Chapter A
Data Protection Standard in the AFSJ

In order to study the observance of the AFSJ actors with European data protection principles, these principles have to be identified.

The following analysis will therefore show the basic data protection standard which is applicable to all of the AFSJ actors as well as to the information exchange systems in the AFSJ. It is interesting to analyse, which rules are actually applicable to an area in which former first pillar structures mix with former third pillar rules. Additionally, due to the fact that this area was for a long time exclusively governed by public international law instead of Community law, the jurisprudence of the ECtHR is an essential source in the search of rules for security-related data processing at EU level. After having given a brief introduction relating to the fundamentals of data protection law (Sect. I), in a second subsection (Sect. II) the framework for the discussion consists therefore of the data protection instruments of the Council of Europe, in particular of the European Convention of Human Rights. On the basis of these data protection rules, a third section focuses on the data protection principles applicable in the AFSJ included in EU law (Sect. III).

I Brief Historical Review and Reasons for Data Protection

As mentioned in the introduction, data protection in EU law constitutes a relatively new individual right which has its roots in public international law instruments such as the OECD Guidelines of 1980, Convention No. 108 and in Article 8 ECHR and its interpretation by the European Court of Human Rights (ECtHR). The earliest provisions on data protection at national level have been developed in the 1970s in response to the rise of information technology and the beginning of the computer age. New techniques which allowed for the collection, processing and storage of large amounts of data made it possible for governmental and private actors to use, process and combine more information than ever. For the first time in European

F. Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice*, DOI 10.1007/978-3-642-22392-1_2,

history, databases could store and processes a huge quantity of personal data.[1] One the one hand, the technical changes facilitated the use of the collected data for various purposes and lead to vast data pools in the property of national authorities. On the other hand, the automatic processing of data increased the risk of misuse of these data.[2]

Against this background, legal scholars point to the fact that every data processing duplicates the risk of abuse (intended or not) of the relevant information.[3] *Simitis* for instance refers to the risks of automated processing. The entry of incorrect data in one database may have serious consequences for the individual concerned when the wrongfully entered data are reproduced in another database, used in another context or even transferred to another actor.[4] The author warns against the risk of losing the context of the original information when processing data automatically. Automated processing often curtails the relevant information which may lead to the removal of important facts from the original information. *Simitis* gives the concrete example, that the reasons for an illness, for an entry in a police file or for the delayed payment of debts may get lost during the automatic processing of data. After repeated data processing, the remaining information may include information limited to an illness, the entry in a police file and the delayed payment without knowing the reasons which lead to these entries. Each of these entries may make it difficult for persons concerned to find a workplace or simply to open a bank account. In the worst case, the transmission of wrong information can lead to an economic, political or social discrimination of the person concerned.[5]

In view of these risks, the national legislators were obliged to adopt rules to standardise data processing. The German federal state of Hessen endorsed the first data protection act worldwide in 1970.[6] Three years later the Swedish legislator followed and adopted the first national data protection law.[7] The German federal legislator enacted its national data protection act in 1977. [8] The Swedish and the

[1] Johlen (2006) Article 8, para 1; Simitis (2006), p. 64, para 8.

[2] Simitis (2006), p. 65, para 10.

[3] Simitis (2006), p. 65, para 9.

[4] Simitis (2006), pp. 65 and 66, paras 10–13.

[5] Simitis (2006), p. 65, para 10.

[6] Hessisches Datenschutz Gesetz, 7 Oktober 1970 – GVBl. (Gesetz- und Verordnungsblatt) I, 1970, p. 625; for criticism with regard to the use of the term "data protection" see Simitis (1971), in particular p. 679.

[7] Swedish data protection act, Datalag SFS 1973:289. In addition to the technological development, a census obliged the Swedish legislator to develop rules regulating the processing and the treatment of the collected data. To the international development of data protection legislations, compare the excellent overview in Simitis (2006) pp. 108–117, paras 127–150. The (German) literature approach makes a distinction between the different generations of data protection regulations, for details see Di Martino (2005), p. 33 et seq.

[8] Gesetz zum Schutz vor Missbrauch von personenbezogenen Daten bei der Datenverarbeitung, BDSG, 27 January 1977, BGBl. I, 201.

German data protection acts based on different approaches.[9] The most functional aspects of both approaches were later combined by other European countries which benefited from the experiences made by the Swedish and German legislators. The first French data protection act[10] of 1978, for instance, principally based on the Swedish model.[11]

Due to the technological developments and the national legislative activity, the first European instruments highlighting the importance of data protection rules followed soon. The most influential actor with regard to the development of data protection rights at European level was the Council of Europe. The adoption of Convention No. 108 in the year 1981 and the case law of the ECtHR regarding Article 8 ECHR considerably influenced the development and understanding of data protection rules in Europe in the last decades. Under the influence of Convention No. 108, even countries with hesitant approaches to privacy and data protection rules, such as the United Kingdom, followed suit and adopted its first data

[9] The Swedish legislator regulated the processing procedure. Control agencies were established and data processors were obliged to disclose their processing modalities and to reveal their methods of collection. Processors had to make a declaration about the procedure of processing and could thereupon receive a processing permit when the procedure was in compliance with the requirements of the control authority. The obligation to obtain a permit from the national control authority made it possible to react in each individual case and facilitated the adaptation to the fast developing technological challenges. However, this procedure implicated enormous administrative efforts and for this reason the Swedish legislator renewed the data protection act already in 1982. Nonetheless, the Swedish data protection act is the basis for the European tradition of the "omnibus approach" which means that general binding rules regulate the legal relations in the public as well as in the private sector. The German legislator followed the so called global approach or self-assessment model. A framework of generally binding rules regulated the processing of personal data, i.e. general rules on data protection built a regulatory framework but details were controlled by the data processors themselves. In consequence each data processor was held responsible for its own area and for the implementation of the general rules within its field of activity. The control authority did not intervene during the data processing procedure as long as no conflict between the data processor and the person concerned emerged. In principle, the German legislator enacted global rules instead of specific regulations formulated by the Swedish legislator. Additionally, the German data protection act was not applicable to private actors; the rules were only applicable to German public authorities. Nevertheless, the Swedish and the German approach represent the basis for following data protection acts in other European countries. For more details compare Burkert (2003), p. 93 et seq.; Ellger (1990), p. 421 et seq.

[10] Loi no. 78–17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés. See with regard to the beginnings of French data protection Maisl (1987); Mallet-Poujol (1999); Nugter (1990), pp. 77–106; Weill (1987).

[11] Some differences nevertheless existed, i.e. even though the act was applicable to public as well as private actors (omnibus approach) and established a control agency, the CNIL (Commission Nationale de l'Informatique et des Libertés), only the public sector was obliged to get prior authorisation for the data processing. For data processing by private actors a notification was sufficient. Nowadays, this system, composed of authorisation and notification, still exists (even though it is modified in details). In consequence, the French data protection act is a combination of the German and the Swedish models. The need of prior authorisation is based on the Swedish data protection act and the notification duty on the German data protection rules. Compare Gruber (2007); Mitrou (1993), pp. 185 et seq.

protection act in 1984.[12] The relevance of the Council of Europe instruments for the shaping and interpretation of data protection rights at EU level is further illustrated in the following section.

II. Council of Europe: Art. 8 ECHR, Convention No. 108 and Recommendation R (87) 15

Illustrating the current European data protection standard from the point of view of the ECtHR allows for the derivation of general data protection principles also for EU law. Article 6 TEU thereby guarantees the respect of fundamental rights as guaranteed by the ECHR and provides for the accession of the EU to the ECHR.[13] Article 52 (3) of the Charter of Fundamental Right underlines the close connection of the rights enumerated in the Charter and the rights of the ECHR by stipulating that in so far as the Charter contains rights which correspond to the rights of the ECHR, "the meaning and the scope of those rights shall be the same as those laid down by the Convention [ECHR]".[14]Additionally, with regard to data protection law, important EU data protection instruments are a further development of the ECHR standard and its Conventions and refer to them.[15] The jurisdiction of the Strasbourg Court is crucial to the development of data protection rights in Europe. Over the last years, the ECtHR developed a data protection system by continually emphasising the respect of the core values of European data protection principles.[16]

---

[12] The Data Protection Act 1984. Although in 1976 the United Kingdom already established a committee (the Lindop Committee) in order to prepare a data protection act, it took almost 10 years to eventually adopt binding rules on data protection. This first data protection act of 1984 was heavily criticised and later amended by the second data protection act in 1998, around 16 month later than required under Directive 95/46. The second data protection act extended data protection rules to forms of manual processing and made important changes with regard to the rights of individuals in data protection law in the United Kingdom. For details see Pinegar (1984); Bainbridge (2005); Carey (2004); Lloyd (1998); Hamilton and Jay (2003); Singleton (1998).

[13] With regard to the consequences of the accession, see Lock (2010).

[14] Article 52 (3) of the Charter of Fundamental Rights, OJ 2010, C-83/02 and joined cases C-92/09 and C-93/09, *Volker and Markus Schecke GbR and Hartmut Eifert* v. *Land Hessen*, judgement of 9 November 2010; compare for a deepend understanding of Article 52 (3) of the Charter and of the influence of the ECHR on the Charter of Fundamental Rights, Ziegenhorn (2009); Gebauer (2007), in particular pp. 343–349; Müller Graff (2006).

[15] Recitals (10) and (11) of Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of the individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995, L-281/31; Recitals (40) and (41) 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 2008, L-350/60; for a brief overview, refer to Breitenmoser et al. (2006), pp. 399–410.

[16] For an excellent overview of the development towards a right to data protection in Europe see Siemen (2006).

The ECtHR repeatedly emphasised that the ECHR is a "living instrument" whose interpretation facilitates immediate adaptation to specific situations.[17]

Although it seems to be difficult to derive principles of general application from the case law tailored to a specific situation, the ECtHR succeeds nonetheless in developing a comprehensive data protection framework.[18] Admittedly, it does not cover all difficulties arising in an EU law enforcement context and is the lowest common denominator as the guarantees of the ECHR apply in a public international law context, but the interpretations of the ECtHR have attained a far-reaching significance for the EU over the years and cooperation between the EU and the Council of Europe in fundamental rights matters continually improves.[19] The Memorandum of Understanding between the Council of Europe and the European Union, adopted in May 2007, clarifies that the EU will refer to the Council of Europe standards, in particular to the ECHR, when developing its fundamental rights standards.[20] Decisions, reports, conclusions, recommendations and opinions of the Council of Europe should be systematically taken as the first Europe-wide reference source for human rights.[21] As corroborated by the Memorandum as well as the case law of the European Courts, this proposal merely confirms existing practice.[22] In a Communication from the Commission to the European Parliament and the Council about the AFSJ, the accession to the ECHR is mentioned as priority

[17] See for example: *Tyrer v. the United Kingdom*, Application no. 5856/75, judgment of 25 April 1978, para 31; *Loizidou v. Turkey*, Application no. 15318/89, judgment of 23 March 1995, para 71; *Mamatkulov and Askarov v. Turkey*, Application nos. 46827/99 and 46951/99, judgment of 4 February (2005), para 121.

[18] See Siemen (2006).

[19] De Schutter (2008). See also: joint declaration on cooperation and partnership between the Council of Europe and the European Commission of 3 April 2001, available at: http://www.jp.coe.int/Upload/110_Joint_Declaration_EF.pdf (accessed February 2011); Memorandum of Understanding between the Council of Europe and the European Union of 10 May 2007, CM(2007)74, available at: https://wcd.coe.int/ViewDoc.jsp?Ref=CM(2007)74&Language=lanEnglish, (accessed February 2011).

[20] Memorandum of Understanding between the Council of Europe and the European Union of 10 May 2007, CM(2007)74, points 16 and 17. This declaration follows a proposal made in the Juncker report on the future relationship between the Council of Europe and the EU which was adopted in April 2006 by the Parliamentary Assembly of the Council of Europe; see De Schutter (2008), p. 511; Juncker Report "A sole ambition for the European continent" of 11 April 2006, available at: http://assembly.coe.int/Sessions/2006/speeches/20060411_report_JCJuncker_EN.pdf (accessed February 2011).

[21] Juncker Report "A sole ambition for the European continent" of 11 April 2006, available at: http://assembly.coe.int/Sessions/2006/speeches/20060411_report_JCJuncker_EN.pdf (accessed February 2011), p. 6.

[22] Memorandum of Understanding between the Council of Europe and the European Union of 10 May 2007, CM(2007)74, point 17; Case C-465/00, *Rechnungshof v. Österreichischer Rundfunk and Others*, judgment of 20 May 2003, paras 10 and 19; details to the relation between the EU Courts and the ECtHR can be found in Häberle (2009), in particular pp. 460–480.

issue.[23] By emphasising that the Union's accession will complete the system of protection in this field, the Commission recognises the close relationship between the fundamental rights system of the ECHR and the EU. The Communication assumes that the accession will encourage the case-law of the European Court of Justice and the ECtHR to develop in step.

Certainly, one important benefit of the close relationship between fundamental rights interpretations of the EU and the Council of Europe is the far reaching scope of the ECtHR's jurisdiction which goes beyond the previously restricted competences of the EU Courts in common foreign and security policy as well as in police and judicial cooperation in criminal matters. The ECtHR's jurisdiction can stipulate overarching principles in fields where the control of European Courts was limited by the treaties.[24] Many EU instruments and national legal orders refer directly or indirectly to the ECHR provisions and their interpretation.[25] The ECHR standard is therefore the broadest and farthest-reaching data protection standard in Europe applicable regardless of (former) EU pillars, national borders or competence obstacles.

The structure of the following section mirrors the method generally used by the ECtHR to examine whether data processing complies with Article 8 ECHR: Does the data processing fall within the scope of Article 8 ECHR, is there an interference with the right to private life and is this interference justified because it is in accordance with the law, pursues a legitimate aim and is necessary in a democratic society.

[23] Communication from the Commission to the European Parliament and the Council, an area of freedom, security and justice serving the citizen, COM(2009) 262 final of 10 June 2009, paragraph 2, p. 7, compare also Lock (2010).

[24] The former limitations of the European Courts are summarised in Bieber et al. (2006), pp. 250–252; With regard to the impact of the ECtHR on the interpretation of privacy, compare De Hert and Guthwirth (2006).

[25] See for instance: Article 6 (2) EU Treaty, United Kingdom's Human Right Act 1998 (HRA), schedule 1, paragraph 2 (1) a ("A ECtHR or tribunal determining a question which has arisen in connection with a Convention right must take into account any judgment, decision, declaration or advisory opinion of the European ECtHR of Human Rights") or Administrative Act of Luxembourg 2007/A, Vol. 1 p. 35. See also: Judgment of the Second Senate of the German Constitutional Court of 14 October 2004, 2 BvR 1481/04, *Görgülü*, headnotes: "The principle that the judge is bound by statute and law (Article 20.3 of the Basic Law (Grundgesetz – GG)) includes taking into account the guarantees of the European Convention for the Protection of Human Rights and Fundamental Freedoms and the decisions of the European ECtHR of Human Rights (ECHR) as part of a methodologically justifiable interpretation of the law. Both a failure to consider a decision of the ECHR and the "enforcement" of such a decision in a schematic way, in violation of prior-ranking law, may violate fundamental rights in conjunction with the principle of the rule of law.

In taking into account decisions of the ECtHR, the state bodies must include the effects on the national legal system in their application of the law. This applies in particular when the relevant national law is a balanced partial system of domestic law that is intended to achieve an equilibrium between differing fundamental rights". For the English legal system see as well: Coppel (2007).

1. *Data Protection Guarantees of Article 8 ECHR*

In the last years, there has been a strong development towards a right to data protection within the framework of Article 8 ECHR.[26] Even though data are not expressly protected by this Article, the ECtHR insists 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.[27] It is commonly acknowledged that data protection guarantees originate from the further development of the right to private life stipulated in Article 8 ECHR, nowadays forming a vital part of this right.[28] The guarantees of Article 8 ECHR therefore represent the basis for an overarching European data protection standard. It reads as follows:

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.

Understanding and analysing the ECtHR's application of the Convention's right to respect for private life is a crucial element in the search of the right to data protection in the Council of Europe context. At this point, it is worth briefly examining the obligations which Article 8 ECHR states in general, before analysing the details of the scope of the right to data protection entailed in the protection of the right for private life based on Article 8 ECHR.

---

[26] See analysis of Siemen (2006); Marauhn and Meljnik (2006), paras 29 and 39.

[27] *Z. v Finland*, Application no. 22009/93, judgment of 25 February 1997, para 95; *Peck v. United Kingdom*, Application no. 44647/98, judgment of 28 January 2003, para 78; *L.L. v France*, Application no. 7508/02, judgment of 10 October 2006, para 43; *Biriuk v Lithuania*, Application no. 23373/03, judgment of 25 November 2008, para 39; *I v Finland* Application no. 20511/03 of 17 July 2008, para 38; *S. and Marper v the United Kingdom*, Application nos. 30562/04 and 30566/04, judgment of 4 December 2008, para 103; *C.C. v. Spain*, Application no. 1425/06, judgment of 6 October 2009, para 31; see also: Breitenmoser (1986), p. 245; Kugelmann (2003), p. 16 et seq.; Meyer-Ladewig (2006), Article 8, para 11; Moreham (2008), pp. 44–79.

