers, remit, resources and activities.

The main source of information regarding rights-awareness – including awareness of practices indicating compliance with data protection law, and practices regarding sanctions, compensation and legal consequences – stem from surveys such as Eurobarometer. The survey conducted in Spain by the National Institute of Communication Technologies, as reported above, offers some indication in relation to awareness of duties of registration under national law. As mentioned above, 82% of the studied companies affirmed that they were aware of the need of comply with the relevant legislation, whereas 79% confirmed their intention to assign economic and/or human resources to comply with the legislation on data protection. These figures are encouraging if one considers that according to the Eurobarometer survey 56.1% of persons responsible for data protection issues within companies were somewhat familiar with the provisions of the data protection law, and 30.2% said they were not really familiar, while only 13.1% said that they were very familiar with the provisions.

110 http://www.ip-rs.si/index.php?id=272&tx_ttnews[tt_news]=621 (30.12.2008).

111 Conducted by Eötvös Károly Institute in cooperation with the Legal Sociology Department of Eötvös Lóránd University.

112 László Majtényi, *Az információs szabadságok. Adatvédelem és a közérdekű adatok nyilvánossága*. [The freedom of information. Data protection and access to public data], 2006, Budapest, Complex Kiadó. pp. 58-61.

113 Szonda Ipsos Media, Opinion and Market Research Institute, http://www.obh.hu/szonda_ipsos_OBH.doc (26.01.2009).

114 *Report on Information Commissioner's Office Annual Track 2007*, p. 7, para. 4.2. Available from: http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/ico_annual_track_2007_individuals_report.pdf (24.02.2010). Full details on the survey questions and responses are provided in the body of this report.

5. Analysis of deficiencies

This section of the report analyzes the main deficiencies emerging from the system of personal data protection at the EU and national level. It will focus firstly on the challenges surrounding Data Protection Authorities, compliance with relevant legislation, remedies, compensation and sanctions available against infringements of privacy rights, and rights awareness-raising activities. It will them move on to identify the main areas that are excluded or exempted from or otherwise not covered by the application of data protection laws.

5.1. Deficiencies in Data Protection Law

5.1.1. Data Protection Authorities

Several deficiencies can be identified in relation to the organization, functioning and practical operation of Data Protection Authorities. At a structural level, a major problem arises due to the lack of independence of several supervisory authorities. In a number of Member States (e.g. Lithuania, Latvia, Estonia, Ireland, United Kingdom) concerns arise as to the effective capability of the officers of DPAs to perform their task in complete autonomy. One of the main explanations for this deficiency relates to the procedure through which officers are nominated or appointed: where the Government holds exclusive power to select managerial staff, without the input, review or consent of the legislature, as noted above in section 3.1.1, the risk of effective subordination or marginalization of the controllers increases significantly. This could be addressed by reforming the nomination/appointment procedure. Another possible amendment to the Data Protection Directive could add greater specificity and detail to the requirement of independence (currently set out in Article 28(1)).

At the functional level understaffing and the lack of adequate financial resources among several supervisory bodies constitutes a significant problem. In many Member States, DPAs are not in a position to carry out the entirety of their tasks because of the limited economic and human resources available to them. This is the case in Austria, Bulgaria, Romania, Cyprus, France, Greece, Italy, Latvia, Netherlands, Portugal and Slovakia. For supervisory bodies, financial autonomy and a specialized professional staff are not only essential for ensuring the effective protection of personal data rights but also a precondition for true independence from the will of the government. Legislative reforms could be directed towards increasing the budget control and human resources management of the DPAs (for instance, by allowing them to hire specialized personnel directly).

At the operative level the limited powers of several supervisory agencies is a cause for concern. In certain Member States, Data Protection Authorities are not endowed with the full range of powers to conduct investigations, effect interventions during data processing operations, offer legal advice and engage in legal proceeding as set out in Articles 28(2), (3) and (4) of the Data Protection Directive. In Austria, Hungary and Poland the supervisory bodies cannot enforce their decisions warning the data processor/controller to end its unlawful conduct. In Belgium and in Germany, it cannot order the blocking, erasure or destruction of data, nor can it impose a temporary or definitive ban on processing. In the United Kingdom and France, it cannot enter premises where personal data are processed without first obtaining a judicial warrant. In many countries (e.g. Ireland, Poland, Czech Republic, Lithuania, Hungary, Malta, Italy, France, Romania, Slovenia, United Kingdom, Austria, Greece), in turn, supervisory bodies are only randomly consulted by the legislature when drafting statutes that may affect privacy and data protection issues because there is no concrete requirement for the legislature to do so. Besides being a violation of EU law, the incomplete implementation of the requirements of the Data Protection Directive constitutes a significant deficiency in the national system of personal data protection that risk jeopardizing the effectiveness of the system. Since EU law appears to be particularly clear with regard to the power of the Data Protection Authorities, amendments should be made in national legislation when needed to bring domestic rules in line with the requirements set at the EU level.