[28] *Z. v Finland*, Application no. 22009/93, judgment of 25 February 1997, para 95; *Peck v. United Kingdom*, Application no. 44647/98, judgment of 28 January 2003, para 78; *L.L. v France*, Application no. 7508/02, judgment of 10 October 2006, para 43; *Biriuk v Lithuania*, Application no. 23373/03, judgment of 25 November 2008, para 39; *I v Finland*, Application no. 20511/03, judgment of 17 July 2008, para 38; *S. and Marper v the United Kingdom*, Application nos. 30562/04 and 30566/04, judgment of 4 December 2008, para 103; *Niemietz v. Germany*, Application no. 13710/88, judgment of 16 September 1992 para 29; *Pretty v. United Kingdom*, Application no. 2346/02, judgment of 29 April 2002, para 61; *P.G. and J.H. v. United Kingdom*, Application no. 44787/98,judgment of 25 September 2001, para 56; see also: Breitenmoser (1986), p. 245; Kugelmann (2003), p. 16 et seq.; Meyer-Ladewig (2006), Article 8, para 11; Moreham (2008); Ovey and White (2006), pp. 286–297; Siemen (2006), pp. 57–132.

a) General Obligations of Article 8 ECHR

Article 8 ECHR as seen by the ECtHR entails two types of obligations, a negative and a positive one.[29] The negative obligation requires the states to assure an exercise free of interference of the rights specified in Article 8 ECHR unless the conditions in Article 8 (2) ECHR are fulfilled, which means that the state should refrain from taking certain actions.[30] The positive obligation entails the adoption of measures designed to protect the individual's rights of Article 8 ECHR, in particular against interference by others.[31]

Generally, with regard to negative obligations, the ECtHR examines firstly if there has been an interference with one of the rights stipulated in Article 8 (1) and if so, whether the interference can be justified by the rights outlined in Article 8 (2) ECHR in a second step. The focus in positive obligations cases is more on the obligation of states to assure the protection of individual's private life through the adoption of protective measures.[32] The ECtHR stipulates that "while the essential object of Article 8 is to protect the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this negative undertaking, there may be positive obligations inherent in an effective respect for private or family life. These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves".[33] Further the ECtHR emphasises that the boundaries between the State's positive and

[29] This is widely acknowledged in literature and ECtHR's case law, see Dröge (2003); Gómez-Arostegui (2005); Siemen (2006), p. 179 et seq.; Mowbray (2007), pp. 485–593, especially p. 519 et seq. See also: *Airey v. Ireland*, Application no. 6289/73, judgment of 9 October 1979, para 32 or *Z. and others v. the United Kingdom*, Application no.29392/95, judgment of 10 May 2001, para 74; compare also De Hert and Guthwirth (2006).

[30] Moreham (2008), pp. 44, 46.

[31] Moreham (2008), pp. 44, 46. 42. To the positive obligation in the ECHR, see *Özgür Gündem v. Turkey*, Application no. 23144/93, judgment of 16 March 2000, para 42: "The Court has long held that, although the essential object of many provisions of the Convention is to protect the individual against arbitrary interference by public authorities, there may in addition be positive obligations inherent in an effective respect of the rights concerned. It has found that such obligations may arise under Article 8 (see, amongst others, the *Gaskin v. the United Kingdom* judgment of 7 July 1989, Series A no. 160, pp. 17–20, §§ 42–49) and Article 11 (see the *Plattform "Ärzte für das Leben" v. Austria* judgment of 21 June 1988, Series A no. 139, p. 12, § 32). Obligations to take steps to undertake effective investigations have also been found to accrue in the context of Article 2 (see, for example, the *McCann and Others v. the United Kingdom* judgment of 27 September 1995, Series A no. 324, p. 49, § 161) and Article 3 (see the *Assenov and Others v. Bulgaria* judgment of 28 October 1998, Reports 1998-VIII, p. 3290, § 102), while a positive obligation to take steps to protect life may also exist under Article 2 (see the *Osman v. the United Kingdom* case of 28 October 1998, Reports 1998-VIII, pp. 3159–61, §§ 115–17)".

[32] For the positive obligations of Article 8 in general see Mowbray (2007), pp. 485–593, especially p. 519 et seq.

[33] *Van Kück v. Germany*, Application no. 35968/97, judgment of 12 June 2003, para 70.

negative obligations under Article 8 ECHR are not easy to define, as the applicable principles are rather similar. In clarifying whether or not such an obligation exists, attention must be paid to the fair balance which has to be struck between the general interest and the interests of the individual.[34] In both situations the State enjoys a particular margin of appreciation.[35]

In a data protection context these two obligations may collide as Article 8 ECHR for instance may justify restrictions on the disclosure of information and at the same time may give a right to access information. The following analysis will show to what extent personal data are protected in the framework of the right to respect for private life and which types of positive obligations exist in this context. The ECtHR uses the traditional three-step analysis – scope, interference and justification – to find out whether a Member States has violated Article 8 ECHR in this respect.

b) Scope of Article 8 ECHR with Regard to Data Protection

Article 1 ECHR covers the general scope of the ECHR, implying a territorial, a personal and a material requirement.[36] According to it, every signatory state of the Convention "shall secure to everyone within their jurisdiction the rights and freedoms" of section one of the ECHR, including the rights guaranteed in Articles 2–18 ECHR and the rights contained in the additional protocols.[37]

The state is obliged to respect the rights of the Convention within the borders of its "jurisdiction" (territorial scope).[38] Article 1 ECHR in connection with Article 34 ECHR restricts the liability of states to governmental actions.[39] There may be nevertheless effects on third parties when a state is held responsible for failing its positive obligation to protect the individual against interferences from private actors.[40] The rights of the ECHR generally apply to every person of the contracting state including civil servants, third country nationals or soldiers providing that they are subjected to the jurisdiction of one of the Convention's states (personal scope "ratione personae").[41] The claim of an alleged violation is restricted to the rights

[34] *Van Kück v. Germany*, Application no. 35968/97, judgment of 12 June 2003, para 71.

[35] *Van Kück v. Germany*, Application no. 35968/97, judgment of 12 June 2003, para 71; to the "margin of appreciation doctrine", see Gebauer (2007), pp. 248–253.

[36] Meyer-Ladewig (2006), Artikel 1, para 1; there is also a temporal requirement which refers to interferences before the ECHR entred into force, see Article 35 ECHR.

[37] Meyer-Ladewig (2006), Artikel 1, para 1.

[38] To the details see Ovey and White (2006), pp. 24–34 or Clapham (2006), pp. 387–400 and *Ilascu and others v. Moldova and Russia*, Application no. 48787/99, judgment of 8 July 2004.

[39] Ovey and White (2006), pp. 31–32.

[40] The notion of positive obligations and the exact extent to which a State may be liable for private actions will considered later in this chapter. To the liability for acts of international organisations, see Ovey and White (2006), p. 29–30.

[41] To the restrictions, see Meyer-Ladewig (2006), Artikel 1, para 10.

and freedoms set forth in the ECHR and in its additional protocols (material requirement).[42]

Data protection elements could be found in cases concerning the protection of the right to private life as guaranteed in Article 8 ECHR since the beginning of the ECHR's interpretation.[43] Up to the late 1990s, the ECtHR avoided using the term "data protection" in the context of Article 8 ECHR when describing the effects of what today is commonly understood as protection of personal data.[44] That is why analysing data protection effects and implications in the ECtHR's case law is always closely connected to the meaning of private life in the course of Article 8 ECHR. This has to be briefly specified.

The term private life in Article 8 ECHR indicates a range of different interests accumulated under the notion of an overarching principle. The ECtHR has repeatedly stated that it is "a broad term not susceptible to exhaustive definition".[45] Some authors qualify the right with regard to the ECtHR's jurisdiction as "ill-defined and amorphous".[46] This assessment arises out of the ECtHR's "unwillingness" to identify categories permitting a clear classification of the content of the right to respect for private life.[47]

However, over the years, the ECtHR specified the scope of Article 8 ECHR with regard to data protection while logically remaining within the boundaries of the scope of private life. For this reason, *Siemen* concludes that the scope of a right to data protection reaches so far as the scope of the right to respect for private life.[48] Whereas in the past, the right to data protection was very closely attached to the right to private life, in recent years, the ECtHR seems to apply the right to data protection more independently from its private life roots.[49] The analysis in the

[42] Meyer-Ladewig (2006), Artikel 1, para 1.

[43] *Klass v. Germany*, Application no. 5029/71, judgment of 6 September 1978; *Malone v. the United Kingdom*, Application no. 8691/79, judgment of 2 August 1984; *Leander v. Sweden*, Application no. 9248/81, judgment of 26 March 1987.

[44] The first time the ECtHR used the term "protection of personal data" was in *Z. v Finland*, Application no. 22009/93, judgment of 25 February 1997, para 95.

[45] *Peck v. United Kingdom*, Application no. 44647/98, judgment of 28 January 2003, para 57; *Niemietz v. Germany*, Application no. 13710/88, judgment of 16 September 1992, para 29; *Pretty v. United Kingdom*Application no. 2346/02, judgment of 29 April 2002, para 61; *P.G. and J.H. v. United Kingdom*Application no. 44787/98, judgment of 25 September 2001, para 56; Ovey and White (2006), p. 246; Siemen (2006), p. 57; Meyer-Ladewig (2006), Artikel 8 para 3.

[46] Moreham (2008), pp. 44, 45.

[47] Moreham (2008), pp. 44, 45; see also: Beck (2008), pp. 214–244, 232–235.

[48] Siemen (2006), p. 57.

[49] Compare case *Reyntjens v. Belgium*, Application no. 16810/90, admissibility decision of 9 September 1992, where the commission stated that passport information did not entail personal information raising private life concerns) to cases giving priority to data protection elements: *Panteleyenko v. Ukraine*, Application no. 11901/02, judgment of 29 June 2006; *S. and Marper v the United Kingdom*, Application nos. 30562/04 and 30566/04, judgment of 4 December 2008; *Z. v. Finland*, Application no. 22009/93, judgment of 25 February 1997; for a exceptionally detailed analysis of this development, see Siemen (2006), pp. 79–132.

following will therefore not describe the comprehensive content of the right to private life, but will focus on the data protection elements resulting from the jurisprudence of the ECtHR on Article 8 ECHR.

In early Court judgments, a distinction was made between private and public life.[50] However, since it is not always possible to distinguish clearly which of an individual's activities form part of his public or professional life and which do not, the ECtHR developed a broader understanding of the content of the right to private life over the course of the following years.[51]

After years of discussing the exact content of the right to private life, in *Niemietz v. Germany* the ECtHR intentionally did not give a clear definition of this right.[52] Following the German "Sphärentheorie",[53] the Court first stated that a fundamental component of the right to private life certainly is the "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Additionally, the respect for private life must comprise the right to establish and develop relationships with other human beings.[54] Other cases show however that the ECtHR entrenched questions of private life referring to legitimate expectation of

[50] Decision of the European Commission of Human Rights, *X. v. Iceland* (1976).

[51] Moreham (2008), p. 44, 45. See also: *Niemietz v. Germany*, Application no. 13710/88, judgment of 16 September 1992, para 29: "The ECtHR does not consider it possible or necessary to attempt an exhaustive definition of the notion of "private life". However, it would be too restrictive to limit the notion to an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings. There appears, furthermore, to be no reason of principle why this understanding of the notion of "private life" should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world. This view is supported by the fact that, as was rightly pointed out by the Commission, it is not always possible to distinguish clearly which of an individual's activities form part of his professional or business life and which do not. [. . .]To deny the protection of Article 8 (art. 8) on the ground that the measure complained of related only to professional activities - as the Government suggested should be done in the present case - could moreover lead to an inequality of treatment, in that such protection would remain available to a person whose professional and non - professional activities were so intermingled that there was no means of distinguishing between them. In fact, the ECtHR has not heretofore drawn such distinctions: it concluded that there had been an interference with private life even where telephone tapping covered both business and private calls [. . .]; and, where a search was directed solely against business activities, it did not rely on that fact as a ground for excluding the applicability of Article 8 (art. 8) under the head of "private life"[. . .]".

[52] *Niemietz v. Germany*, Application no. 13710/88, judgment of 16 September 1992.

[53] For a general overview of the German "Recht auf informationelle Selbstbestimmung", refer to, Gartska (2008).

[54] *Niemietz v. Germany*, Application no. 13710/88, judgment of 16 September 1992, para 29.

protection and respect for private life.[55] This broad interpretation of the scope allows adapting the terms of Article 8 ECHR, which were developed in the 1950, in the light of the current data protection context. The ECtHR constantly stresses that the "convention as a living instrument must be interpreted in the light of present-day conditions".[56]

In general, the ECtHR does not specify the scope of the right to data protection in more detail.[57] The Court restricts its argumentation to the reference to Convention No. 108 by emphasising repeatedly that the broad interpretation of Article 8 with regard to private life corresponds to that of Convention No. 108 "whose purpose is to secure [...] for every individual [...] respect for his rights and fundamental freedoms, and in particular his right to privacy with regard to automatic processing of personal data relating to him",[58] such personal data being defined in Article 2 Convention No. 108 as "any information relating to an identified or identifiable individual".[59]

Limits of the scope are therefore not easy to define, as the covered subject matter generally has to comply with the two requirements mentioned in Convention No. 108: firstly, it must be information and secondly, the information must be of personal nature. Exemptions to this general rule exist, but are difficult to find.[60]

In *Smith v. the United Kingdom*, one of the rare cases concerning the personal nature of information, the ECtHR did not clarify the notion in detail.[61] The applicant sought access to business related documents held by a bank with an eye to possible further legal proceedings. The documents mainly dealt with a loan granted to the applicant in his function as managing director and controlling shareholder of an electronic group. The Court clarified that on one hand it would be artificial to declare that the requested files did not concern the applicant; however, on the other, the information at hand did not concern the applicant's identity or personal history, nor did the information have "formative implications"

[55] *Copland v. the United Kingdom*, Application no.62617/00, judgment of 3 April 2007, paras 41–42; *Von Hannover v. Germany*, Application no. 59320/00, judgment of 24 June 2004, para 51; Ovey and White (2006), p. 296; to the term legitimate expectation, see Gómez-Arostegui (2005), pp. 153–200.

[56] See for instance: *Tyrer v. the United Kingdom*, Application no. 5856/75, judgment of 25 April 1978, para 31; *Loizidou v. Turkey*, Application no. 15318/89, judgment of 23 March 1995, para 71; *Mamatkulov and Askarov v. Turkey*, Application nos. 46827/99 and 46951/99, judgment of 4 February 2005, para 121.

[57] Esser (2008), in particular pp. 282–283.

[58] Article 1 Convention No. 108.

[59] *Rotaru v. Romania*, Application no. 28341/954, judgment of 4 May 2000, para 43; see also: *Amann v. Switzerland*, Application no. 27798/95, judgment of 16 February 2000, para 65.

[60] One exemption was *Herbecq and the Association "ligue des droits des l'homme" v. Belgium*, Application no. 32200/96 and 32201/96, admissibility decision of 14 January 1998; see also De Hert and Gutwirth (2009), in particular pp. 24–25.

[61] *Smith v. the United Kingdom*, Application no. 39658/05, admissibility decision of 4 January 2007.

for his personality.[62] Additionally the information was not contained in a database currently in use, nor was it obtained through any invasive means. Under such circumstances, the ECtHR denied a violation of Article 8 ECHR without clarifying whether it based its decision on the non-compliance with the scope or with the interference of Article 8 ECHR.

However, while the ECtHR's interpretation of Article 8 ECHR covers in principle any personal information, one can distinguish the different data categories which have been identified as being protected so far. When looking in more detail at the relevant case law, there are several types of data which can be "extracted" from the ECtHR's jurisdiction. Protected data categories are amongst others: any personal information stored in a public file,[63] telecommunication data,[64] audio or video material containing personal information,[65]

[62] *Smith v. the United Kingdom*, Application no. 39658/05, admissibility decision of 4 January 2007.

[63] For instance: *Leander v. Sweden*, Application no. 9248/81, judgment of 26 March 1987; *Amann v. Switzerland*, Application no. 27798/95, judgment of 16 February 2000; *Panteleyenko v. Ukraine*, Application no. 11901/02, judgment of 29 June 2006; *S. and Marper v the United Kingdom*, Application nos. 30562/04 and 30566/04, judgment of 4 December 2008; *Z. v. Finland*, Application no. 22009/93, judgment of 25 February 1997; *Rotaru v. Romania*, Application no. 28341/954, judgment of 4 May 2000; *Cemalettin Canl v. Turkey,* Application no. 22427/04, judgment of 18 November 2008; *Segerstedt-Wiberg and others v. Sweden,* Application no. 62332/00, judgment of 6 June 2006; for cellular samples, fingerprints and DNA, see *Mc Veigh and others v. United Kingdom*, Application no. 8022/77, Commission decision of 18 March 1981; *Kinnunen v. Finland*, Application no. 18291/91, Commission decision of 13 October 1993; *S. and Marper v the United Kingdom*, Application nos. 30562/04 and 30566/04, judgment of 4 December 2008.

[64] For instance: *Liberty and others v. the United Kingdom*, Application no. 58234/00, judgment of 1 July 2008, para 56; *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006, para 78; *P.G. and J.H. v. the United Kingdom*, Application no. 44787/98, judgment of 25 September 2001; *Allan v. the United Kingdom*, Application no. 48539/99, judgment of 5 November 2002, para 35; *Wood v. the United Kingdom*, Application no. 23414/02, judgment of 16 November 2004 and *Doerga v. Netherlands*, Application no. 50210/99, judgment of 27 April 2004; *Kopp v. Switzerland*, Application no. 23224/94, judgment of 25 March 1998; *Halford v. the United Kingdom*, Application no. 20605/92, judgment of 25 June 1997 and *Amann v. Switzerland*, Application no. 27798/95, judgment of 16 February 2000; *Kruslin v. France*, Application no. 11801/85, judgment of 24 April 1990; *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, Application no. 62540/00, judgment of 28 June 2007.

[65] For instance: *Klass v. Germany*, Application no. 5029/71, judgment of 6 September 1978; *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006, para 78; *Chalkley v. the United Kingdom*, Application no. 63831/00, judgment of 12 June 2003, para 24; *Lewis v. the United Kingdom*, Application no. 1303/02, judgment of 25 November 2003, para 18; *Khan v. the United Kingdom*, Application no. 35394/97, judgment of 12 May 2000, paras 25–28, and *Armstrong v. the United Kingdom*, Application no. 48521/99, judgment of 16 July 2002, para 19; *Hewitson v. the United Kingdom*, Application no. 50015/99, judgment of 27 May 2003, para 20; *Huvig v. France*, Application no. 11105/84, judgment of 24 April 1990, para 25; *Malone v. the United Kingdom*, Application no. 8691/79, judgment of 2 August 1984; *Valenzuela Contreras v. Spain*, Application no. 27671/95, judgment of 30 July 1998; *Allan v.*

images,[66] medical data,[67] DNA and fingerprints records[68]; personal information published on the internet[69] etc.