5.1.2. Compliance

Various deficiencies emerge when taking into account the level of effective compliance with relevant data protection legislation, especially with regard to the duty of registration by public and private actors engaged in data processing operations. While the assessment of effective compliance with data protection legislation is difficult in a number of Member States due to the lack of reliable or precise information, it seems that in various countries (e.g. Bulgaria, Denmark, Latvia, Netherlands, Portugal, Slovakia, Romania), a gap exists between the protection of the right to privacy in theory, which may formally conform to the requirements of EU and international law, and its protection in the law in practice. Thus, for instance, compliance with data protection legislation is surprisingly low among public institutions in Estonia and Romania. On the other hand, in most countries, the absence of clear notions (or shared interpretations) of the relevant concepts (such as 'personal data', 'file', and 'processing') create uncertainties over what activities fall under the relevant laws on personal data. The "Article 29 Working Party" plays a crucial role in developing a shared interpretation of these vague terms, but this process also depends on the acceptance and implementation of these interpretations in the Member States. Complexities and inconsistencies may also be produced by the dispersion of the legislation concerning data protection into different sector-specific legislative acts, as has happened in Finland and Greece. From this point of view, hence, whereas better enforcement in practice of data protection norms by the interested parties could be sufficient to address the first problem, additional

legislation, replacing vague provisions and simplifying the legal framework, would be helpful for the second one. Most deficiencies relating to complexities and vagueness of the data protection legislation, to a large extent, are related to the wording of the Data Protection Directive: solutions in this respect therefore are best to be found at the EU level.

A major problem is the widespread disregard, documented in various Member States (notably the United Kingdom), of the basic duty to register with the Personal Data Authority prior to engaging in data processing operations. A recurrent example is that of video surveillance cameras: in Austria, Bulgaria, France, Lithuania, Czech Republic and Sweden the vast majority of surveillance cameras are not registered in practice and thus not under the supervision and control of national supervisory bodies. Another major area of concern is the Internet (e.g. Spain and Slovenia). Often, non-compliance with the registration duties by data processors/controllers is caused by the lack of adequate knowledge of the legislation rather conscious disregard. This deficiency poses a particular challenge to the effectiveness of data protection legislation. Notwithstanding the difficulties that the law faces when trying to keep up with new technological developments, additional legislation introducing or improving the legislation to regulate technologies that have an impact on personal data rights (such as camera surveillance, wiretapping, cell samples or DNA code retention), therefore seem to be urgently needed (also to avoid discrimination in the protection of data rights on the basis of economic status, as has worryingly happened in the Czech Republic).[115]

5.1.3. Sanctions, Compensation and Legal Consequences

Certain problems arise out of the domestic systems of remedies, sanctions and compensation as well as the application of data protection rules in the context of employment. Deficiencies in the sanctions that may be imposed by the Data Protection Authority emerged in various countries, either because the fines had limited dissuasive force and/or were imposed infrequently or because supervisory bodies has simply not developed a practice of imposing them (Poland, Austria, United Kingdom, Finland, Hungary, Lithuania, Denmark, Belgium). The lack of a legal obligation for data controllers/processors to report data breaches in some Member States (for example in Ireland) may then aggravate the weakness of the enforcement system. In some countries (e.g. Germany, Latvia, Netherlands, Poland, United Kingdom, Austria, France, Hungary) then, prosecutions and sanctions for violations of data protection law are extremely limited. With regard to damages in various Member States (e.g. Finland, Ireland, Netherlands, United Kingdom, Cyprus, Malta, Poland, Latvia, Estonia, and Sweden as far as compensation from private entities is concerned) the national legal system effectively rules out the possibility of seeking compensation for the violation of data protection rights, due to the combination of several factors such as burden of proof, difficulties relating to quantification of the damage and infrequent support from the supervisory bodies, which are mainly engaged in promotional activities. While the use of *ex ante* "soft" methods can be noted as a positive practice in contributing to securing compliance, it is essential that Member States also provide for "hard law" instruments which allow those in violation of privacy related rights to be punished and obliged to compensate victims. Legislative reforms, – essentially at the national level, may play a relevant role here, by providing more effective and comprehensive legal remedies in the form of redress for violations. At the same time, raising awareness of the importance of data protection rights among data subjects as well as among judges and prosecutors, may allow for better enforcement of the already existing provisions for punishing violations of data protection law.

Many Member States (Belgium, Sweden, Romania, United Kingdom, Bulgaria, Malta, Lithuania, Cyprus, France, Estonia, Denmark, and Austria) still lack legislation adapting data protection rules specifically to the employment relationship, failing to acknowledge the necessity to adopt special data protection provisions to regulate the use of personal data in the employment sector. As a consequence, violations of personal rights of individuals have been highlighted in some countries (e.g. in Cyprus, Sweden and Germany in the private sector) because of secret (video) surveillance of workers at their work place. In other Member States (e.g. Finland), on the contrary, while the legal framework has been satisfactory to date, recent legislative amendments have actually weakened protection in the context of employment.[116] The EU, founded on the principles of a social market economy, attributes great importance to labour, and the free movement of workers represents a fundamental liberty enshrined in the EU Treaties. Since divergences between the legislation of Member States may adversely affect the functioning of the internal market, intervention in this sector by the EU to establish a minimum standard of personal data protection in the field of employment would be highly beneficial. At the same time as respecting the principle of subsidiarity this is essential to ensure that the fundamental rights of workers, as recognized in the common constitutional traditions of the Member States and in relevant EU legislation, receive full protection.

5.1.4. Rights Awareness

In section 4.4, above, a comparative overview relating to rights-awareness was presented, and in section 6.3, below, good practices relating to rights-awareness will be identified. The involvement of Data Protection Authorities in the activity of rights awareness-raising among various stakeholders has been generally positive.

Few negative examples are however identifiable where Data Protection Authorities have not dedicated themselves to awareness-raising (e.g. Estonia, Romania). Thus, in a number of Member States (e.g. Lithuania, Bulgaria, Slovakia), supervisory bodies have not yet set up user-friendly and/or comprehensive updated web sites where all information relating to data

115 For more information about the so called 'OpenCard' case: http://opencard.praha.eu/jnp/en/home/index.html (in English) (last accessed on 23.01.2009).

116 http://www.hs.fi/english/article/Lex+Nokia+passes+in+Parliament+-+government+party+ranks+split/1135244038215 (09.03.2009).

protection may be accessed by the general public and where opinions and regulations drafted by the Data Protection Authority are readily available. Furthermore, concerns as to the degree of publicity and transparency of activities performed by the Data Protection Authority have been raised in some countries (e.g. Bulgaria, Malta) especially when the supervisory authority negotiates amicable resolutions of disputes with violators of data protection law, without making this public (e.g. United Kingdom). Finally, in several Member States (e.g. Austria, Greece), while the performance of the supervisory body is generally satisfactory, it may take an unreasonably long time for individuals to obtain information, often because DPAs lack sufficient resources to answer all the requests received by data subjects swiftly. As such, it may be doubted that new legislation, be it at the EU or national level, could improve the current situation. Rather, national Data Protection Authorities may need to reorganize their work to provide prompt support to data subjects. Changes in attitudes are then needed to increase the publicity of their work and to raise awareness about data protection rights among the interested stakeholders. Data Protection Authorities should acknowledge the importance of their practical role in raising rights awareness and may easily draw examples from the good practice of other European supervisory bodies to tackle those deficiencies.

Even more problematic, in a few Member States (e.g. United Kingdom) the Data Protection Authorities have made it clear that it is not their task to ensure that national data protection legislation is interpreted in a manner consistent with the EU and international standards of personal data protection (even if, to a large extent, national legislation constitutes the domestic implementation of relevant EU and international provision). Indeed the work of the national Data Protection Authorities is essential in creating a common understanding of the principles of data protection rights. Their (spontaneous) convergence therefore should be praised as a good practice not only to ensure consistency between the various legal systems but also to define the appropriate standard of protection of privacy related rights. The power of legislation here is limited: changes in the approaches of national supervisory authorities need to take place at a cultural level rather than a political/legislative level.

5.2. Problematic areas regarding data protection

This subsection will identify the main problem areas that are excluded or exempted from, or are otherwise not effectively covered by, the application of data protection law. In this regard, there are three broad categories which must be mentioned: the exclusion from the data protection regime of the activities related to national security (such as intelligence services, military activities); protection of data relating to an individual's health; and video surveillance.

5.2.1. Data protection in relation to national security

Article 13(1) of the Data Protection Directive (relating to exemptions and restrictions) stipulates that "Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1), 10, 11(1), 12 and 21 when such a restriction constitutes a necessary measure to safeguard: (a) national security; (b) defence; (c) public security".

The exceptions listed in Article 13(1)(a)-(c) of the Data Protection Directive are interconnected. In various Member States (Luxembourg, Denmark, Ireland, Romania, Greece and Portugal) they are identified as the principal areas excluded from the ambit of data protection law. This is anticipated due to the wording of Article 13 of the Data Protection Directive. However, there are three important issues to be considered in relation to the interpretation of this provision.

Firstly, the wording allows for "restriction" in relation to security issues. This is not to be construed as equivalent to "exemption" from the scope of application of the Directive. A grammatical interpretation is not the only reason for asserting that the scope of activities of various branches of the executive do come within the scope of the Directive.

Secondly, the first preambular recital to the Directive sets the European Convention on Human Rights as the backdrop of the processing to personal data. Further, the third preambular recital explicitly states that the fundamental rights of individuals should be safeguarded. As already indicated in other parts of this comparative study the protection of human rights and the integrity of the individual are fundamental conditions in the area of data protection.[117]

Thirdly, the essence of the overall edifice of the Directive is not to carve out an unsupervised field in which States may operate outside the requirements of the law. On the contrary, when confronted with national security issues what is called for is a proportionality test, i.e. balancing fundamental rights against other interests and not simply overriding the former.