It is worth noting that by examining the scope, the ECtHR does not pay attention to the means by which personal data are collected, registered or released.[70] In cases related to access to personal data, the ECtHR generally admits a wide scope to applicants invoking this right, however, under the condition that the requested information contains personal information.[71] Whereas in the past the ECtHR focused on the private nature of the data at issue by examining whether the content of the data was related to the right to private life, the analysis of the data very closely connected to private life is less common nowadays.[72]

the United Kingdom, Application no. 48539/99, judgment of 5 November 2002; *P.G. and J.H. v. the United Kingdom*, Application no. 44787/98, judgment of 25 September 2001; *Peck v. the United Kingdom*, Application no. 44647/98, judgment of 28 January 2003, para 57; *Wisse v. France*, Application no. 71611/01, preliminary objection of 20 December 2005; *Perry v. the United Kingdom*, Application no. 63737/00, judgment of 17 July 2002; *Peck v. the United Kingdom*, Application no. 44647/98, judgment of 28 January 2003; *Bykov v. Russia,* Application no. 4378/02, judgment of 10 March 2009.

[66] For instance: *Von Hannover v. Germany*, Application no. 59320/00, judgment of 24 June 2004; *Sciacca v. Italy*, Application no. 50774/99, judgment of 11 January 2005; *Friedl v. Austria*, Application no. 15225/89, judgment of 31 January 1995; *Schüssel v. Austria*, Application no. 42409/98, judgment of 21 February 2002, para 2;

[67] For instance: *Z. v. Finland*, Application no. 22009/93, judgment of 25 February 1997; *M.S. v. Sweden*, Application no. 20837/92, judgment of 27 August 1997; *Gaskin v. the United Kingdom*, Application no. 10454/83, judgment of 7 July 1989; *Martin v. the United Kingdom*, Application no. 27533/95, admissibility decision of 28 February 1996; *Biriuk v. Lithuania*, Application no. 23373/03, judgment of 25 November 2008; *I. v. Finland*, Application no. 20511/03, judgment of 17 July 2008; *Panteleyenko v. Ukraine*, Application no. 11901/02, judgment of 29 June 2006.

[68] *S. and Marper v. the United Kingdom*, Application nos. 30562/04 and 30566/04, judgment of 4 December 2008.

[69] *K.U. v. Finland*, Application no. 2872/02, judgment of 2 December 2008.

[70] See for instance: *Bykov v. Russia,* Application no. 4378/02, judgment of 10 March 2009, para 79; according to Article 3 (1) Convention No. 108 is restricted to automated processing of personal data whereas Directive 95/46 applies to automatic and not automatic means of data processing (Article 3).

[71] *C.G. and others v. Bulgaria*, Application no. 1365/07, judgment of 24 April 2008; *Amann v. Switzerland*, Application no. 27798/95, judgment of 16 February 2000; *Rotaru v. Romania*, Application no. 28341/95, judgment of 4 May 2000; *Gaskin v. the United Kingdom*, Application no. 10454/83, judgment of 7 July 1989; to the limits of this right, see *Smith v. the United Kingdom*, Application no. 39658/05, admissibility decision of 4 January 2007.

[72] Compare case *Reyntjens v. Belgium*, Application no. 16810/90, admissibility decision of 9 September 1992, where the commission stated that passport information did not entail personal information raising private life concerns, and *S. and Marper v the United Kingdom*, Application nos. 30562/04 and 30566/04, judgment of 4 December 2008; for a detailed analysis of this development, see Siemen (2006), pp. 79–132.

In summary, the scope of Article 8 ECHR covers the following activities: storage, release as well as different forms of collection and processing of and access to personal data.[73]

All in all, the question as to whether the right in fact is covered by the guarantees of Article 8 is usually examined in the assessment of the interference.[74] The following case law therefore demonstrates fundamental principles which were developed over the last years.

c) Interferences

The interference is closely related to the scope and refers to it by "shaping" and defining its substance and limits.[75]

Except for the fact that according to Article 8 (2) ECHR the interference must be attributable to a public authority, the ECtHR neither developed an exhaustive definition of the notion of the interference, nor did it specify its requirements in detail over the last few years. In the majority of cases the Court applied a case-by-case approach.

However, the ECtHR increasingly seeks to support the weight of its judgments by stipulating general principles which are supposed to serve as guidelines for similar questions. Clarifying the existence of an interference is nevertheless important for the distinction between actions (or omissions) which interfere with the Convention and which therefore require justification, and activities which are not legally relevant to the Convention.[76] The recognition of a violation of a Convention right due to a failure to act may have effects on third parties, such as private actors. In this way the ECtHR can affirm an indirect secondary effect ("Drittwirkung") of the right at stake.[77]

The following examples of significant judgments, mainly including general principles, should illustrate the ECtHR's approach of what amounts to an interference in a data protection context.

aa) Surveillance and Unwanted Release of Personal Information

Unwanted surveillance can have an influence on an individual's physical and psychological integrity as protected by Article 8 ECHR. In this category, three types of cases occur in connection with data protection: Unwanted listening to and watching of individuals (surveillance), as well as unwanted publishing of personal

[73] See also: Ovey and White (2006), pp. 286–299; Grabenwarter (2009a), p. 201, para 10; Meyer-Ladewig (2006), Article 8, para 11-14a; Marauhn and Meljnik (2006), paras 29 and 39; Peters (2003), pp. 160–162.

[74] Grabenwarter (2009a), p. 210, para 25; Heselhaus and Nowak (2006), p. 623 para 31.

[75] Grabenwarter (2009a), p. 112, para 6; Heselhaus and Nowak (2006), p. 623 para 31.

[76] Grabenwarter (2009a), p. 112, para 6.

[77] Ibid.

information. Even if the first two types do not exclusively concern the right to protect personal data, surveillance measures affect components of it in any case, and have a strong influence on the ECtHR's interpretation of the right to data protection in the framework of Article 8 ECHR.

(1) Unwanted Listening

An early example of the protection offered by Article 8 ECHR against unwanted surveillance measures is the judgment in the case *Klass v. Germany* in 1978.[78] *Klass*, a German lawyer, filed a suit against security legislation enacted by Germany monitoring mail and telephone communication (the G-10 Act) in the aftermath of the terrorist threats of the 1970s.

The ECtHR used this case as an opportunity to stipulate basic principles balancing the state's secret surveillance powers against the rights of targeted individuals, in particular the right to be informed of the surveillance measures and the possibility of having recourse to the courts after termination of such measures.[79]

Before however discussing the guarantees of Article 8 ECHR, the Court had to clarify the applicants' victim status, as neither of the applicants had already been the subject of surveillance measures, and the ECHR does not permit individuals to complain against a law *in abstracto*.[80] Due to the secrecy of the measures in question, and the establishment of a system of surveillance under which all German citizens could potentially have their mail, post and telecommunications unknowingly monitored, the ECtHR found that it was intolerable that the guarantees of Article 8 ECHR could be circumvented by the simple fact that the person concerned was kept uninformed of its violation.[81] Therefore, the applicant could claim to be victim of a violation of Article 8 ECHR without proving that he had in fact been the subject of secret surveillance measures.[82]

The fact that *Klass* was allowed to allege a violation of the Convention's rights without proving the he had been the concrete target of the measure at stake plays an essential role, even today. It is not only important in surveillance cases, but also in the context of collective data processing measures where it seems to be impossible for an individual to demonstrate that precisely his/her personal data had been collected or processed.

Additionally the ECtHR declared that secret telephone surveillance and recording constitutes an interference with Article 8 ECHR. It stated that the *mere existence of the legislation* (G-10 Act) itself creates the danger of surveillance. This menace necessarily attacks freedom of communication between users of the postal and

[78] *Klass v. Germany*, Application no. 5029/71, judgment of 6 September 1978.

[79] *Klass v. Germany*, Application no. 5029/71, judgment of 6 September 1978, para 39.

[80] Ibid, paras 33 and 37.

[81] Ibid, paras 36 and 37.

[82] Ibid, para 38.

telecommunication services, and thereby constitutes an interference by a public authority with the exercise of the applicants' right according to Article 8 ECHR.[83]

More recently, the ECtHR confirmed this jurisdiction. In *Liberty and other organisations v. the United Kingdom*, the Court ruled on the lawfulness of the British Communication Act of 1985 which allowed, in principle, the interception of any telecommunication outside the British Islands between 1990 and 1997.[84] The applicant organisations alleged that during the period in question, their telephone, facsimile, e-mail and data communications (including legally privileged and confidential information) were intercepted by an electronic test facility operated by the British Ministry of Defence. Moreover, under the 1985 Act, the authorities had wide discretion to decide which communications (out of the total volume of those physically captured) were listened to or read. Indeed, section 6 of the 1985 Act obliged the Secretary of the State to make "arrangements" to ensure safeguards against abuse of power in the selection process for the examination, dissemination and storage of intercepted material, but those "arrangements" had not been contained in legislation, or otherwise made available to the public.[85] The ECtHR reiterates its finding in *Klass v. Germany* that the mere existence of secret monitoring legislation constitutes a threat of observation for all people who might be affected by this legislation.[86] This threat strikes at the guarantees of Article 8 ECHR and thereby amounts in itself to an interference, irrespective of any measures in fact taken against them.[87]

It is noteworthy in this context that the use of undercover agents to obtain information does not necessarily constitute an interference with Article 8 ECHR, as individuals engaged in a criminal act must therefore be aware that they are running the risk of encountering an undercover police officer whose task would, in fact, be to expose them.[88]

Yet, in general, the *mere existence of legislation* which allows secret monitoring constitutes an interference by a public authority, within the meaning of Article 8 ECHR. However, where the actual fact that interception has taken place is alleged and contested, the ECtHR requires applicants to demonstrate a "reasonable likelihood" that the measures had been actually applied to them.[89]

---

[83] Ibid, para 41.

[84] *Liberty and others v. the United Kingdom*, Application no. 58234/00, judgment of 1 July 2008, para 64.

[85] Ibid, para 66.

[86] *Liberty and others v. the United Kingdom*, Application no. 58234/00, judgment of 1 July 2008, para 56; see also: *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006, para 78.

[87] *Liberty and others v. the United Kingdom*, Application no. 58234/00, judgment of 1 July 2008, para 56.

[88] *Lüdi v. Switzerland*, Application no. 12433/86, judgment of 15 June 1992, para 40.

[89] *Halford v. the United Kingdom*, Application no. 20605/92, judgment of 25 June 1997, para 58, and *Kennedy v. the United Kingdom*, Application no. 26839/05, judgment of 18 May 2010, para 123.

In addition to the existence of monitoring legislation, implementation measures, such as the installation of wiretapping instruments in an individual's house,[90] in a prison, (or prison cell)[91] or at the workplace,[92] or the interception of telephone calls,[93] interferes with the right to respect private life.[94] Legislation permitting public authorities to examine and monitor mail, telegraphic messages,[95] as well as the interception (unwanted listening) or monitoring of pager messages[96] or of workplace telephone or internet usage[97] moreover amounts to an interference with Article 8 ECHR.

(2) Unwanted Watching and Recording in Public and Private Places

Unwanted watching and recording in private or public places can also interfere with the right to respect for private life.[98] However, the latter will only interfere with Article 8 ECHR if the movements of the person concerned are recorded.[99] There are several cases in which the ECtHR was faced with the question as to whether monitoring or recording in public places constitutes an interference with Article 8 ECHR.

---

[90] *Chalkley v. the United Kingdom*, Application no. 63831/00, judgment of 12 June 2003, para 24; *Lewis v. the United Kingdom*, Application no. 1303/02, judgment of 25 November 2003, para 18; *Khan v. the United Kingdom*, Application no. 35394/97, judgment of 12 May 2000, paras 25–28, and *Armstrong v. the United Kingdom*, Application no. 48521/99, judgment of 16 July 2002, para 19; *Hewitson v. the United Kingdom*, Application no. 50015/99, judgment of 27 May 2003, para 20; *Huvig v. France*, Application no. 11105/84, judgment of 24 April 1990, para 25; *Klass and others v. Germany*, Application no. 5029/71, judgment of 6 September 1978, para 41; *Malone v. the United Kingdom*, Application no. 8691/79, judgment of 2 August 1984, para 64; *Valenzuela Contreras v. Spain*, Application no. 27671/95, judgment of 30 July 1998, para 46.

[91] *P.G. and J.H. v. the United Kingdom*, Application no. 44787/98, para 60 of 25 September 2001; *Allan v. the United Kingdom*, Application no. 48539/99, para 35 of 5 November 2002; *Wood v. the United Kingdom*, Application no. 23414/02, para 33 of 16 November 2004 and *Doerga v. Netherlands*, Application no. 50210/99, para 43 of 27 April 2004.

[92] *Kopp v. Switzerland*, Application no. 23224/94, judgment of 25 March 1998, para 50; *Halford v. the United Kingdom*, Application no. 20605/92, judgment of 25 June 1997, paras 44 and 45, and *Amann v. Switzerland*, Application no. 27798/95, judgment of 16 February 2000, para 45.

[93] *Kopp v. Switzerland*, Application no. 23224/94, judgment of 25 March 2003, para 53.

[94] Moreham (2008), pp. 44, 53.

[95] *Klass and others v. Germany*, Application no. 5029/71, judgment of 6 September 1978, para 41.

[96] *Taylor-Sabori v. the United Kingdom*, Application no. 47114/99, judgment of 22 October 2002, para 19.

[97] *Copland v. the United Kingdom*, Application no.62617/00, judgment of 3 April 2007, para 42.

[98] *Allan v. the United Kingdom,* Application no. 48539/99, judgment of 5 November 2002, para 35; *Khan v. the United Kingdom*, Application no. 35394/97, judgment of 12 May 2000, paras 26–28.

[99] Moreham (2008), pp. 44, 54. For video surveillance in public places by public authorities, see also: Opinion on video surveillance in public places by public authorities and the protection of human rights, adopted by the Venice Commission at its 70th plenary session (16–17 March 2007), Study no. 404/2006, Council of Europe, Strasbourg, 23 March 2007.

In *Perry v. the United Kingdom*, the court made a distinction between, "...the monitoring of the actions of an individual in a public place by the use of photographic equipment which does not record the visual data [...] and the recording of the data and the systematic or permanent nature of the record."[100] Only the latter constituted an interference with the individual's private life.

In *P.G. and J.H. v. the United Kingdom*, a recording of the applicants' voices was made while they answered questions in a public area of a police station as police officers listened to them.[101] This recording was made for further analysis and therefore it was regarded as the processing of personal data about them amounting to an interference with their right to respect for their private life.[102] The ECtHR emphasised that, "There are a number of elements relevant to a consideration of whether a person's private life is concerned by measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations[103] as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character."

Private-life concerns may arise, however, if any systematic or permanent record comes into existence of such material from the public domain.[104]

Regardless of the restriction to the recording requirement and the reduced privacy expectation in public places, the ECtHR recognises that there is, "... a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life."[105]

In *Peck v. the United Kingdom*, the disclosure to the media for broadcast use of video footage of the applicant whose suicide attempt was filmed on CCTV

[100] *Perry v. the United Kingdom*, Application no. 63737/00, judgment of 17 July 2002, para 38. See also para 41: "Whether or not he was aware of the security cameras running in the custody suite, there is no indication that the applicant had any expectation that footage was being taken of him within the police station for use in a video identification procedure and, potentially, as evidence prejudicial to his defence at trial. [...] The permanent recording of the footage and its inclusion in a montage for further use may therefore be regarded as the processing or collecting of personal data about the applicant."

[101] *P.G. and J.H. v. the United Kingdom*, Application no. 44787/98, judgment of 25 September 2001.

[102] *P.G. and J.H. v. the United Kingdom*, Application no. 44787/98, judgment of 25 September 2001, para 59.

[103] To the term "reasonable expectations" see Gómez-Arostegui (2005), pp. 153–200.

[104] *P.G. and J.H. v. the United Kingdom*, Application no. 44787/98, judgment of 25 September 2001, para 57.

[105] *P.G. and J.H. v. the United Kingdom*, Application no. 44787/98, judgment of 25 September 2001, para 56. See also: *Peck v. the United Kingdom*, Application no. 44647/98, judgment of 28 January 2003, para 57; *Von Hannover v. Germany*, Application no. 59320/00, judgment of 24 June 2004, para 50, and *Sciacca v. Italy*, Application no. 50774/99, judgment of 11 January 2005, para 29.

cameras,[106] amounted to an interference with the applicant's private life, despite the fact that he was filmed in a public place at the time of the attempt.[107]

To determine to what degree the state has interfered with Article 8 ECHR in cases involving the surveillance of public places, the ECtHR distinguishes between surveillance for security reasons and surveillance for unpredictable other reasons.[108] When deciding whether unwanted watching in public places represents an interference with Article 8 ECHR, the forseeability of the use of the surveillance measure is of fundamental importance. The more the person concerned expects not to be monitored in public, the more seriously the person's rights are abridged.

As regards the use of new techniques for surveillance, the question of whether the use of a Global Positioning System (GPS)[109] to track the movements of suspects in the public sphere constitutes an interference, was recently subject to the case *Uzun v. Germany*.[110] The applicant, Mr. *Uzun*, was suspected of having participated in bomb attacks for which an organisation pursuing the armed combat of the Red Army Fraction had claimed responsibility. For surveillance purposes, a GPS receiver had been built into the car of the applicant's accomplice to observe his and *Uzun's* movement. The data collected via GPS surveillance were later used in trial against both. The ECtHR first noted that the collection of data on the applicant to obtain information on the movements of the applicant and his accomplice interfered with their rights protected by Article 8 (1) ECHR.[111] Surveillance via GPS leads to the systematic collection and storage of data revealing in this case the

[106] Close circuit television cameras.