Fourthly, the Directive needs to be interpreted in line with Article 8 of the EU Charter of Fundamental Rights which, according to the new Article 6 of the Treaty of European Union has "the same legal value as the Treaties". Article 8 may only be limited under the conditions set in Article 52 of the Charter. Article 13(1) of the Data Protection Directive provides for broad exemptions and restrictions concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law. There is lack of clarity regarding the extent of these exemptions and restrictions. In various Member States, these areas are altogether excluded from the protection of data protection law. This leaves a considerably large area unregulated with potentially serious consequences for fundamental rights protection. According to Article 52 of the Charter, any limitation of the rights and

117 See above section 2.1 on the fundamental standards of data protection at the level of the Council of Europe.

freedoms recognised by the Charter "must be provided by law and respect the essence of those rights and freedoms".

It is for these reasons that the option of national legislatures to provide blanket exemptions for certain branches of the executive (such as intelligence services or the ministry of defence) does not fit with the normative framework of the Data Protection Directive.

5.2.2. Data protection relating to an individual's health

Concerns have been raised in several countries (e.g. Sweden, Bulgaria and Slovenia) over the framework of protection for health-related data. Article 8(2) of the Data Protection Directive obliges Member States to prohibit the processing of data concerning individuals' health. Article 8(3) provides for an exception to this "where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy".

Allowing all health workers access to all patient data increases efficiency, and helps in cases of medical emergencies, when time is of the essence. However, it also means that more people have access to sensitive data (meaning a greater infringement of personal integrity), as well as increasing the risks of leaking of sensitive data. The accessibility can be decided on the basis of, for example, position, medical specialty and established co-operation. Divisions that regularly co-operate because they belong to the same organisation normally should be able to get access to one another's information, assuming that confidentiality is ensured. There must also be efficient tools for follow-up and traceability. The identification of the user must comply with security restrictions.

Providing a straight-jacket solution to this, through an EU instrument, may lead to severe repercussions in the health care sector in Member States. It seems more plausible to ensure that the regulations for health care professionals relating to confidentiality and privacy are in line with the objectives of the Directive, in order to ensure the effective protection of the individual's rights without at the same time compromising his or her right to health.[118]

In some Member States legislatures have recently drafted legislation in the field. For example, in Belgium a bill was proposed concerning the organisation of a platform called 'e-health',[119] through which electronic exchange of medical and other data between health care professionals and institutions will take place, in order to simplify and improve the health care system. The system also allows for the transmission of electronic prescriptions of pharmaceutical products. Since, however, doctors, hospitals, health insurance funds and some social security institutions will have access there are concerns that the privacy of patients will not be sufficiently protected. In drafting national legislation with regard to the sensitive area of health, citizens' rights should be carefully balanced.

5.2.3. Data protection in relation to video surveillance

As noted above, video surveillance has been singled out as an area of possible concern. In Austria the vast majority of surveillance cameras are not registered at all and thus not under the supervision and control of the national data protection authority. In Germany there have been reported cases of secret video surveillance of workers at their places of work. Also, the right to personal self-determination is frequently violated if data subjects are insufficiently informed about the use and/or processing of their data. A prominent example of video surveillance at work places is the case of surveillance of the administrators of the National Competition Authority of Cyprus by the head of the Authority, which eventually led to his resignation. It is reminded that in Greece the national data protection authority was denied access to police premises where data processing was taking place. In the United Kingdom, there are few restrictions on the use of public area CCTV cameras, and there are more CCTV cameras in this Member State than anywhere else in the world.[120]

The Data Protection Directive fails to offer detailed guidance in relation to video surveillance. Recital 14 of the preamble reads as follows: "Whereas, given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data." It may be understood that such data may fall largely within the definition of 'personal data', as provided by Article 2 of the Data Protection Directive and thus an individual may avail themselves of the protection provided in EU law.

However, Article 33 of the Data Protection Directive provides that: "The Commission shall examine, in particular, the application of this Directive to the data processing of sound and image data relating to natural persons and shall submit any appropriate proposals which prove to be necessary, taking account of developments in information technology and in the light of the state of progress in the information society". It

118 See also working document WP131 of Article 29 Working Party dated 15 February 2007: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_en.pdf (24.02.2010).

119 Belgium/Commissie voor de bescherming van de persoonlijke levenssfeer, Advies nr. 33/2008 (24.09.2008), available at www.privacycommission.be/nl/docs/Commission/2008/advies_33_2008.pdf (24.01.2009); Commission de la protection de la vie privée, Avis no. 33/2008 (24.09.2008), available at www.privacycommission.be/fr/docs/Commission/2008/avis_33_2008.pdf (24.01.2009) (French).

120 http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1806.htm#a41, at para 213 (06.10.2009).

is evident from this reference that the EU places a particular interest in video surveillance. It should be noted that the Article 29 Working Party has provided some guidance in this respect.[121] Keeping in mind the intrinsic technical particularities of sound and image data, as well as the wide-ranging potential impact on individuals' rights, a separate EU legislative measure ought to be considered in the future.

The legislature of some countries has recently been involved in this field, but it may be doubted whether the road undertaken is appropriate. Two laws related to video surveillance were passed in Denmark in June 2007. The first one gives private enterprises extended powers to perform surveillance in areas related to their property. There is no longer a duty to notify the data protection authority prior to installing surveillance equipment. The second gives the intelligence services of the police increased powers to exchange information with the defence intelligence services and to collect information from other public authorities, e.g. hospitals, schools, libraries, social services etc. without a court order. It also gives the police increased powers to demand from public offices and private parties that they install and conduct video surveillance.

The issue of data protection in the context of video surveillance is part of a larger debate: the need to update data protection legislation to keep up with technological developments. Recent and ongoing technological developments (including "cloud" and "autonomic" computing, ICT implants in the human body, nanotechnologies, brain/machine interfaces) pose new challenges that urgently need to be addressed. The implications of the Internet and new social networking technologies like "facebook" and "twitter" for the protection of fundamental personal data rights also need to be duly taken into consideration: the importance of the individual's "digital identity" can hardly be overstated.[122] Nowadays, it constitutes an essential component of one's overall identity and personality. As such it deserves a level of protection equivalent to other "traditional" facets of personality. Digital identity is inextricably linked to an individual's "digital existence". In the wide cyberspace an individual may establish his or her presence and perform activities that were previously conceived only in the 'real' public domain. Special attention needs to be paid in this respect to the work of the Internet Governance Forum and the emerging "Internet Bill of Rights", as referred to in a resolution on strengthening security and fundamental rights on the internet of the European Parliament.[123]

121 See working document WP 67 from 25 November 2002: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp67_en.pdf (24.02.2010); opinion 4/2004, WP 89 from 11 February 2004, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp89_en.pdf (24.02.2010).

122 Report with a proposal for a European Parliament recommendation to the Council on strengthening security and fundamental freedoms on the Internet (2008/2160(INI)), Committee on Civil Liberties, Justice and Home Affairs, http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/a6-0103_2009_/a6-0103_2009_en.pdf (07.03.2009).

123 T6-0194/2009 dated 26 March 2009.

6. Good practices

This section of the report will provide a brief account of the most relevant good practices concerning data protection in the EU Member States, highlighting positive national examples with regard to Data Protection Authorities, compliance, remedies and right-awareness. The identification of examples of 'good practice' acknowledges the value of a practice and contributes to supporting a culture of continuous progress. However the identification as 'good practice' does not imply that the respective practice has been directly scrutinised in depth by the Agency

6.1. Data Protection Authorities

With regard to national Data Protection Authorities the good practices have either to do with the structure of the supervisory bodies or with their work. On the one hand, several Member States have endowed their national Data Protection Authorities with specific powers and ensured them a high degree of independence. On the other hand, Data Protection Authorities have established cooperation with three categories of stakeholders: state institutions, NGOs active in this field, and Data Protection Authorities of other Member States.

The independence of the Data Protection Authorities is an essential factor in ensuring a high level of data protection. From this point of view, therefore, structural measures such as the attribution of a distinct legal personality to the supervisory body (as has been done in Spain and Malta) or the constitutional codification of its powers and remit (as has happened in the Constitution of Portugal and Greece) constitute positive examples to enhance the independence of supervisory bodies. Even if election by the legislature does not necessarily ensure the independence of the officers of the supervisory body, procedures requiring consensus between the majority and the opposition (as in Greece) should be regarded as a good practice. Another good practice ensuring a high level of autonomy for the Data Protection Authority is provided in Slovenia where it enjoys *locus standi* to challenge the constitutionality of legislation in front of the Constitutional Court.

The power of the Data Protection Authorities to engage actively in the preparation of codes of conduct represents a positive practice. Involvement in drafting codes of conduct in data protection matters not only enhances overall protection for citizens, but also contributes to increasing the visibility of national authorities in society and DPAs should engage in this proactively. In Ireland, in particular, domestic legislation gives the national data protection authority the power to propose and prepare codes, which if approved by the legislature will have binding legal effect.[124]

Cooperation and regular communication between different public bodies and DPAs has the potential to ensure the smoother running of the data protection system as a whole. In Germany, for example, extensive training programmes are run in the form of a data protection academy which has developed comprehensive and systematic training programmes for all areas of administration.

Close cooperation and communication with NGOs which are active in the field of data protection provides several advantages. Firstly, NGOs are in a position to signal systematic and/or flagrant violations of data protection laws to national authorities and civil society. Thus an additional, informal supervisory body is in place. In certain instances they effectively contribute to a comprehensive monitoring of the data protection field. Secondly, NGOs provide for a 'bottom-up' channel of communication, providing active citizens with the opportunity to propose amendments to the legal framework. From this point of view, the national Data Protection Authority in Hungary has reportedly been open to assist and cooperate with NGOs. For instance, in 2000 it reviewed the data protection plan of a research project on Roma rights conducted by the Hungarian Helsinki Committee, and in 2004 the staff of the authority, in cooperation with the Hungarian Civil Liberties Union, tested several public health premises to ascertain whether HIV tests were in fact facilitated anonymously and free of charge as announced. On the basis of the findings a recommendation was issued.[125]

Finally, cooperation and constant communication among Data Protection Authorities of other States (EU and non-EU) is also useful. At the EU level this is achieved mainly through the Working Party established by Article 29 of the Data Protection Directive. This forum provides for the necessary institutional environment for DPAs to harmonise the application of their respective laws. Bilateral or multilateral cooperation, on the basis of regional or linguistic affinity, should also be encouraged both within the EU and with non-EU countries. A good example here is that of Portugal where an informal annual, meeting with its Spanish counterpart is held to discuss the important developments in data protection.