[107] *Peck v. the United Kingdom*, Application no. 44647/98, judgment of 28 January 2003. It is noteworthy that the protection of correspondence within Article 8 ECHR extends to all types of communication, whether or not taking place in a private, public or in professional context. The ECtHR stipulated that Article 8 ECHR does not use, as it does for the word "life", any adjective to qualify the word "correspondence", therefore no such distinction is made. See *Niemietz v. Germany*, Application no. 13710/88, judgment of 16 September 1992, para 32. In this context, opening and censoring prisoner's correspondence constitutes an interference with the right to respect for correspondence according to Article 8 ECHR.

[108] *Wisse v. France*, Application no. 71611/01, preliminary objection of 20 December 2005, para 26; *Perry v. the United Kingdom*, Application no. 63737/00, judgment of 17 July 2002, paras 41–42; *Peck v. the United Kingdom*, Application no. 44647/98, judgment of 28 January 2003, paras 59–62.

[109] GPS is defined as "a radio navigation system working with the help of satellites. It allows the continuous location, without lapse of time, of objects equipped with a GPS receiver anywhere on earth, with a maximum tolerance of 50 metres at the time. It does not comprise any visual or acoustical surveillance. As opposed to transmitters, its use does not necessitate the knowledge of where approximately the person to be located can be found.", compare *Uzun v. Germany*, Application no. 35623/05, judgment of 2 September 2010, para 13.

[110] *Uzun v. Germany*, Application no. 35623/05, judgment of 2 September 2010, paras 41–53.

[111] The GPS receiver was placed into a car belonging to a third person (*Uzun's* accomplice) and not into the applicant's car, however, the use of the GPS receiver to obtain information on both suspects consequently constituted an interference with the rights of both, *Uzun v. Germany*, Application no. 35623/05, judgment of 2 September 2010, paras 49–50.

applicant's whereabouts and movements in public places.[112] The data were further used to establish patterns on the applicant's movements. The Court argued that, although the GPS surveillance "is by its very nature to be distinguished from other methods of visual or acoustical surveillance which are, as a rule, more susceptible of interfering with a person's right to respect for private life, because they disclose more information on a person's conduct, opinions or feelings", the systematic collection and storage of data disclosing the whereabouts and movements, mentioned above, amounted to an interference.[113]

In conclusion, unwanted watching and recording in private or public places can interfere with the right to respect for private life. It has to be clarified that whereas recording of the movements of the individual concerned may represent (under the conditions mentioned above) an interference[114] – the use of security cameras per se, whether in public streets or on premises where they serve a legitimate and foreseeable purpose, does not amount to an interference with Article 8 ECHR.[115]

(3) Unwanted Publishing of Personal Information

The unwanted publishing of information principally concerns two problems: the publication of images and the unwanted release of medical information.

The obligation includes the responsibility of the Member States to abstain from the release of pictures of individuals. The ECtHR developed three criteria to assess if disseminating images interferes with Article 8 ECHR: In the above mentioned cases *Peck v. the United Kingdom* and *Perry v. the United Kingdom* the Court asks firstly if publication of the applicant's photos was foreseeable at the time of recording.[116] Secondly, in the *Peck* case, the ECtHR also takes the mental condition of the applicant into consideration. It emphasised that he, ". . .was in a public street but he was not there for the purposes of participating in any public event and he was not a public figure. It was late at night, he was deeply perturbed and in a state of distress."[117] Finally the

[112] *Uzun v. Germany*, Application no. 35623/05, judgment of 2 September 2010, para 51.

[113] *Uzun v. Germany*, Application no. 35623/05, judgment of 2 September 2010, para 52.

[114] In *Friedl v. Austria*, Application no. 15225/89, judgment of 31 January 1995, para 48, the Commission stressed three factors when assessing if there was an interference with Article 8 in a case concerning a photograph taken on a demonstration: "*whether the taking of photographs amounted to an intrusion into the individual's privacy*, *whether it related to privacy matters or public incidents*, *and whether the material thus obtained was envisaged for a limited use or was likely to be made available to the general public*".

[115] *Perry v. the United Kingdom*, Application no. 63737/00, judgment of 17 July 2002, para 40.

[116] *Peck v. the United Kingdom*, Application no. 44647/98, judgment of 28 January 2003, para 62, and *Perry v. the United Kingdom*, Application no. 63737/00, judgment of 17 July 2002, para 38.

[117] *Peck v. the United Kingdom*, Application no. 44647/98, judgment of 28 January 2003, para 62, further, the ECtHR adds: "While he was walking in public wielding a knife, he was not later charged with any offence. The actual suicide attempt was neither recorded nor therefore disclosed. However, footage of the immediate aftermath was recorded and disclosed by the Council directly to the public in its CCTV News publication. In addition, the footage was disclosed to the media for

ECtHR assesses the way in which the images were taken. All in all, the foreseeability of the recording, the circumstances and the way in which images are recorded must be considered when publishing images of a person in public.

As to the disclosure of medical information, as a general rule, release of such information usually constitutes an interference with Article 8 ECHR due to the high sensitivity of the information at stake.[118] Dissemination of medical records without the consent of the person concerned during court proceedings, for instance, clearly interferes with the right to private life, as the release of such information widens the circle of people acquainted with the details of a disease, making it possible that very private information comes into the public sphere.[119]

With regard to the notion of "publication", the ECHR Commission[120] noted in *Lupker v. Netherlands* that if photographs were kept in police or other official archives, and were used exclusively for the purpose of the identification of the offenders in the criminal proceedings against the applicants, and there was no suggestion that they have been made available to the general public or used for any other purpose, then they were not taken in a way which constitutes an intrusion upon the applicant's privacy.[121]

Generally, if the state decides to publish photos or video material of individuals, it has to pay attention to the circumstances in which the material was taken, the foreseeability of publication at the time of recording and the situation in which the individuals concerned were filmed.

bb) The Right to Be Free from Gathering, Collection, Use and Storing of Personal Information

(1) Gathering, Use and Storing of Personal Information

The first case that is classified as one of the key cases in developing a right to data protection within the framework of Article 8 ECHR while being part of the right to

further broadcasting and publication purposes. Those media included the audiovisual media [. . .] The applicant's identity was not adequately, or in some cases not at all, masked in the photographs and footage so published and broadcast. He was recognised by certain members of his family and by his friends, neighbours and colleagues".

[118] See for instance, medical data published in newspapers or court proceeding: *Panteleyenko v. Ukraine*, Application no. 11901/02, judgment of 29 June 2006, paras 56–58; *Z. v. Finland*, Application no. 22009/93, judgment of 25 February 1997, para 71; *M.S. v. Sweden*, Application no. 20837/92, judgment of 27 August 1997, paras 33–35; *C.C. v. Spain*, Application no. 1425/06, judgment of 6 October 2009, para 26.

[119] *Panteleyenko v. Ukraine*, Application no. 11901/02, judgment of 29 June 2006, paras 56–58.

[120] Before the entry into force of Protocol No. 11 in 1998 which changed, amongst other, the procedural framework of the ECtHR, the ECHR was also overseen by a Commission which decided on the admissibility of complaints by individuals; it is referred to as ECHR Commission in the following.

[121] *Lupker v. Netherlands*, Application no. 18395/91, judgment of 7 December 1992, para 5.

respect for private life, is a case dealing with the storing and usage of personal information.[122] In *Leander v. Sweden*, the applicant started to work as a temporary replacement in a post of museum technician at the naval museum on a Swedish military base. After a few days of working he was told to leave his workplace as the employer obtained secret information from the Swedish secret service. After this termination, the applicant requested to be informed of the exact reasons for his sudden dismissal, but they were withheld.

The ECtHR stated in 1987, "It is uncontested that the secret police-register contained information relating to Mr. Leander's private life. Both the *storing and the release* of such information, which were coupled with a refusal to allow Mr. Leander an opportunity to refute it, amounted to an interference with his right to respect for private life as guaranteed by Article 8 § 1."[123]

In subsequent cases, the ECtHR confirms this interpretation by reiterating that, "...both the storing by a public authority of information relating to an individual's private life and the use of it," amount to interference with Article 8 ECHR, even if the information contained no sensitive information and had possibly never been consulted.[124] In connection with the increasing storing of telecommunications data,[125] the ECtHR regularly refers to the *Amann v. Switzerland* case, and clarified for instance in *Copland v. the United Kingdom* that the collection and storage of telephone data, especially the numbers dialled, as well as information relating to e-mail and internet usage, without the knowledge of the persons concerned, also interferes with Article 8 ECHR.[126]

Even where personal information has not been collected by any intrusive or secret means, these files nevertheless fall within the scope of Article 8 ECHR.[127] In *P.G. and J.H. v. the United Kingdom* the ECtHR takes into consideration the definition of data within Convention No. 108. Article 2 Convention No. 108 classifies personal data as, "any information relating to an identified or identifiable individual."[128] Then the Court refers to the case *Amann v. Switzerland*, where the storing of information about the applicant on a card in a file was found to be an

[122] *Leander v. Sweden*, Application no. 9248/81, judgment of 26 March 1987.

[123] *Leander v. Sweden*, Application no. 9248/81, judgment of 26 March 1987, para 48 (emphasis added).

[124] *Amann v. Switzerland*, Application no. 27798/95, judgment of 16 February 2000, para 65, and *Panteleyenko v. Ukraine*, Application no. 11901/02, judgment of 29 June 2006, para 56; *S. and Marper v the United Kingdom*, Application nos. 30562/04 and 30566/04, judgment of 4 December 2008, para 67.

[125] For instance through the Date Retention Directive, compare Chap. D III 1.

[126] *Copland v. the United Kingdom*, Application no. 62617/00, judgment of 3 April 2007, para 44.

[127] *P.G. and J.H. v. the United Kingdom*, Application no. 44787/98, judgment of 25 September 2001, para 57. The Court refers to the case *Rotaru v. Romania*, Application no. 28341, judgment of 4 May 2000, paras 43–44.

[128] *P.G. and J.H. v. the United Kingdom*, Application no. 44787/98, judgment of 25 September 2001, para 57.

interference with Article 8 ECHR, although it contained no sensitive information, and had possibly never been consulted.[129]

In addition to the storing of communication information, the retention of *cellular samples*, *DNA profiles* and *fingerprints* constitutes an interference with the right to respect for private life. Since *Mc Veigh and others v. the United Kingdom*, the question of whether the retention of fingerprints alone amounts to an interference was highly controversial.[130] At that time, the question was left open by the ECtHR. A subsequent decision did not recognise the retention of fingerprints as an interference with Article 8 ECHR.[131] Recently, in *S. and Marper v. the United Kingdom* the ECtHR clarified that fingerprints contain exclusive information about an individual allowing for precise identification in a wide range of circumstances.[132] Retention of this information without the consent of the individual concerned cannot be regarded as neutral or irrelevant.[133] Accordingly, the ECtHR considered, "...that the retention of fingerprints on the authorities' records in connection with an identified or identifiable individual may in itself give rise, notwithstanding their objective and irrefutable character, to important private-life concerns."[134]

Finally, both the retention of cellular samples and DNA profiles on the one hand, and the retention of fingerprints on the other, constitutes an interference.[135]

The different methods of gathering and collecting personal information may also interfere with the right to private life.[136] Files or data gathered by security services or other authorities of the state,[137] as well as the metering and subsequent transfer of data obtained in this way to public authorities,[138] constitutes an interference with the right to respect for private life.

---

[129] *Amann v. Switzerland*, Application no. 27798/95, judgment of 16 February 2000, paras 65–67.

[130] *Mc Veigh and others v. United Kingdom*, Application no. 8022/77, Commission decision of 18 March 1981.

[131] *Kinnunen v. Finland*, Application no. 18291/91, Commission decision of 13 October 1993.

[132] *S. and Marper v the United Kingdom*, Application nos. 30562/04 and 30566/04, judgment of 4 December 2008, para 84; see also Beattie (2009).

[133] *S. and Marper v the United Kingdom*, Application nos. 30562/04 and 30566/04, judgment of 4 December 2008, para 84.

[134] *S. and Marper v the United Kingdom*, Application nos. 30562/04 and 30566/04, judgment of 4 December 2008, para 85.

[135] *S. and Marper v the United Kingdom*, Application nos. 30562/04 and 30566/04, judgment of 4 December 2008.

[136] *Leander v. Sweden*, Application no. 9248/81, judgment of 26 March 1987, para 48; *S. and Marper v. the United Kingdom*, Application nos. 30562/04 and 30566/04, judgment of 4 December 2008, para 67; Siemen (2006), p. 135 et seq.

[137] *Amann v. Switzerland*, Application no. 27798/95, judgment of 16 February 2000, para 65; *Panteleyenko v. Ukraine*, Application no. 11901/02, judgment of 29 June 2006, para 56; *Z. v Finland*, Application no. 22009/93, judgment of 25 February 1997 and *Rotaru v. Romania*, Application no. 28341/954, judgment of 4 May 2000.

[138] *Malone* v. *the United Kingdom*, Application no. 8691/79, judgment of 2 August 1984, para 84.

Further, the ECtHR deals with (restricted) disclosure of sensitive data and systematic collection and storage of information by public authorities.[139] In this context, even public information can fall within the scope of private life, "...where it is systematically collected and stored in files held by the authorities".[140]

(2) Transfer of Personal Data

Inextricably linked with the storing of personal data is the subsequent use, and in some cases, the transfer of information obtained. In *Malone v. the United Kingdom*, the British post office, and the British Telephone Company, respectively, made use of a "meter check", a device which registers the numbers dialed and the time and duration of the call on a particular telephone, to collect telephone data. These data were released to the British police without the consent of the subscriber. The ECtHR stated that, "...the Court does not accept [...] that the use of data obtained from metering, whatever the circumstances and purposes, cannot give rise to an issue under Article 8. The records of metering contain information, in particular the numbers dialed, which is an integral element in the communications made by telephone." Consequently, release of that information to the police without the consent of the subscriber also amounted to an interference with the right to private life.[141]

Another type of interference is the transfer of medical records containing highly personal and sensitive data to other authorities. The ECtHR refers to the purpose limitation principle in this context. Disclosing medical data to another authority without the patient's consent interferes with Article 8 ECHR even though the information may remain confidential.[142] In *M.S. v. Sweden* a patient's records had been transferred to another office due to the fact that the applicant enacted a compensation claim.[143] The ECtHR held that the transfer of the medical information to the authority responsible for compensation claims did not serve the same purpose as the storing of the information in question to assure medical treatment at the clinic. The fact that the applicant had sought treatment at a clinic did not mean that she would consent to the data being disclosed to another authority, or to a wider circle of public servants.[144] By initiating compensation proceedings against the alleged violation, the applicant does not waive his/her right to confidentiality.[145]

The next decision refers to the transmission of data to other authorities and contains important statements relating to the aforementioned context of the

[139] *Z. v. Finland*, Application no. 22009/93, judgment of 25 February 1997 and *Rotaru v. Romania*, Application no. 28341/954, judgment of 4 May 2000.

[140] *Rotaru v. Romania*, Application no. 28341/954, judgment of 4 May 2000, para 43; *Panteleyenko v. Ukraine*, Application no. 11901/02, judgment of 29 June 2006, para 56.

[141] *Malone v. the United Kingdom*, Application no. 8691/79, judgment of 2 August 1984, para 84.

[142] *M.S. v. Sweden*, Application no. 20837/92, judgment of 17 August 1997, para 35.

[143] *M.S. v. Sweden*, Application no. 20837/92, judgment of 17 August 1997.

[144] Ibid, para 35.

[145] Ibid, para 32.

cooperation between the different AFSJ actors. In *Weber and Saravia v. Germany*, the ECtHR was faced with an amendment of the German G 10 act extending the powers of the Federal Intelligence Service with regard to the recording of telecommunications in the course of so-called strategic monitoring, as well as the use of personal data obtained thereby, and their transmission to other authorities.[146] Whereas the same legislation, in its initial version, was already the subject of the case *Klass v. Germany*, the ECtHR goes a step further than in this earlier judgment. While reiterating the acceptance of an interference through the mere existence of monitoring legislation, it additionally holds that the *transmission of data* to other authorities and the *subsequent use by them* enlarges the group of individuals with knowledge of the personal data intercepted and can therefore lead to investigations being instituted against the persons concerned.[147] This danger constitutes a *further separate interference* with the applicants' rights under Article 8 ECHR.[148]

cc) Summary of Interferences Within the Framework of Negative Obligations

Summarising, within the scope of negative obligations, the following activities constitute a separate interference with Article 8 ECHR:

- Measures of secret surveillance and recording (e.g. *Klass v. Germany* and *Liberty and others v. the United Kingdom*);
- The mere existence of monitoring legislation (e.g. *Klass v. Germany*);
- The implementation measures of monitoring legislation, such as the installation of wiretapping instruments in an individual's house, in a prison or prison cell, or at the workplace, or the interception of telephone calls (e.g. *Khan v. the United Kingdom* or *Kopp v. Switzerland*);
- The interception via GPS, (*Uzun v. Germany*);
- The recording of a person's voice for further analysis (e.g. *P.G. and J.H. v. the United Kingdom*);
- The unwanted watching and recording in private or even public places, in the latter case, only if recorded (e.g. *Perry v. the United Kingdom*). General rule: The more the person concerned expects not to be monitored in public, the more serious the interference;
- The dissemination of photos or videos if not foreseeable at the time of shooting (e.g. *Peck v. the United Kingdom*): the circumstances in which the material was taken, the foreseeability of dissemination at the time of recording and the situation in which the persons concerned were photographed/filmed have to be taken into account;

[146] *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006.
[147] Ibid, para 79.
[148] Ibid, para 79.