6.2. Compliance

With regard to compliance, good practices arise out of the enhanced capacities of the Data Protection Authorities to detect violations and prosecute those who have infringed the law. An interesting feature of the good practices existing in Italy is the cooperation between the national agency and police bodies, through the medium of an *ad hoc* memorandum with the Financial Police. The same is valid for Romania where the national Data Protection Authority signed cooperation agreements with public institutions such as the National Authority for Consumer Protection, the General Inspectorate

124 Ireland Data Protection Act (1988-2003), Section 13.

125 http://beszelo.c3.hu/03/11/04zadori.htm (28.01.2009); http://abiweb.obh.hu/dpc/index.php?menu=reports/2004/III/2&dok=reports/2004/27 (28.01.2009).

of the Romanian Police, the Financial Guard, the Ministry of Communications and Information Technology, and the National Office of Trade Registry.

An interesting facet of the Dutch system is the obligation of the government, within five years from the entry into force of the national law, to present a report to the Dutch parliament on the effectiveness and effects of the law in practice. This evaluation of the Dutch DPA has been conducted in two stages. The first stage of the evaluation, a study of secondary sources, was concluded in 2007 and presented in the report *First Phase of the Evaluation of the Personal Data Protection Act* ("Eerste fase evaluatie Wet bescherming persoonsgegevens").[126] The second stage of the evaluation consists of case studies and interviews, concerning the effectiveness of the Personal Data Protection Act in practice. The report was published in February 2009.[127]

6.3. Rights-Awareness

In section 4.4 above, a comparative overview related to rights awareness was presented, and in section 5.1.4 deficiencies related to rights awareness were discussed. A wide array of good practice has emerged with regard to the activities of rights awareness-raising performed by national Data Protection Authorities. To begin with, many national agencies have set up user-friendly web sites where relevant information concerning data protection may be found. Often these web sites are available in more than one language. A second set of good practices concerns the educational activities undertaken by the DPAs to foster a culture of privacy with a particular focus on, but not limited to, younger generations. Specific courses, seminars and lectures may then be organized to address the actors involved in data processing operations. Issuing guidance to those actors represents another important good practice carried out by the Data Protection Authorities. Finally, special prizes may be awarded to promote compliance with data protection legislation.

In pursuing the most effective functioning of the legislation and facilitating access to effective remedies, many national DPAs have set up elaborate internet sites and web pages. Through the latter, it is possible to submit official documents provided for in the legislation, to register or notify the processing of personal data, to request and receive advice and/or information as well as to file a complaint. In Germany, for instance, the Independent Centre for Data Protection of Schleswig-Holstein (supported by of almost all German-speaking DPAs) hosts a website containing extensive information on recent developments, court cases, reports and press releases and a database on key concepts.[128] A comprehensive homepage with information on how to protect oneself against data protection violations, especially aimed at educators and other persons in so-called "multiplier functions" is also in place.[129] In both Spain[130] and Italy, a data transmission system for notifications to the Data Protection Authority also allows the notification of files via Internet.

In many instances the official web page is multilingual, either because of the linguistic regime in a given Member State, which calls for more than one language to be used, or because an English-language version is also provided in order to widen access. Adoption of this feature by DPAs should be given serious consideration, bearing in mind the free movement of EU citizens throughout the 27 Member States. In Luxembourg, for example, the national DPA's multilingual website materials are quite extensive and provide a wealth of information to data subjects, controllers, processors and lawmakers.[131] Also in Finland, the website of the Data protection authority is another important channel for providing information in multiple languages.[132]

The educational policy devised by certain national DPAs is an innovative element which is multi-faceted. On the one hand, providing educational programmes in all levels of education, i.e. from primary school to university, encourages the development of awareness in data protection matters. On the other hand, targeting different age sections of society through specifically adapted programmes may provide useful feedback as to the peculiarities and necessities that different levels of our societies need. Mass media provides ample space for further elaborating TV programmes, interactive web pages and other initiatives that would raise public awareness. In the Czech Republic, for instance, the DPA runs a project aimed at children and youth and an educational program called "Protection of Personal Data in Education". The national authority also cooperated in the creation of a TV serial about data protection in 2006 "Ignorance is no Excuse – We all Have Secrets" (according to the Annual Report of 2006 each episode was viewed by approx. 160,000–310,000 persons).[133] Another good practice in the field of education is the participation of experts of the Data Protection Authority in lectures and seminars given to interest groups. This is the case of Finland where a magazine published by the DPA and aimed at controllers in particular is issued four times a year. Moreover, advice is also given by telephone. In Portugal and Belgium, the DPAs run internship programmes allowing law students and graduates to undertake a period of practical training in order to familiarise themselves with its work. In Italy specific communication initiatives were launched with particular regard to youth (among these, the DPA collaborated with the *Ministero dell'Istruzione* [Ministry of Education] on Guidelines for the appropriate use of mobile telephones and their video cameras during school classes).

Offering guidance and advice relating to various data system projects is an important and constantly growing task. The DPA in Spain has been very active in issuing guides in relation to many fields that have implications for data protection matters:

126 G. Zwenne et al. (2007), *Eerste fase evaluatie Wet bescherming persoonsgegevens*, online at: http://www.wodc.nl/images/1382a_volledige_tekst_tcm44-61969 (24.02.2010). An English summary can be consulted at page 207 of the report.
127 H.B. Winter et al. (2008), Wat niet weet wat niet deert, WODC 2008, http://www.wodc.nl/onderzoeksdatabase/evaluatie-wet-bescherming-persoonsgegevens-wbp-2e-fase.aspx# (24.02.2010)..
128 http://www.datenschutz.de (09.10.2009).
129 http://www.datenparty.de/ (30.01.09).
130 https://212.170.242.196/portalweb/canalresponsable/inscripcion_ficheros/Notificaciones_tele/que_es/index-ides- idphp.php (24.02.2010).
131 http://www.cnpd.lu/fr/ (24.02.2010).
132 www.tietosuoja.fi (24.02.2010).
133 See *Výroční zpráva za rok 2006* (Annual Report of 2006), p. 2 available at http://www.uoou.cz/vz_2006.pdf (02.01.2009).

the rights of children and the duties of parents;[134] data security measures;[135] filing;[136] data protection as a fundamental right;[137] personal data for city councils;[138] for State Schools and State universities; Professional Associations; public health services, and public social services. The same is true for Estonia[139] and for Italy[140] as well. In France and United Kingdom, the data protection authorities have issued data protection guides in the context of employment.

With regard to awareness-raising, a good practice to highlight is the informational and advisory campaigning conducted by the national DPA in the fight against 'spam' or unsolicited e-mail. In France, for instance, the objective of the Data Protection Authority was to collect and process the complaints of Internet users, and to direct them to the different actors involved in the campaign against 'spam', such as public and political authorities and professionals, according to their diverse missions and capabilities.[141] Also in Spain, the national supervisory authority has been directly engaged in drafting information guides[142] and a Decalogue of recommendations[143] to combat spam.

A good practice can also be found in the establishment of special prizes to be awarded by DPAs. In Slovenia, every year on the occasion of European Data Protection Day, the national supervisory body selects the private company or public body that it considers has been the most successful at personal data protection. It is awarded a "good practice" prize and recommended as a role model in the field.[144] In France, a doctoral prize *Data Processing, Data Files and Individual Liberties* was created by the national supervisory authority, for the amount of 7,000 Euros. Along the same lines, a proposal for the creation of a Noble Prize in the field of Data Protection and Liberties was approved in 2008 and will be first awarded from 2010.[145] Further, a prize for best practices in data protection across European public services has been instituted in Spain.

134 https://www.agpd.es/portalweb/canal_joven/common/pdfs/recomendaciones_menores_2008.pdf (09.01.2009)
135 https://www.agpd.es/portalweb/canaldocumentacion/publicaciones/common/pdfs/guia_seguridad_datos_2008.pdf (09.01.2009).
136 https://212.170.242.196/portalweb/canaldocumentacion/publicaciones/common/pdfs/guia_responsable_ficheros.pdf (09.01.2009).
137 https://212.170.242.196/portalweb/canal_joven/common/pdfs/FOLLETO.pdf (09.01.2009)
138 http://www.madrid.org/cs/Satellite?c=CM_Publicacion_FA&cid=1114180060765&idPage=1109266885968&language=es&pagename=APDCM%2FCM_Publicacion_FA%2FfichaPublicacionAPDCM (24.02.2010).
139 See: http://www.aki.ee/est/?part=html&id=56 (23.01.2009).
140 Among the most relevant guidelines, the practical guidelines for SMEs, on employer-employee relationships in both private public sector, on customer relations in the banking sector, on publishing and disseminating documents and by local authorities, on data processing within the framework of clinical drug trials, on loyalty cards..
141 See partnership agreement signed on 30.10.2007 between the French DPA and the association Signal Spam.
142 µhttps://www.agpd.es/portalweb/canaldocumentacion/lucha_contra_spam/common/pdfs/INFORMACI-OO-N- SPAM--ap-V.-30-mayo-cp-.pdf§ (09.01.2009).
143 https://212.170.242.196/portalweb/canaldocumentacion/lucha_contra_spam/common/pdfs/CONSEJOS-para-prevenir-el-Spam_guia.pdf (09.01.2009).
144 http://www.lek.si/slo/mediji/sporocila-za-javnost/3849/§ and µhttp://www.ip-rs.si/novice/detajl/nagrajenca-ob-2-evropskem-dnevu-varstva-osebnih-podatkov-sta-zavod-za-zdravstveno-zavarovanje-slove/ (30.12.2008).
145 IPA Declaration «International Privacy Association» on the creation of a Nobel Prize in the field of Data protection and liberties, to be awarded annually by the global conference of authorities on the protection of data. http://www.privacyconference2008.org/index.php?langue=2&page_id=1 (12.12.2008).