- The omission to prevent the dissemination of photos or videos taken in a private context (e.g. *Peck v. the United Kingdom*);
- The dissemination of medical records (e.g. *Z. v. Finland*);
- The collection, retention and storing of personal information (including telephone data or information relating to e-mail and internet usage), as well as its release, whereby even public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities (e.g. *Rotaru v. Romania*);
- The retention of cellular samples, DNA profiles and fingerprints (e.g. *Marper v. the United Kingdom*);
- The different methods to gather and to collect personal information (e.g. *Weber and Saravia v. Germany*), and
- The transfer of personal data to third parties (e.g. *Malone v. the United Kingdom* or *Weber and Saravia v. Germany*).

dd) Interferences with Regard to Positive Obligations: The Denying of the Right to Access Personal Data

In the context of positive obligation cases, i.e. cases in which the state interferes with Article 8 ECHR by omitting to do something, the denying of the access to personal data plays an important role.

Personal information such as data stored in public files, data about an individual's early development, medical data, information about risks to one's health resulting from environmental pollution, information permitting to asses risks resulting from participation in nuclear tests or tests including toxic chemicals can contain information which might be of vital interest for individuals concerned.

In this context, the most delicate question for states regarding the right of access is surely the question of releasing information stored in secret security files. In this regard, already in *Leander v. Sweden*, the refusal to allow the applicant an opportunity to refute raised allegations which were based on secret service information amounted to an interference with Article 8 ECHR. In this case, the ECtHR had not yet based its decision on the fact that access had been denied, as shown by its subsequent clarification that the right of access to data kept in secret service files as such is not enshrined in the ECHR, but nevertheless considered it to be a potential element of an interference.[149]

In *C.G. and others v. Bulgaria* the ECtHR elucidates that when a state takes a decision to the detriment of an individual on national security grounds basing itself on secret service information, the person concerned must at least be able to challenge the assertion that national security is at stake.[150] An independent

[149] *Leander v. Sweden*, Application no. 9248/81, judgment of 26 March 1987, paras 48, 59 and 67.
[150] *C.G. and others v. Bulgaria*, Application no. 1365/07, judgment of 24 April 2008, para 40.

authority or court must be able to assess whether the invocation of the concept of national security has no reasonable basis in the facts or reveals an interpretation of national security that is unlawful or contrary to common sense and arbitrary.[151]

Twenty years after the *Leander v. Sweden* decision, in the case *Segerstedt-Wilberg and others v. Sweden* the ECtHR clarified this position by emphasising that the Court considers it as established that the refusal to advise the applicants of the full extent to which information was being kept about them on a security police register amounted to an interference with Article 8 ECHR.[152]

The refusal to grant access to information concerning an individual's origin, medical data or information related to other risks to the individual's health may also interfere with the right to private life.

In one of the first cases related to this question, in *Gaskin v. the United Kingdom* dealing with access to childhood social service records, the ECtHR clearly stipulates that such information is undeniably related to private and family life and that the question of access thereto falls within the scope of Article 8 ECHR. However, it concluded that by refusing the applicant complete access to the records, the United Kingdom can not have "interfered" with Article 8 ECHR. Therefore the Court went directly to the justification and analysed whether there had been a positive obligation for the state to grant access.[153]

Consequently, when it is questionable whether a state has to allow access to personal data, the ECtHR directly examines whether or not such a positive obligation exists and if a fair balance had to be struck between the general interest of the community and the interests of the individual.

With regard to medical data and information related to the risks to an individual's health mentioned above, the Court applies the same approach.[154]

d) Justification

According to Article 8 (2) ECHR, the interference with the right to private life must satisfy three conditions to be considered legal: it must be in accordance with the law, it must pursue one or more of the legitimate aims referred to in paragraph 2 and

[151] Ibid.

[152] *Segerstedt-Wiberg and others v. Sweden,* Application no. 62332/00, judgment of 6 June 2006, para 99.

[153] *Gaskin v. the United Kingdom*, Application no. 10454/83, judgment of 7 July 1989, paras 41–42; see for a similar case: *M.G. v. the United Kingdom*, Application no. 39393/98, judgment of 24 September 2002, para 27.

[154] *Martin v. the United Kingdom*, Application no. 27533/95, admissibility decision of 28 February 1996; *K.H. and others v. Slovakia*, Application no. 32881/04, judgment of 28 April 2009, paras 44–46; *McGinley and Egan v. the United Kingdom*, Application nos. 21825/93 and 23414/94, judgment of 9 June 1998; *Roche v. the United Kingdom*, Application no. 32555/96, judgment of 19 October 2005; *Guerra and others v. Italy*, Application no. 14967/89, judgment of 19 February 1998.

it must be necessary in a democratic society in order to achieve the aim or aims.[155] These aims can be the interests of national security, public safety or the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others. Generally, the ECtHR examines very carefully the question of justification carrying out a detailed proportionality assessment in cases related to data protection issues.

aa) In accordance with the Law

To be in accordance with the law, the interference in question must have some basis in domestic law.[156] In addition, this basis must be adequately accessible: the citizen must be able to have an indication as to whether his behaviour is adequate in the circumstances of the legal rules applicable to a given case.[157] A norm cannot be regarded as a law unless it is formulated with sufficient precision to enable the citizen to regulate his/her conduct: the individual must be able to foresee – if need be with appropriate advice –, to a degree that is reasonable in the situation, the consequences which a given action may entail.[158] The use of indefinite legal terms/concepts does not conflict with Article 8 ECHR as long as they are further defined by "settled case-law" [159] specifying those terms and as long as they are not "deduced from a wide construction of statutory provisions or court decisions".[160] Consequently the impugned measures refer additionally to the quality of law, requiring that the law be accessible to the person concerned, who must moreover be able to foresee its consequences for him.Finally, the measure must be compatible with the rule of law.[161] The notion "in accordance with the law" implies conditions which go well beyond the mere existence of some legal basis in domestic law.[162]

[155] *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006, para 80, *Liberty and others v. the United Kingdom*, Application no. 58234/00, judgment of 1 July 2008, para 58.

[156] The wording in Articles 9, 10 and 11 ECHR differs from the wording "in accordance with the law". In these articles the formulation "prescribed by the law" has been chosen. The ECtHR clarified that both formulations have to be interpreted in an identical way, as a different interpretation could lead to different conclusions in respect of the same interference. See *Silver v. the United Kingdom*, Application no. 5947/72 and others, judgment of 25 March 1983, para 85.

[157] Ovey and White (2006), p. 224.

[158] *Silver v. the United Kingdom*, Application no. 5947/72 and others, judgment of 25 March 1983, paras 85–88.

[159] *Huvig v. France*, Application no. 11105/84, judgment of 24 April 1990, para 28, and *Kruslin v. France*, Application no. 11801/85, judgment of 24 April 1990, para 35.

[160] *Valenzuela Contreras v. Spain*, Application no. 27671/95, judgment of 30 July 1998, para 57, and *Kopp v. Switzerland*, Application no. 23244/94, judgment of 25 March 1998, paras 60 and 73.

[161] *Kopp v. Switzerland*, Application no. 23244/94, judgment of 25 March 1998, para 55.

[162] *Amann v. Switzerland*, Application no. 27798/95, judgment of 16 February 2000, para 55.

(1) Basis in Domestic Law

The ECtHR applies a wide margin of interpretation of the term "law".[163] The expression within the meaning of the ECHR refers back to national law, including rules of public international law applicable in the state concerned.[164] It covers not only statute but also unwritten law.[165] "Law" in the expression "in accordance with the law" has always been understood in its "substantive" sense, not in its "formal" one.[166] Moreover, it includes enactments of lower rank than statues.[167]

Additionally, the Court's power to review compliance with domestic law is limited and it is in the first place for the national authorities, particularly the courts, to interpret and apply that law.[168] However, the limits of this power are not always easy to set.[169] While the ECtHR occasionally examines compliance of the legal basis with domestic law in general, the specific examination remains with national courts.[170]

In the data protection context, a special problem regarding the "extraterritoriality" of the basis in domestic law could arise concerning the monitoring of international wireless telecommunications, i.e. telecommunications "which are not effected via fixed telephone lines, but, for example, via satellite or radio relay links".[171] Signals from foreign countries are monitored by interception sites situated in one state which subsequently uses the collected data for its own purposes.

In *Weber and Saravia v. Germany*, the ECtHR was faced with the question whether such a form of monitoring constitutes a valid statutory basis in domestic law because the interception might have interfered illegally with the sovereignty of the foreign states in which the person being monitored resided.[172] The Strasbourg Court briefly comments that signals emitted from foreign countries are monitored

[163] Siemen (2006), p. 141.

[164] *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006, para 87 (with further references).

[165] *Sunday Times v. the United Kingdom*, Application no. 6538/74, judgment of 26 April 1979, para 47.

[166] *Huvig v. France*, Application no. 11105/84, judgment of 24 April 1990, para 28.

[167] *De Wilde, Ooms and Versyp v. Belgium*, Application no. 2832/66 and others, judgment of 18 June 1997, para 93, and *Huvig v. France*, Application no. 11105/84, judgment of 24 April 1990, para 28: "*In a sphere covered by the written law, the "law" is the enactment in force as the competent courts have interpreted it in the light, if necessary, of any new practical developments*".

[168] *Barthold v. Germany*, Application no. 8734/79, judgment of 25 March 1985, para 48, and *Chappell v. the United Kingdom*, Application no. 10461/83, judgment of 30 March 1989, para 54.

[169] Siemen (2006), p. 141.

[170] See for an exhaustive review of the compliance with domestic law: *Chappell v. the United Kingdom*, Application no. 10461/83, judgment of 30 March 1989, paras 52 et seq.; *Kopp v. Switzerland*, Application no. 23244/94, judgment of 25 March 1998, paras 62 et seq.; or *Craxi v. Italy*, Application no. 25337/94, judgment of 17 July 2003, paras 77 et seq.

[171] *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006, para 88.

[172] *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006, paras 83–88.

by interception sites situated on German territory and the data collected are used in Germany and therefore the territorial sovereignty of foreign States as protected in public international law is not infringed.[173]

(2) Quality of the Law

To specify the first criterion within the justification's examination, the ECtHR developed further criteria, such as compliance with the rule of law as well as accessibility and foreseeability of the legal basis in domestic law.

Compliance with the rule of law not only means a superficial connection to the roots of the rule of law, moreover, the phrase implies – and that follows from the object and purpose of Article 8 – that "there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by paragraph 1 Article 8".[174] Two other criteria with which domestic law has to comply are accessibility and foreseeability.

The first principle usually does not meet major problems. However, for instance the non-publication of a domestic act interferes with the accessibility criterion.[175]

In addition, in case a law confers discretion, it must indicate the scope of that discretion, although the ECtHR recognises "the impossibility of attaining absolute certainty in the framing of laws and the risk that the search for certainty may entail excessive rigidity".[176]

(3) Foreseeability

With regard to data protection, situations in which executive power is exercised in secret are commonly occurring. The threat of arbitrariness is apparent. To comply nonetheless with the requirement of the quality of law, the law's foreseeability plays a key role.[177] Precise formulations which enable an individual to regulate his behavior and to foresee the consequences which a given action may entail – to a degree that is reasonable in the circumstances – are most important.[178] Individuals to whom a law applies must be able to predict its application.

Where the contested measure takes place in secret, the criterion of foreseeability must be seen in this context: The ECtHR emphasises that especially in the context of

---

[173] *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006, para 88.

[174] *Malone v. the United Kingdom*, Application no. 8691/79, judgment of 2 August 1984, para 67.

[175] *Silver v. the United Kingdom*, Application no. 5947/72 and others, judgment of 25 March 1983, para 87.

[176] *Silver v. the United Kingdom*, Application no. 5947/72 and others, judgment of 25 March 1983, para 88.

[177] Siemen (2006), p. 147.

[178] *Sunday Times v. the United Kingdom*, Application no. 6538/74, judgment of 26 April 1979, para 49.

secret measures of surveillance, such as the interception of communications, foreseeability "cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly".[179] But, although in certain situations the foreseeability needs to be restricted, the risks of arbitrariness, especially where an authority vested in the executive is exercised in secret, needs to be taken into account. It is therefore indispensable to have understandable and detailed rules on the interception of telephone conversations, especially in view of the fast technological progress made in this field.[180] It would be contrary to the rule of law, if the domestic law is not sufficiently clear to give the individual adequate protection against arbitrary interference.

The ECtHR has developed the following minimum safeguards in order to avoid abuses of power related to secret measures of surveillance. To comply with the foreseeability requirement, the following conditions must be laid down in the applicable legal basis[181]:

- The nature of the offences which may give rise to an interception order,[182]
- A definition of the categories of people liable to have their telephones tapped,
- A limit on the duration of telephone tapping,
- The procedure to be followed for examining, using and storing the data obtained,
- The precautions to be taken when communicating the data to other parties and
- The circumstances in which recordings may or must be erased or the tapes destroyed.

On the basis of these detailed conditions, the ECtHR examines the quality of law in similar cases.[183] The Court repeatedly emphasised that tapping of telephone

[179] *Weber and Saravia v. Germany*, Application no. 54934/00 Admissibility Decision, para 93 of 29 June 2006; see also: *Malone v. the United Kingdom*, Application no. 8691/79, judgment of 2 August 1984, para 67.

[180] *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006, para 93.

[181] *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006, para 95; these criteria were developed at first in: *Huvig v. France*, Application no. 11105/84, judgment of 24 April 1990, para 34, and *Kruslin v. France*, Application no. 11801/85, judgment of 24 April 1990, para 35.

[182] Whereby the state does not have to set out exhaustively by name the specific offences giving rise to an interception, but "sufficient detail" should be provided of the nature of the offences in question, see *Kennedy v. the United Kingdom*, Application no. 26839/05, judgment of 18 May 2010, para 159.

[183] See *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006, paras 93 and 94, or *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, Application no. 62540/00, judgment of 28 June 2007, para 75: "In the context of covert measures of surveillance, the law must be sufficiently clear in its terms to give citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort its secret and potentially dangerous interference with the right to respect for private life and correspondence [. . .]. In view of the risk of abuse intrinsic to any system of secret surveillance, such measures must be based on a law that is particularly precise. It is essential to

conversations and other forms of interception constitute a serious interference with private life (and correspondence) and must therefore be based on a "law" that is particularly precise.

In *Valenzuela v. Spain* the ECtHR made clear that even a constitutional basis permitting telephone tapping has to comply with the requirements stipulated above.[184] In that case, the only legal basis allowing telephone interception in Spain stemmed from the Spanish Constitution. It did not provide the guarantees developed by the ECtHR case law and there was no implementing provision concretising the broad constitutional standards. Even though the Spanish judiciary had developed criteria filling the gap, the ECtHR criticised that guarantees derived from a wide construction of statutory provisions or court decisions were not sufficient to satisfy the foreseeability requirement as laid down by the ECtHR.[185]

In *Amann v. Switzerland* the ECtHR returned to the detailed criteria and considered that the Swiss legal bases allowing to record telephone calls did not comply with the Court's requirements as the surveillance measures did not contain any "indication as to the persons concerned by such measures, the circumstances in which they may be ordered, the means to be employed or the procedures to be observed".[186]

In *Bykov v. Russia*, the government tried to circumvent the ECtHR principles by arguing that existing regulations on telephone tapping were not applicable to a radio transmitting device and that therefore no judicial authorisation for the use of such a device was required.[187] The ECtHR clearly points out that by using a radio-transmitting device instead of telephone tapping equipment, the degree and the nature of the intrusion involved remain virtually identical and that as a result, the same procedural principles apply equally to the use of radio-transmitting tools.[188] Legislation permitting in general so-called "operative experiments" without regulating any technical monitoring details of radio-transmitting does not satisfy the requirements of the quality of law as understood by the ECtHR.[189]

In addition to secret measures of surveillance, in context of actions concerning national security, the requirement of foreseeability also plays a special role. In the aforementioned case *C.G. and others v. Bulgaria* the emphasis lays on the fact that

have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated [. . .]." To the limits of restriction of the foreseeability criterion, see also: *Antunes Rocha v. Portugal*, Application no. 64330/01, judgment of 31 May 2005, paras 69–80.

[184] *Valenzuela Contreras v. Spain*, Application no. 27671/95, judgment of 30 July 1998, para 60.

[185] Ibid, para 57.

[186] *Amann v. Switzerland*, Application no. 27798/95, judgment of 16 February 2000, para 58. See also, Siemen (2006), p. 148.

[187] *Bykov v. Russia,* Application no. 4378/02, judgment of 10 March 2009, para 77.

[188] Ibid, para 79.

[189] Ibid, paras 77–83.

threats to national security may vary in character and may be unexpected or difficult to define in advance.[190] However, even under such circumstances, the concepts of lawfulness and the rule of law in a democratic society require that a decision taken to the detriment of an individual and affecting fundamental rights is subject to a form of adversarial proceedings before an independent authority or court to effectively examine and analyse the reasons and the relevant evidence on which the decision is based. If needed, appropriate procedural restrictions on the use of classified information could be taken. However, the individual must be able in any case to challenge the assertion that national security is a risk.[191]

The case *Kennedy v. the United Kingdom* entails an interesting argument of the applicant which also matters at EU level: *Kennedy* claimed that the term "serious crime", used in a British act to justify restrictive measures, in particular telephone tapping, is not sufficiently clear and therefore blurs the boundaries of what is foreseeable in terms of the ECHR.[192] In view of the Court, the reference to serious crime seems to comply with the foreseeability requirement, although only under the condition that the term is further explained in the interpretative provisions of the contested act as well as in the act itself.[193] It stipulates: ". . . the reference to serious crime, together with the interpretative clarifications in the Act, gives the citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to secret surveillance measures".[194]

While the linking of the lawfulness of the term "serious crime" to the presence of additional clarifications provided for within the act, seems to indicate that the term "serious crime" alone would probably not meet the terms of the foreseeability criterion of the ECHR, the question remains regrettably unanswered in the end. However, the wording used by the ECtHR supports the conclusion that supplementary explanations are necessary to be in compliance with the foreseeability standard of the ECHR. Without prejudice to the findings in Chaps. B and C, this ECtHR statement should be kept in mind, in particular when considering that almost all EU instruments later discussed make use of the term "serious crime" to justify measures interfering with the right to data protection.