7. Conclusion

There exist a number of ways forward, both at the EU and national levels, in addressing some of the most pressing challenges faced by the current data protection regime. While national measures could certainly be adopted, a coordinated and harmonized approach through the EU may be more successful in strengthening personal data protection.

The role of the EU institutions is particularly important in these issues, and the European Parliament has taken a keen interest in data protection.[146] The European Parliament, along with the Council of the EU and the European Commission, are called upon to introduce legislative reforms in order to guarantee the effectiveness of the data protection regime. In this respect, it is reassuring that the Commissioner for Justice, Fundamental Rights and Citizenship has stressed the importance of data protection and her intention to bring together the EU's data protection rules into a modern and comprehensive legal instrument.[147] The ECJ, in turn, has taken a proactive stance concerning data protection. Thus, it has so far interpreted an instrument of internal market harmonization (the Data Protection Directive) in such a manner that fosters the protection of a fundamental right within the Community. In this respect, it has adopted an extensive reading of the protective scope of the Data Protection Directive, which goes beyond the exercise of economic activities, and a restrictive interpretation of the areas exempted from protection.

Improvements to existing data protection legislation can also be achieved through cooperation between the national Data Protection Authorities and the Article 29 Working Party. In particular, the opinions and recommendations of the Working Party, insofar as they are taken into account by the national DPAs, contribute to the development of a common EU standard with a high level of personal data protection. The European Data Protection Supervisor too is entrusted with the task of ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to privacy, are respected by the Community institutions and bodies. The consultation task of the European Data Protection Supervisor is of particular importance, in that it contributes effectively to the safeguarding of the fundamental freedoms of the Union's citizens when new legislation is passed.

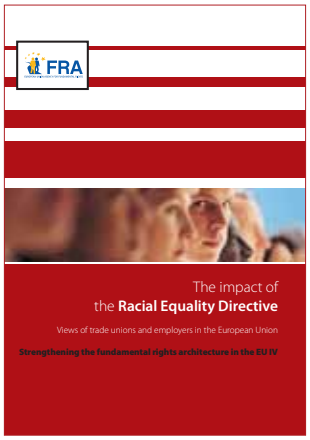
Improvements also need to take place concerning the independence, effectiveness, resources and powers of DPAs. They play a crucial role as guardians of data protection in the eyes of the public. The whole data protection system depends on public trust of these authorities. It will be difficult to convince citizens that their data protection and privacy concerns are taken seriously, if doubts about the independence of data protection authorities persist or if these authorities are not seen to be resourced in such a way as to allow them to discharge their duties effectively and efficiently.

Data protection authorities are also a crucial part of the EU fundamental rights architecture because the EU plays a pioneering role for data protection as a fundamental right and because the EU has been instrumental in driving the development of data protection systems in many Member States. Data protection is also a key policy area for the EU where the EU has competence to legislate in the field of fundamental rights. For this reason, the overall effectiveness of the data protection system could also have a positive impact on the public's perception of the EU as a guardian of fundamental rights.

146 Note for example the Proposal of the European Parliament Committee on Civil Liberties; Justice and Home Affairs for a European Parliament recommendation to the Council on strengthening security and fundamental freedoms on the internet (2008/2160(INI)).

147 See Notice to Members of the European Parliament, 7.1.2010, doc. PE431.139v02-00, http://www.europarl.europa.eu/hearings/static/commissioners/answers/reding_replies_en.pdf (23.02.2010).

These four reports by European Union Agency for Fundamental Rights (FRA) look at closely related issues, institutions, and EU legislation, which contribute to the overarching architecture of fundamental rights in the European Union. The building blocks of this fundamental rights landscape are the data protection authorities and national human rights institutions (NHRIs), as well as Equality Bodies set up under the Racial Equality Directive (2000/43/EC).



European Union Agency for Fundamental Rights

Data Protection in the European Union: the role of National Data Protection Authorities

Luxembourg: Publications office of the European Union, 2010

2010 – 50 p. – 21 x 29,7 cm

ISBN 978-92-9192-509-4
doi:10.2811/47216

A great deal of information on the European Union Agency for Fundamental Rights is available on the Internet. It can be accessed through the FRA website (http://fra.europa.eu).

TK-31-09-265-EN-C

doi:10.2811/47216

FRA - European Union Agency for Fundamental Rights, 2010
Schwarzenbergplatz 11
1040 - Wien
Austria
Tel.: +43 (0)1 580 30 - 0
Fax: +43 (0)1 580 30 - 691
E-Mail: information@fra.europa.eu
http://fra.europa.eu

ISBN 978-92-9192-509-4