In conclusion, concerning the foreseeability criterion in secret tapping cases the ECtHR lays down detailed model principles with which the parties of the Convention have to comply, regardless of the device used for the wiretapping. In cases where national security is invoked to justify a decision to the detriment of an individual, the ECtHR assures that an independent authority overlooks the evidence at issue.

---

[190] *C.G. and others v. Bulgaria*, Application no. 1365/07, judgment of 24 April 2008, para 40.

[191] Ibid.

[192] *Kennedy v. the United Kingdom*, Application no. 26839/05, judgment of 18 May 2010, para 159.

[193] Ibid.

[194] Ibid.

In contrast to visual or acoustical means of surveillance, the foreseeability requirement in cases in which the authorities made use of a GPS is less strict. In the case *Uzun v. Germany* the surveillance via GPS was found to be less susceptible of interfering with the right to respect for private life than (telephone) tapping.[195] Therefore, the requirement to have the surveillance measure previously ordered by a judge does not apply when using a GPS for surveillance purposes. In this case, the Court agreed that it was sufficient if only the prosecution ordered a suspect's surveillance via GPS.[196] However, other safeguards, such as judicial review, the possibility to exclude evidence obtained from an illegal GPS surveillance and a provision ensuring the respect of the proportionality principle, must have been in place before the surveillance via GPS can be ordered.[197] Moreover, the German Criminal Code provided for the information of the person under surveillance under certain circumstances.[198]

A further restriction applies to the foreseeability criterion where the law confers discretion.[199] According to the ECtHR, a law which confers discretion is not in itself contradictory to the requirement of foreseeability, "provided that the scope of the discretion and the manner of its exercise are indicated with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference [. . .]".[200] In general, the scope of the discretion must be indicated,[201] whereas the definition and interpretation of the scope depend on the issue at stake.[202]

In *Leander v. Sweden*, the ECtHR underlined that, even though the law provided a wide discretion on the national police board as to what information could be entered in the police register, detailed provisions about the "hand out procedure" and about the transfer to other authorities sufficiently assured the applicants rights.[203]

In the case *M.S. v. Sweden* the applicant submitted that the disclosure of her medical records by a clinic had exceeded the request of a public authority,

---

[195] *Uzun v. Germany*, Application no. 35623/05, judgment of 2 September 2010, paras 41–53, compare Sect. II 1 c aa 2.

[196] *Uzun v. Germany*, Application no. 35623/05, judgment of 2 September 2010, para 71.

[197] Ibid, paras 64–74.

[198] Ibid, para 72.

[199] Siemen (2006), p. 146.

[200] *Gillow v. the United Kingdom*, Application no. 9063/80, judgment of 24 November 1986, para 51, and *Amann v. Switzerland*, Application no. 27798/95, judgment of 16 February 2000, para 56.

[201] *Silver and others v. the United Kingdom*, Application no. 5947/72 and others, judgment of 25 March 1983, para 88.

[202] Siemen (2006), p. 146.

[203] "*Furthermore, the Ordinance contains explicit and detailed provisions as to what information may be handed out, the authorities to which information may be communicated, the circumstances in which such communication may take place and the procedure to be followed by the National Police Board when taking decisions to release information*", *Leander v. Sweden*, Application no. 9248/81, judgment of 26 March 1987, para 55.

consequently, too many data concerning the applicant's medical condition had been revealed.[204] Whilst the office had only asked for medical records relating to the time of her injury allegedly sustained at work in 1981, the clinic had produced records covering a period up to 1986. The ECtHR clearly emphasised that the decisive factor in determining the scope of the imparting authority's duty to provide information is the relevance of the information rather than "the precise wording" of the demand.[205] Therefore the interference was found to have a legal basis and to be foreseeable as regards Article 8 paragraph 2 ECHR. While these two cases were decided some time ago, they still express the Court's understanding of a wide discretion conceded to the Member States in discretion cases.

However, as to the limits of discretion, the ECtHR clearly states in *Liberty v. the United Kingdom* that if domestic law confers extensive discretion it has to provide "adequate protection against abuse of power" and "the scope or manner of exercise" of the discretion conferred on the State, e.g. to intercept and examine external communications.[206] In addition, the provisions restricting the discretion have to be accessible to the public.[207] The ECtHR refers to *Weber and Saravia v. Germany* and concludes that it is possible for a State to make public certain details about the operation of a scheme of external surveillance without compromising national security by, amongst others, enacting detailed provisions about the use, storage, communication and destruction of the obtained data.[208] The German legislator provided for rules on storing and destroying of the data involved, such as a 6 month review period whether the data obtained were still necessary to achieve the purpose for which they had been obtained by or transmitted to them.[209] If that was not the case, the relevant data had to be destroyed and deleted from the files or access to them had to be blocked and the destruction had to be recorded in minutes.[210] The legal basis in *Liberty v. the United Kingdom* was not in compliance with these criteria as it did not contain any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying the data obtained and was additionally not set out in a form available to the public.[211]

Summarising, foreseeability can be restricted by the discretion set down in the relevant law. This discretion generally is a wide one. However, two factors have to be taken into account: Firstly, the scope of the discretion, secondly, its limits which have to be clearly defined and which must be accessible to the public.

---

[204] *M.S. v. Sweden*, Application no. 20837/92, judgment of 17 August 1997.

[205] Ibid, para 37.

[206] *Liberty and others v. the United Kingdom*, Application no. 58234/00, judgment of 1 July 2008, para 69.

[207] Ibid, paras 67 and 69.

[208] Ibid, para 68.

[209] Ibid.

[210] Ibid.

[211] Ibid, paras 68 and 69.

Moreover, foreseeability becomes important in context with *collection and storing* of personal data.[212] The ECtHR developed certain minimum requirements with which a domestic legal basis has to comply. In the view of the ECtHR, in *Rotaru v. Romania* the legal basis provided for gathering, recording and archiving of information affecting national security, but it did not lay down any limits on the exercise of those powers.[213] The Court criticised that the Romanian Law did not define the type of information that might be recorded, the categories of people against whom surveillance measures might be taken, the circumstances in which such measures might be taken or the procedure to be followed.[214] In addition it did not contain provisions regulating the age of information held or the length of time for which it might be kept. Further, the contested law did not contain an explicit, detailed provision concerning the persons authorised to consult the files, the nature of the files, the procedure to be followed or the use that might be made of the information thus obtained.[215] Consequently, the ECtHR developed detailed criteria with which domestic law has to comply when regulating the collection and storage of personal information.

As a result, when assessing the quality of law in data protection cases, the foreseeability of the legal basis plays a crucial rule.

For specific cases, the ECtHR developed a catalogue of protective measures. Three different factors have to be basically taken into consideration:

- In the context of *secret measures of surveillance*, for instance in wiretapping cases, the nature of the offences which give rise to an interception order, the categories of people liable to have their telephones tapped, a limit on the duration of the tapping, the procedure to be followed for examining, using and storing the data obtained, rules regulating the transfer of data to other parties and the circumstances in which recordings have to be erased or the tapes destroyed, have to be laid down in the legal basis.
- In case the domestic law provides *discretion*, its scope, its limits as well as the relevance of the information disclosed have to be set out in the national provisions.
- A legal basis regulating *collection and storage* of personal data must include provisions about the type of information that might be recorded, the categories of people against whom surveillance measures might be taken, the circumstances in which such measures might be taken and the procedure to be followed. In addition, it must include provisions regulating the age of information held, the length of time for which this information might be kept, explicit and detailed provisions concerning the *persons authorised to consult the files*, the nature of

[212] Siemen (2006), p. 149.

[213] *Rotaru v. Romania*, Application no. 28341/954, judgment of 4 May 2000, para 57.

[214] Ibid.

[215] Ibid.

the files, the procedure to be followed and the use that might be made of the information thus obtained.

In consequence, when evaluating the foreseeability criterion in data protection cases, the ECtHR developed specific and detailed requirements which have to be fulfilled by the domestic law to be in accordance with the law. *Siemen* assumes that this "technique" sometimes goes beyond the principle of a limited examination power of the ECtHR as regards the abstract interpretation of domestic law.[216] Principally, the Court has to be careful to rule on whether domestic law conformed to the ECHR *in abstracto* – usually its examination competence is limited to the present case.[217] In *Huvig v. France* the ECtHR recognised this problem and states that "since it [the ECtHR] must ascertain whether the interference complained of was "in accordance with the law", it must inevitably assess the relevant French law in force at the time in relation to the requirements of the fundamental principle of the rule of law. Such a review necessarily entails some degree of abstraction. It is none the less concerned with the "quality" of the national legal rules applicable to Mr. and Mrs. Huvig in the instant case".[218]

The Court added that especially tapping and other forms of interception of telephone conversations represent a serious interference with private life and correspondence and must accordingly be based on provisions that are particularly precise.[219] For this reason it would be essential to have clear, detailed rules on the subject, in particular as the technology available for use is constantly becoming more complicated.[220]

bb) Legitimate Aim

After assessing whether the interference is in accordance with the law, the measure at stake has to pursue the legitimate aims of paragraph 2 Article 8 ECHR. These aims are the interest of national security, public safety and the economic well-being of the country as well as the prevention of disorder or crime, the protection of health, morals or the rights and freedoms of others. No final definition of these aims exist, however, the ECtHR acknowledges a wide margin of appreciation to the Member States.[221] In *Z. v. Finland* the ECtHR emphasised that an *ex post facto*

[216] Siemen (2006), p. 150; compare also *Golder v. the United Kingdom*, Application no. 4451/70, judgment of 21 February 1975, para 46.

[217] *Golder v. the United Kingdom*, Application no. 4451/70, judgment of 21 February 1975, paras 39 and 46.

[218] *Huvig v. France*, Application no. 11105/84, judgment of 24 April 1990 para 31; to this problematic, see also: Siemen (2006), p. 150.

[219] *Huvig v. France*, Application no. 11105/84, judgment of 24 April 1990, para 32.

[220] Ibid.

[221] Siemen (2006), p. 151; Meyer-Ladewig (2006), Article 8, p. 180, para 41.

assessment of the legitimate aim does not comply with the Court's requirements by stressing that the legitimate aim has to be evaluated at the time when the contested measures are taken and the relevant authorities sought to achieve a legitimate aim.[222] In the vast majority of the cases, the ECtHR examines the necessity of the interference in much more detail than the legitimate aim, as examining this point permits an exhaustive and sophisticated analysis with regard to the conflicting interests.

cc) Necessary in a Democratic Society

In the following section, it has to be determined whether the means provided under the impugned measure for the achievement of the above mentioned aim remain within the bounds of what is necessary in a democratic society.

At various occasions, the ECtHR has stated its general understanding of the phrase "necessary in a democratic society". In *Silver v. the United Kingdom* clarifies that:

- the adjective "necessary" is not synonymous with "indispensable", neither has it the flexibility of such expressions as "admissible", "ordinary", "useful", "reasonable" or "desirable" [. . .];
- the Contracting States enjoy a certain but not unlimited margin of appreciation in the matter of the imposition of restrictions, but it is for the Court to give the final ruling on whether they are compatible with the Convention [. . .];
- the phrase "necessary in a democratic society" means that, to be compatible with the Convention, the interference must, inter alia, correspond to a "pressing social need" and be "proportionate to the legitimate aim pursued" [. . .].[223]

With regard to Article 8 (2) ECHR, in *Kvasnica v. Slovakia* and *Kennedy v. the United Kingdom* the Court added:

- The Court has to determine whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the interference to what is necessary in a democratic society;
- in addition, the values of a democratic society must be followed as faithfully as possible in the supervisory procedures if the bounds of necessity, within the meaning of Article 8 (2), are not to be exceeded.[224]

Summarising, the ECtHR is in search for a balance between the demands of the general interest of the Member States and the requirements of the protection of the individual's fundamental rights.[225] Member States enjoy a wide *margin of*

[222] *Z. v Finland*, Application no. 22009/93, judgment of 25 February 1997, para 75.

[223] *Silver v. the United Kingdom*, Application no. 5947/72 and others, judgment of 25 March 1983, para 7.

[224] *Kennedy v. the United Kingdom*, Application no. 26839/05, judgment of 18 May 2010, para 154, and *Kvasnica v. Slovakia*, Application no. 72094/01, judgment of 9 June 2009, para 80.

[225] *Soering v. the United Kingdom*, Application no. 14038/88, judgment of 7 July 1987, para 89.

appreciation which is given both to the domestic legislator and to the judicial bodies that are called upon to interpret and apply the law in force.[226] This margin is an expression of judicial self-restraint and a concession to the Member States regarding the principle of the choice of means.[227] However, it is subject to European supervision[228]; therefore the exceptions provided for in paragraph 2 of Article 8 ECHR have to be interpreted narrowly. The scope of this margin depends on such factors as the nature and seriousness of the interests at stake and the gravity of the interference.[229] That means that it varies depending on the circumstances of the case, the subject-matter and its background.[230] In addition, it is not identical as it regards each of the different aims justifying restrictions on paragraph 1 of Article 8 ECHR.[231]

This flexible and casuistic approach implies that there is neither a definition of the margin of appreciation doctrine, nor is there one common academic consensus explaining the content of this principle.[232]

---

[226] *Handyside v. the United Kingdom*, Application no. 5493/72, judgment of 7 December 1976, para 48.

[227] Siemen (2006), pp. 154–155; see more generally to the doctrine of the margin of appreciation: Mowbray (2007), pp. 629–633; Greer (2006), pp. 222–226; Lavender (1997); Brems (1996), Arai-Takahashi (2002); Callewaert et al. (1998); Hutchinson (1999). Critical to this doctrine: Jones (1995); Brauch (2004–2005).

[228] *Funke v. France*, Application no. 10828/84, judgment of 25 February 1993, para 55, and *Kennedy v. the United Kingdom*, Application no. 26839/05, judgment of 18 May 2010, para 154.

[229] *Z. v Finland*, Application no. 22009/93, judgment of 25 February 1997, para 99, and *Peck v. United Kingdom*, Application no. 44647/98, judgment of 28 January 2003, para 77.

[230] *Rasmussen v. Denmark*, Application no. 8777/79, judgment of 28 November 1984, para 40: "The scope of the margin of appreciation will vary according to the circumstances, the subject-matter and its background; in this respect, one of the relevant factors may be the existence or non-existence of common ground between the laws of the Contracting States".

[231] *Dudgeon v. the United Kingdom*, Application no. 7525/76, judgment of 22 October 1981, para 52, and *Sunday Times v. the United Kingdom*, Application no. 6538/74, judgment of 26 April 1979, para 59.

[232] Greer (2006), pp. 222–223; Ovey and White (2006), p. 233; Sottiaux and van der Schyff (2008), pp. 115–156, 134. Due to the vagueness of this doctrine, some argue for the elimination of it, see Partly dissenting opinion of Judge de Meyer in *Z. v Finland*, point III, Application no. 22009/93, judgment of 25 February 1997: In the present judgment the Court once again relies on the national authorities' "margin of appreciation". I believe that it is high time for the Court to banish that concept from its reasoning. It has already delayed too long in abandoning this hackneyed phrase and recanting the relativism it implies. It is possible to envisage a margin of appreciation in certain domains. It is, for example, entirely natural for a criminal court to determine sentence – within the range of penalties laid down by the legislature – according to its assessment of the seriousness of the case. But where human rights are concerned, there is no room for a margin of appreciation which would enable the States to decide what is acceptable and what is not. On that subject the boundary not to be overstepped must be as clear and precise as possible. It is for the Court, not each State individually, to decide that issue, and the Court's views must apply to everyone within the jurisdiction of each State. The empty phrases concerning the State's margin of appreciation – repeated in the Court's judgments for too long already – are unnecessary circumlocutions, serving only to indicate abstrusely that the States may do anything the Court does not consider

However, by applying the margin of appreciation to private life protection cases there is a broad consent on the relationship between the seriousness of the interference, the nature of the rights at stake and the scope accorded to the margin of appreciation[233]: the more intimate or private areas of private life are affected, the narrower the scope of the margin of appreciation acknowledged to the Member States will be.[234] Where there is no common understanding within the Member States of the Council of Europe as to the importance of the interest at stake or as to how best to protect it, the margin will be wider.[235]

The following analysis will show whether this observation remains valid with regard to data protection cases and whether general conclusions can be drawn by analysing the relevant case law. It has to be clarified in advance that a clear division between the categories stipulated in the following will not be possible. The circles of different actions do intersect and overlap since the case law on hand sometimes fits into more than one category.

(1) Retention of Information Relating to Criminal Offences Including Biometric Data[236]

The ECtHR has held that the retention of information related to criminal offences of the past can be necessary in a modern democratic society for the prevention of disorder and crime.[237] Until recently, Member States enjoyed a wide margin of appreciation, not at least because, in the cases examined by the ECtHR in this context, the information obtained was only kept in a general administrative file recording the events in question. The information was not entered into an automatic

incompatible with human rights. Such terminology, as wrong in principle as it is pointless in practice, should be abandoned without delay.

[233] Greer (2006), p. 224.

[234] Siemen (2006), p. 156; Ovey and White (2006), p. 234. See also: *S. and Marper v the United Kingdom*, Application nos. 30562/04 and 30566/04, judgment of 4 December 2008, para 102; *Z. v Finland*, Application no. 22009/93, judgment of 25 February 1997 and *Dudgeon v the United Kingdom*, Application no. 7525/76, judgment of 22 October 1981; *S. and Marper v the United Kingdom*, Application nos. 30562/04 and 30566/04, judgment of 4 December 2008.

[235] *Dickson v. the United Kingdom*, Application no. 44262/04, judgment of 4 December 2007, para 78; *S. and Marper v the United Kingdom*, Application nos. 30562/04 and 30566/04, judgment of 4 December 2008, para 102.

[236] Biometric data are defined in the Article 29 Working Partly, WP 136, Opinion 4/2007 on the concept of personal data, adopted 20 June 2007, pp. 8 and 9, para III (1) as "biological properties, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability. Typical examples of such biometric data are provided by fingerprints, retinal patterns, facial structure, voices, but also hand geometry, vein patterns or even some deeply ingrained skill or other behavioural characteristic (such as handwritten signature, keystrokes, particular way to walk or to speak, etc.)" and DNA information.

[237] *Friedl v. Austria*, Application no. 15225/89, judgment of 31 January 1995, para 66.

data processing system.[238] The ECHR Commission found a relatively slight interference with the applicant's right to respect for his private life in cases related to the keeping of records relating to criminal offences of the past.[239] They could reasonably be considered as necessary in a democratic society for the prevention of disorder and crime. In *Friedl v. Austria* the ECHR Commission concluded that "even if no criminal proceedings are subsequently brought and there is no reasonable suspicion against the individual concerned in relation to any specific offence, special considerations, such as combating organised terrorism, can justify the retention of the material concerned".[240] However, the keeping (and publishing) of an inaccurate police report obviously violates Article 8 ECHR.[241]

It is noteworthy that in *Friedl v. Austria*, the ECtHR attached special weight to the fact that the photographs concerned had not been entered into a data-processing system and that the authorities had taken no steps to identify the persons photographed by means of data processing.[242] *Siemen* argued that from a present day perspective, this argument could no longer serve as justification of the interference, as nowadays almost every database would operate with an automatic data processing system. In view of the various possibilities of collecting, exchanging as well as interlinking or storing data in vast databases, *Siemen* doubted that the ECtHR would decide in the same way which it did 15 years ago. [243]

In *S. and Marper v. the United Kingdom* this observation proved to be true.[244] The applicants opposed the fact that British authorities retained DNA and fingerprint data of them taken during a previous investigation despite the acquittal of one of them and the discontinuance of the criminal proceedings against the other.[245]

On the one hand, the ECtHR recognised the importance of the use of modern scientific techniques of investigation and identification as regards cellular samples, DNA and fingerprint information, on the other hand it underlined the limits of their storage and use. It referred to the principles specified in Convention No. 108 of the

[238] *Friedl v. Austria*, Application no. 15225/89, judgment of 31 January 1995; *X. v. Germany*, Application no. 1307/61, Commission decision of 4 October 1962.

[239] *Friedl v. Austria*, Application no. 15225/89, judgment of 31 January 1995, para 66.

[240] *Friedl v. Austria*, Application no. 15225/89, judgment of 31 January 1995, para 66. The reference to "*special considerations*, *such as combating organised crime*" is astonishing, in particular under the perspective that the defendant state did not refers to this justification. See Siemen (2006), p. 159.

[241] *Cemalettin Canli v. Turkey,* Application no. 22427/04, judgment of 18. November 2008, paras 42–44.

[242] *Friedl v. Austria*, Application no. 15225/89, judgment of 31 January 1995, paras 49–51.

[243] Siemen (2006), p. 159.

[244] *S. and Marper v. the United Kingdom*, Application nos. 30562/04 and 30566/04, judgment of 4 December 2008.

[245] Compare to this case: De Beer et al. (2010).

Council of Europe and laid emphasis on the need for safeguards when automatic processing is concerned, in particular when such data are used for police purposes.[246] It emphasised that statistics on hits between large databases and crime scenes are not sufficient to justify the establishment of such databases as "the figures do not reveal the extent to which this "link" with crime scenes resulted in convictions of the persons concerned or the number of convictions that were contingent on the retention of the samples of unconvicted persons".[247] Nor do they reveal that the high number of successful matches with crime-scene evidence was only achieved "through indefinite retention of DNA records of all such persons".[248]

It stressed that the retention of data must be proportionate in relation to the purpose of collection and insisted on a limited period of storage.[249] England, Wales and Northern Ireland appeared to be the only jurisdictions within the Council of Europe to allow the indefinite retention of fingerprint and DNA material of any person of any age suspected of any recordable offence.[250] The Court was "struck by the blanket and indiscriminate nature of the power of retention in England and Wales".[251] Data were retained irrespective of the nature or gravity of the offence or the age of the suspect, there existed only limited possibilities to have the data removed from the database, additionally there was no provision for independent review of the justification for the retention according to defined criteria (such as the seriousness of the offence, previous arrests, the strength of the suspicion against the person and any other special circumstances).[252] No time limit was provided.[253] This lack of corrective provisions led to the risk of stigmatisation, stemming from the fact that persons in the position of the applicants, who had not been convicted of any offence and are entitled to the presumption of innocence, have their data stored in a law enforcement database while being treated in the same way as convicted persons.[254]

Against this background, the ECtHR found that the retention of the fingerprints, cellular samples and DNA profiles in a nationwide database failed to strike the balance between the competing interests and that the state had overstepped any tolerable margin of appreciation.[255]

---

[246] *S. and Marper v. the United Kingdom*, Application nos. 30562/04 and 30566/04, judgment of 4 December 2008, para 103.

[247] Ibid, para 116.

[248] Ibid.

[249] Ibid, para 107.

[250] Ibid, para 110.

[251] Ibid, para 119.

[252] Ibid.

[253] Ibid.

[254] Ibid, para 122.

[255] Ibid, para 125.

This decision allows the derivation of important general principles as regards the minimum data protection standard in databases serving crime detection and prevention. States must consider the following rules[256]:

- First, the presumption of innocence demands a different treatment of data of persons who have been convicted of an offence and those who have never been.
- A distinction has to be made between serious and less serious offences.
- The age of the suspected has to be taken into account.
- Possibilities to have the data removed from the database have to be established.
- Provisions for independent review of the justification for the retention according to defined criteria, such as the seriousness of the offence, previous arrests, the strength of the suspicion against the person and any other special circumstances, have to assure the lawfulness of the provided measure.
- Finally, retention has to be limited in time.

All in all, the case *S. and Marper v. the United Kingdom* shows an important development towards an increasing awareness and sensibility of the Court vis-à-vis the fast changing technology and the risks resulting from the collection and retention of personal data in modern databases. The mandatory establishment of corrective provisions and procedural rights such as provisions to have the data removed from the database, keep up with the current state of technological possibilities and correct the constrained approach taken in *Friedl v. Austria* 15 years ago.

(2) Data Collection, Storing and Retention with Regard to Measures Against Terrorism and Transmission of Data to Third Parties

One of the first cases dealing with measures regarding legislation enacted against terrorism established basic criteria still applicable in those cases. In the aforementioned judgment *Klass and others v. Germany* from 1978, the German government referred to the protection of national security and the prevention of crime to justify security legislation (G-10 Act) implementing secret mail, post and telephone surveillance.[257] The applicants, lawyers, public prosecutors and judges, claimed

[256] Ibid, paras 66–125.

[257] *Klass v. Germany*, Application no. 5029/71, judgment of 6 September 1978; for measures such as fingerprinting or photographing during detention and/or the retention of records after release do not constitute a breach of Article 8, see *Mc Veigh and others v. United Kingdom*, Application no. 8022/77, Commission decision of 18 March 1981. As regards the notion of "national security", the ECtHR has not yet found a clear Definition. In *C.G. and others v. Bulgaria*, Application no. 1365/07, judgment of 24 April 2008, it admits that: "It is true that the notion of "national security" is not capable of being comprehensively defined (see Esbester v. the United Kingdom, no. 18601/91, Commission decision of 2 April 1993, unreported; Hewitt and Harman v. the United Kingdom, no. 20317/92, Commission decision of 1 September 1993, unreported; and Christie v. the United Kingdom, no. 21482/93, Commission decision of 27 June 1994, DR 78-A, p. 119, at p. 134). It may, indeed, be a very wide one, with a large margin of appreciation left to the executive to

among others that the G-10 Act empowers the authorities to monitor their correspondence and telephone communication without requiring the authorities to subsequently inform the persons concerned of the measures taken against them.[258] After clarifying the notion of victim, the Court accepts that the mere existence of legislation permitting secret measures could interfere with the right of individuals, even if those measures did not in fact apply to them.[259]

In determining whether the interference is justified, the ECtHR bases itself on two facts: Firstly, it recognises the technological progress made in espionage and surveillance techniques.[260] Secondly, it refers to the development of terrorism in Europe in the years before 1978. The ECtHR held that: "Democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction. Therefore, the Court has to accept that the existence of some legislation granting powers of secret surveillance over the mail and telecommunications is, under exceptional conditions, necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime".[261]

Even though this statement was made in 1978, it exemplarily illustrates the Court's understanding with regard to secret surveillance measures and legislation enacted against terrorism. Member States enjoy a wide margin of appreciation relating to the implementation of counter terrorism measures.

The Court, however, restricts its approach to the effect that it is nevertheless aware "of the danger such a law poses of undermining or even destroying democracy on the ground of defending it".[262] It affirms that the Member States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they consider appropriate.[263] It demands adequate and effective guarantees against abuse on the one hand which depend on the other hand "on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering such measures, the authorities competent to permit, carry out and supervise such measures, and the kind of remedy provided by the respective national law".[264] In this case, in the Court's view, the G-10 Act laid down strict conditions regarding the implementation of surveillance measures and

determine what is in the interests of that security. However, that does not mean that its limits may be stretched beyond its natural meaning."

[258] *Klass v. Germany*, Application no. 5029/71, para 26 of 6 September 1978.

[259] Ibid, para 34.

[260] Ibid, para 48.

[261] Ibid.

[262] Ibid, para 49.

[263] Ibid.

[264] Ibid, para 50.

the processing of the information thereby obtained.[265] Subsequent to a detailed examination of the German legislation, the ECtHR concludes that the G-10 Act is justified in the light of paragraph 2 Article 8 ECHR and does not exceed the limits of what is deemed being necessary in a democratic society in the interests of national security and for the prevention of disorder or crime.[266]

Equally related to anti-terrorism measures in the 1970s is the case *A*., *B*., *C*. *and D*. *v*. *Germany*. It concerns the recording and storing of telephone conversations, which the applicants had had with a law firm whose telephone had been tapped, as a lawyer working in this firm was accused of taking active and decisive part in setting up an information centre serving to exchange information between detained persons suspected of terrorist activities as well as disseminating terrorist ideas aimed at violent revolution.[267]

The ECtHR concludes that the storing of telephone records even beyond the actual need and not related to any criminal acts, can be in accordance with Article 8 ECHR since a definite answer with regard to the question of which records would finally be relevant in criminal proceedings could only be given at the end of the process against the suspect.[268] In other words, storing of telephone records during a criminal investigation is justified until the end of the proceedings for which they were originally obtained, whether or not they are related to criminal acts. However, the ECHR Commission took into consideration that the data had been destroyed after the conviction of the suspect and had not been used for any other purpose than remaining available as possible evidence in the proceedings against the suspect.[269]

The wide margin of appreciation of Member States in cases related to the prevention of terrorist crime is also reflected in *Murray v*. *the United Kingdom*.[270] The ECtHR emphasises that "terrorist crime falls into a special category. Because of the attendant risk of loss of life and human suffering, the police are obliged to act with utmost urgency in following up all information [. . .]".[271]

In *Murray v*. *the United Kingdom*, the applicant was arrested and accused of collecting money for the Provisional Irish Republican Army (Provisional IRA).

[265] *Klass v*. *Germany*, Application no. 5029/71, judgment of 6 September 1978, para 52: "The measures in question remain in force for a maximum of three months and may be renewed only on fresh application; the measures must immediately be discontinued once the required conditions have ceased to exist or the measures themselves are no longer necessary; knowledge and documents thereby obtained may not be used for other ends, and documents must be destroyed as soon as they are no longer needed to achieve the required purpose".

[266] *Klass v*. *Germany*, Application no. 5029/71, judgment of 6 September 1978, para 60.

[267] *A*., *B*., *C*. *and D*. *v*. *Germany*, Application no. 8290/78, judgment of 13 December 1979, para 177.

[268] Ibid, para 180.

[269] Ibid.

[270] *Murray v*. *the United Kingdom*, Application no. 14310/88, judgment of 28 October 1994.

[271] Ibid, para 51.

Amongst others, he contested the taking of photographs without his knowledge or consent as well as the recording of personal details concerning his family life.[272] In evaluating the necessity of such information gathering in a democratic society, the ECtHR clarifies that "it is not for the Court to substitute for the assessment of the national authorities its own assessment of what might be the best policy in the field of investigation of terrorist crime".[273] In view of the threats posed by organised terrorism, the ECtHR concludes that neither recording nor retaining basic personal details concerning the arrested person or even other persons present at the time and place of the arrest, nor taking and retention of photographs can be regarded as falling outside the legitimate bounds of the process of investigation of terrorist crime.[274]

In June 2006, almost 30 years after the *Klass* judgment, an amendment of the G-10 Act was again subject-matter before the ECtHR. In this case, *Weber and Saravia v. Germany*, the applicants impugned the legality of four amendments which extended the powers of the secret service, referring to extended strategic monitoring, the transmission and use of personal data to the Federal Government including the Offices for the Protection of the Constitution and other authorities, the destruction of personal data as well as the failure to give notice of restrictions on the secrecy of telecommunications.[275] The ECtHR examined in detail the applicant's complaints and established important basic principles of general application with which states have to comply when extending the powers of their secret services.[276] To be in accordance with Article 8 ECHR specific and particular minimum requirements have to be fulfilled.

The Court observes that before enacting strategic monitoring, a series of restrictive conditions have to be satisfied. Detailed safeguards against abuse have to be established. Examples are: restriction of monitoring measures to a short period of time (3 months), immediate interruption of the measures if the conditions set out in the monitoring order were no longer fulfilled or the measures themselves were no longer necessary, as well as the destruction of data as soon as they were no longer needed to achieve the purpose pursued.[277] Additionally, independent supervision (in this case a parliamentary board and a special commission) empowered with

[272] Ibid, para 84.

[273] Ibid, para 90.

[274] Ibid, para 93.

[275] *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006.

[276] The ECtHR uses the principles outlined in *Weber and Saravia v. Germany* in subsequent cases as a standard of reference when it comes to the assessment of safeguards and guarantees against abuse, see for instance *Kennedy v. the United Kingdom*, Application no. 26839/05, judgment of 18 May 2010, para 158, and *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, Application no. 62540/00, judgment of 28 June 2007, para 86.

[277] *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006, para 114.

substantial power in relation to all stages of interception and the establishment of reporting duties, at least for the Federal Minister authorising monitoring measures, have to be provided.[278] Detailed provisions must regulate storage and destruction of data.[279]

As to the transmission and use of personal data, the ECtHR refers to the contested judgment of the German Federal Constitutional Court which ruled that the transfer of data between the Federal Intelligence Service and the Federal Government could only be accomplished if the personal data contained in the report to the Federal Government were marked and remained connected to the purposes which had justified their collection.[280] These additional safeguards were considered appropriate by the ECtHR for the purpose of limiting the use of the information obtained to what is necessary to serve the purpose of strategic monitoring.[281] With regard to the transmission of personal data to the Offices for the Protection of the Constitution and other authorities and their use by these authorities, the ECtHR found that the German Federal Constitutional Court again adequately counterbalanced the interference by setting reasonable limitations of the offence (s) on behalf of which data transmission was permitted and by providing supervisory mechanisms against abuse.[282] Precautions to be taken when communicating the data to other parties must be laid down in the legal basis allowing for transfer.[283] The German court ordered that, the G-10 could only be applied and data be transmitted if specific facts – as opposed to mere factual indications – aroused the suspicion that someone had committed one of the limited offences listed in a special Article of the G-10 Act.[284] Moreover, the transmission had to be recorded in minutes. Already in *Leander v. Sweden*, the ECtHR referred to the transfer conditions requiring "explicit and detailed provisions as to what information may be handed out, the authorities to which information may be communicated, the circumstances in which such communication may take place and the procedure to be followed" prior to transferring personal data to other authorities.[285]

The ECtHR also takes the view that the provisions for the destruction of data "as soon as they were no longer needed to achieve their statutory purpose, and for the verification at regular, fairly short intervals of whether the conditions for such destruction were met", constituted an important element in reducing the effects of

[278] Ibid, para 115.

[279] Ibid, para 116.

[280] Ibid, para 121.

[281] Ibid, para 122.

[282] Ibid, para 129.

[283] *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006, para 95, and *Kennedy v. the United Kingdom*, Application no. 26839/05, judgment of 18 May 2010, para 144.

[284] *Weber and Saravia*, Application no. 54934/00, admissibility decision of 29 June 2006, para 127.

[285] *Leander v. Sweden*, Application no. 9248/81, judgment of 26 March 1987, para 55.

the interference with the secrecy of telecommunications to an unavoidable minimum. Moreover, the Federal Constitutional Court ruled that data which were still needed for the purposes of court proceedings could not be destroyed immediately and that the supervisory powers of the independent G-10 Commission covered the whole process of using data, including their destruction".[286]

Concerning the subsequent notification of surveillance measures, the ECtHR emphasises that this question is closely linked to the effectiveness of remedies before the courts and therefore to the existence of effective safeguards against the abuse of monitoring powers.[287] It adds: "As soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, [...], information should be provided to the persons concerned".[288]

In conclusion, the ECtHR found that adequate and effective guarantees existed against abuses of the State's strategic monitoring powers in the G-10 Act.[289]

In *Weber and Saravia v. Germany* the ECtHR established detailed principles with which the states have to comply when enacting legislation on combatting terrorism or other serious crime. The decision's essential requirements for compliance with Article 8 ECHR include independent control of the surveillance measures and of the data obtained through it, adequate procedures for preserving the data's integrity and confidentiality as well as procedures for its destruction, adequate remedies in case of misuse, independent control and information of the persons concerned after the termination of such measures. Whereas the ECtHR had already carefully examined the G-10 legislation in *Klass and others v. Germany*, in *Weber and Saravia v. Germany* it clearly summarized the most important principles to be respected when setting up anti-terrorism legislation.[290] Cases such as *Kennedy v. the United Kingdom* and *Kvasnica v. Slovakia* later confirmed the standards outlined in this judgment.[291]

Summarising the relevant case law, relatively serious interferences regarding data collection, storing or retention can be justified on the grounds of the establishment of legislation against terrorism, the prevention of crime and the protection of

[286] *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006, para 132.

[287] "since there is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively", Weber and Saravia v. Germany, Application no. 54934/00, admissibility decision of 29 June 2006, para 135.

[288] *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006, para 135.

[289] Ibid, para 137.

[290] For a breach of these principles, see *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, Application no. 62540/00, judgment of 28 June 2007 and *Volokhy v. Ukraine*, Application no. 23543/02, judgment of 2 November 2006.

[291] *Kennedy v. the United Kingdom*, Application no. 26839/05, judgment of 18 May 2010 and *Kvasnica v. Slovakia*, Application no. 72094/01 of 9 June 2009.

national security. On the one hand, the ECtHR acknowledges a wide margin of appreciation to the Member States in this respect, on the other hand it demands adequate and effective guarantees against abuse which are examined in detail and require relatively far reaching protection, including rules on the transmission of personal data.

(3) Surveillance Measures

The ECtHR's assessment in *Klass v. Germany* not only refers to data processing with regard to measures against terrorism, it also sets general principles pertaining to cases related to governmental secret surveillance measures.[292] Both aims are often closely connected and therefore can not be clearly distinguished. The ECtHR clearly points out that powers of secret surveillance "characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions".[293] Putting the emphasis on the wording "strictly necessary", this statement suggests a strict interpretation of the reasons for justification.[294] However, it is rather a question of whether the two factors mentioned above (technical advances and threat of terrorism) are sufficiently balanced with regard to effective and adequate safeguards provided by the Member States.[295] This evaluation depends on all the circumstances of the case, for instance the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law in question.[296] As a basic rule, "exploratory or general surveillance" goes beyond what is necessary in a democratic society.[297]

The ECtHR acknowledges a certain discretion in determining the conditions under which the system of surveillance may be operated.[298] Domestic legislation may be adapted to increasing threats and can therefore justify even serious interferences. The ECtHR refers to the *Golder*, *Handyside* and *De Wilde and others* judgments and reiterates that it is not the task of the Court "to substitute for the

[292] Siemen (2006), p. 161; to the notion of "secret surveillance" in the ECtHR's jurisprudence, see Cameron (2000), pp. 74–169.

[293] *Klass v. Germany*, Application no. 5029/71, judgment of 6 September 1978, para 42.

[294] Siemen (2006), p. 161.

[295] Ibid, para 48, and *Rotaru v. Romania*, Application no. 28341/95, judgment of 4 May 2000, para 59; Siemen (2006), p. 161.

[296] *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006, para 106; *Leander v. Sweden*, Application no. 9248/81, judgment of 26 March 1987, para 59.

[297] *Klass v. Germany*, Application no. 5029/71, judgment of 6 September 1978, para 51, and *Leander v. Sweden*, Application no. 9248/81, judgment of 26 March 1987, para 53.

[298] *Klass v. Germany*, Application no. 5029/71, judgment of 6 September 1978, para 49.

assessment of the national authorities any other assessment of what might be the best policy in this field".[299]

Since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public, discretion is nevertheless limited.[300] By emphasising that secret surveillance measures "must follow the values of a democratic society as faithfully as possible, in particular the rule of law [. . .]", the Court restricts the discretion.[301] The ECtHR adds that the rule of law demands effective supervision which should usually be carried out by the judiciary, as "judicial control affords the best guarantees of independence, impartiality and a proper procedure".[302]

This careful approach is also reflected in the case *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*. In 2007 the ECtHR set limits to restrict sprawling powers of governmental secret surveillance. In the present case the ECtHR was faced with the Bulgarian "Special Surveillance Means Act" (SSMA) which granted far reaching surveillance rights to the police and the Bulgarian secret service.[303] It held that Bulgarian law does not provide sufficient guarantees against the risk of abuse which is inherent in any system of secret surveillance.[304]

The ECtHR compared the Bulgarian legislation with the German G-10 Act (subject-matter in *Weber and Saravia v. Germany* as well as in *Klass v. Germany*) and primarily based itself on four main arguments:

Firstly, no external independent control assured compliance with the rules of the SSMA. There was no independent review of the implementation of secret surveillance measures or compliance with warrants authorising the use of such means. Nor was there was any control over whether the secret service faithfully reproduced the original data in the written record or whether the data were destroyed within the legal time limit if surveillance has proved fruitless.[305] Solely the Minister of Internal Affairs – who was directly involved in the commissioning of special means of surveillance and whose competences of control were not set out in the law – was entrusted with a certain overall control.

---

[299] *Klass v. Germany*, Application no. 5029/71, judgment of 6 September 1978, para 49. See also *Mersch and others v. Luxembourg*, Application no. 10439/83, 10440/83, 10441/83, 10452/83 10512/83 and 10513/83, admissibility decision of 10 May 1985 with a detailed debate about the different measures provided by the contested Luxembourgish law.

[300] *Amann v. Switzerland*, Application no. 27798/95, judgment of 16 February 2000, para 56.

[301] *Rotaru v. Romania*, Application no. 28341/95, judgment of 4 May 2000, para 59.

[302] Ibid.

[303] *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, Application no. 62540/00, judgment of 28 June 2007.

[304] Ibid, para 93.

[305] *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, Application no. 62540/00, judgment of 28 June 2007, para 85. To the lack of supervision, see also: *Volokhy v. Ukraine*, Application no. 23543/02, judgment of 2 November 2006, paras 42–54.

Moreover, the ECtHR identified an apparent lack of regulations precisely specifying the manner of screening the intelligence obtained through surveillance, the procedures for preserving its integrity and confidentiality and the procedures for its destruction.[306]

In addition, the ECtHR refers to the transmission of data to third parties. It compares the Bulgarian legislation with the German G-10 Act and criticises the SSMA for not providing strict rules regulating the transmission of intelligence to other services, nor independent monitoring of those rules.[307]

Finally, the ECtHR reiterates that after the termination of surveillance, "as soon as notification can be made without jeopardising the purpose of the measure", information should be provided to the persons concerned.[308] The SSMA did not provide for notification of persons subjected to surreptitious monitoring under any circumstances nor at any point in time. It even explicitly prohibited the disclosure of information that a person had been subjected to surveillance, or that warrants had been issued for this purpose.[309]

Summarising the Court's arguments in the *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria* case, independent control during and after the exercise of secret surveillance measures as well as information of the persons concerned after the termination of such measures, represent essential requirements which have to be fulfilled when states implement surveillance legislation.

Against the background of the weak legislative Bulgarian framework, the ECtHR clarified in *C.G. and others v. Bulgaria* that even a secret service file, if it is used to justify measures against an individual, must contain information making it possible to verify whether or not the secret surveillance measures taken were lawfully ordered and executed.[310]

It is noteworthy that compared to the above mentioned case *Leander v. Sweden*, this judgment seems to show a certain development towards a right of access to secret service files. However, this right is granted only under the following two conditions: first, the legal basis allowing for secret service measures which lead to a secret service entry is doubtful and second, the entry is subsequently used to justify restrictive measures against persons concerned.

Both Bulgarian cases nevertheless demonstrate that the ECtHR is becoming more sensitive as regards the criteria of independent control of secret surveillance measures and the information of persons concerned in connection with measures taken against them. The Court insists that basic data protection principles also apply within the framework of secret surveillance measures.

---

[306] *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, Application no. 62540/00, judgment of 28 June 2007, para 86.

[307] Ibid, para 89.

[308] Ibid, para 90.

[309] Ibid.

[310] *C.G. and others v. Bulgaria*, Application no. 1365/07, judgment of 24 April 2008, para 48.

Summarising the ECtHR's case law in respect to the purpose and necessity of secret surveillance measures, in general the ECtHR has consistently accepted that national authorities enjoy a fairly wide margin of appreciation in selecting the means for achieving the aim of protecting national security.[311] However, in view of the risk that systems of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the ECtHR seems to be satisfied that adequate and effective guarantees against abuse exist.[312] These guarantees entail the respect of basic data protection principles, such as independent control of the measures, deletion of unnecessary information, regulations specifying the screening as well as the destruction of information and procedures preserving its integrity and confidentiality, rules regulating the transmission of data to third parties and the informing of persons concerned after termination of surveillance (as soon as notification can be made without jeopardising the purpose of the measure).[313]

Bearing in mind the previous observations, it also has to be taken into consideration that the judgments examined above – except for *Weber and Saravia v. Germany* and the Bulgarian cases – refer to the threat of terrorism of the 1970s. Since then, investigation and tracing methods as well as the forms of terrorism have changed radically. The development of the internet has led to growing fragmentation and complexity of communication. Police and secret services are employing more and more sophisticated technologies and methods of tracking. In the development of those competences, states have to respect the criteria stipulated by the ECtHR's case law. The principles initially developed in the 1970s are still of general application; they have to be cautiously adapted to new technologies and current security challenges. The main values developed in the *Weber and Saravia v. Germany* judgment provide helpful guidance during this process.

(4) Secret Security Files

In *Leander v. Sweden*, the ECtHR expressly refers to the secret collection and storing of personal information.[314] It recognises the necessity to collect and store personal information in registers not accessible to the public as well as the use afterwards when assessing the suitability of candidates for employment in a post of

[311] *Leander v. Sweden*, Application no. 9248/81, judgment of 26 March 1987, para 59; *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006, para 106.

[312] *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006, para 106.

[313] *Klass v. Germany*, Application no. 5029/71, judgment of 6 September 1978; *Leander v. Sweden*, Application no. 9248/81, judgment of 26 March 1987 and *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, Application no. 62540/00, judgment of 28 June 2007.

[314] To the notion of "secret security files" in the ECtHR's jurisprudence, see Cameron (2000), pp. 170–258.

importance for national security.[315] After considering the guarantees against misuse, the ECtHR admits a wide margin of appreciation available to the respondent state, in particular in choosing the means for achieving the legitimate aim of protecting national security.[316]

Against this background, more than 20 years after *Leander v. Sweden*, the ECtHR was confronted with three cases coming from Romania, Sweden and Germany challenging the use and the storage of information obtained by a former security service.

In *Rotaru v. Romania* the Romanian state refused to grant to the applicant damages for suffered injustice during the communistic period on the basis of information obtained by the former communist secret service.[317] Although the complaint referred to the question whether the refusal was in accordance with the law, the ECtHR makes interesting remarks as to the supervision procedure of secret service activities. It notesthat even if it is up to the national authorities to interpret and apply domestic law, the system for gathering and archiving information did not provide sufficient safeguards against abuse, for example a supervision procedure during and after the time secret service activities were in force. Such a supervision procedure must follow democratic values, in particular the rule of law and has to be carried out effectively.[318] The ECtHR considers that this was not the case in *Rotaru v. Romania* and therefore decides that the holding and use of data by the Romanian secret service were not in accordance with the law.[319]

In this case, the concurring opinion of judge *Wildhaber*, who was joined by six other judges, is of great interest.[320] The judges agree with the decision of the ECtHR; however they make further observations in view of a possible time limit of the storage and use of the information obtained by a former secret service.[321]

Firstly they refer to the age of the entries. The file contained personal information dating mostly from the years 1946–1948, whereas one entry was made in 1937 where the applicant was bareley 16 years old. They criticise that even if the latter information was declared false by the Bucharest Court of Appeal, the entry was still recorded in the applicant's secret service file. Further he obtained no damages and no corrective actions were taken by the secret service to update the file. Additionally, the judges seriously doubt whether the interference pursued a legitimate aim and whether it was necessary in a democratic society. *Wildhaber* concludes: "In respect of national security as in respect of other purposes, there has to be at least

[315] *Leander v. Sweden*, Application no. 9248/81, judgment of 26 March 1987, para 59.

[316] Ibid.

[317] *Rotaru v. Romania*, Application no. 28341/95, judgment of 4 May 2000.

[318] Ibid, para 59.

[319] Ibid, para 62.

[320] See also: Siemen (2006), pp. 170–171.

[321] Concurring opinion of judge *Wildhaber* joined by the judges *Makaraczyk*, *Türmen*, *Costa*, *Tulkens*, *Casadevall* and *Weber* in *Rotaru v. Romania*, Application no. 28341/95, judgment of 4 May 2000.

a reasonable and genuine link between the aim invoked and the measures interfering with private life for the aim to be regarded as legitimate. To refer to the more or less indiscriminate storing of information relating to the private lives of individuals in terms of pursuing a legitimate national security concern is, to my mind, evidently problematic". Further they criticise that the data collected under a previous regime in an unlawful and arbitrary way continued to be kept on file without adequate and effective safeguards against abuse. The judges admit on the one hand that it should not be for the court to fix a time limit for the destruction of such data or whether comprehensive rights of access and rectification should be guaranteed, but on the other, they emphasise that they do not see a legitimate concern of national security which could justify the continued storing of such information in these circumstances.[322]

The judges conclude that even if a foreseeable legal basis had existed in the *Rotaru* case, the ECtHR "would have had to find a violation of Article 8 nevertheless, either on the ground that there was no legitimate aim for continuing an abusive system of secret files, or because such continuation was clearly not necessary in a democratic society".[323]

The concurring opinion hence clarifies two points:

Firstly it stipulates that the continuous storing of personal information, even in a secret service file, needs to be justified by a significant concern of national security. If this requirement can not be proven by the state, the retention of personal information does not pursue a legitimate aim, i.e. even if the ECtHR can not prescribe a time limit for destruction, it still has the possibility to examine the legitimate aim in detail.

Secondly, if the state is able to prove the pursuance of a legitimate aim, it does not enjoy unlimited discretion to subject individuals to a system of secret service files. Such a system must be strictly necessary for safeguarding democratic institutions, and adequate and effective safeguards against abuse must be established.[324]

Following this concurring opinion in *Rotaru v. Romania*, in 2006, the ECtHR was confronted with the question whether the continued storage of (true) secret service information was justified even 30 years after the entries were made. In *Segerstedt-Wilberg and others v. Sweden*, the Court went a step further than in *Rotaru v. Romania* and recognised a time limit for the storage of rather trivial information.

The ECtHR based its reasoning on the age and the nature of the records.[325] The gravity of the offences once committed played an important role. The ECtHR made a difference between records concerning, on the one hand, information about

[322] Ibid.

[323] Ibid.

[324] Ibid.

[325] *Segerstedt-Wiberg and others v. Sweden,* Application no. 62332/00, judgment of 6 June 2006, paras 88–92.

political commitment or the alleged advocacy of violent resistance to police control and, on the other, information concerning bomb threats against the applicant.[326]

In addition to the seriousness of the secret file's content, the age of the records was also taken into account.

In *Segerstedt-Wilberg and others v. Sweden* the ECtHR clearly opposes indefinite data storage by concluding that the retention of rather old (about 30 years) and fairly harmless entries is not necessary for the protection of national security any longer. However, more recent records concerning rather serious information were in accordance with Article 8 ECHR.[327] By arguing in this way, the ECtHR creates indirectly a right to erasure of information which is no longer relevant for the protection of national security or the prevention of disorder and crime. While this right nevertheless depends on the nature and the age of the entries, it constitutes a very important aspect in the development towards a right of deletion of entries in security files.

Related to the retention of data obtained by a (former) secret service is the use of secret service information.

In *Knauth v. Germany* the applicant worked as a nursery-school teacher in Berlin in the German Democratic Republic (GDR).[328] After the reunification she continued working in this profession until she was dismissed in 1994 for having collaborated with the GDR's Ministry of Security. As a consequence thereof, the ECtHR assessed whether there was an interference with the applicant's rights through the use of the information about her political past. In contrast to *Rotaru v. Romania*, the ECtHR found the German legislation to be foreseeable, precise and accessible to everyone and therefore in accordance with the law. As regards the question of a legitimate aim, the ECtHR considers that the dismissal pursued the aims of preventing disorder and protecting the rights of others: "it appeared legitimate for the FRG [Federal Republic of Germany] to carry out an ex post facto review of the conduct of persons who, after reunification, had been incorporated into the civil service, the members of which are the guarantors of the Constitution and of democracy. It also appeared legitimate for the FRG to dismiss from the civil service, after examining each individual case, members who did not satisfy those criteria, for example because they had collaborated with the GDR Ministry of National Security, and above all because they had lied about their collaboration to their new employer".[329] Moreover, the ECtHR carefully and explicitly balanced the severe consequence that the dismissal had for the applicant against the general interest of German society. It came to the conclusion that the interference was not disproportionate to the legitimate aim pursued, especially in consideration of the

[326] Ibid, paras 89–91.

[327] Ibid, paras 89–92.

[328] *Knauth v. Germany*, Application no. 41111/98, admissibility decision of 22 November 2001.

[329] Ibid.

exceptional historical context and the State's margin of appreciation in such matters.

The *Knauth v. Germany* judgment shows the detail and thoroughness with which the ECtHR assesses the question of the use of data obtained by a former secret service. It carefully examines whether the state pursued a legitimate aim and whether the measure at issue is essentially necessary in a democratic society.

e) The Role of Positive Obligations and Direct Horizontal Effect in Data Protection Cases

While most of the cases referred to above deal with privacy violations by public authorities, dangers to the protection of personal data also originate from the private sector. Article 3 of Convention No. 108 stipulates therefore that the Parties of the Convention "undertake to apply this convention to automated personal data files and automatic processing of personal data in the public and private sectors". This reference indicates that the Council of Europe is well aware of possible negative impacts of private data processing.

In some of the cases examined above, the ECtHR developed the duty of Member States to take legislative steps in order to prevent a breach of the right to data protection through private actors. This obligation results from a state's failure to intervene which can result in a failure to secure respect for the rights protected by Article 8 ECHR. In that case, the failure amounts to a breach of Article 8 ECHR even though the interference is not caused directly by the state.[330] This positive element of Article 8 is described by the term positive obligations.[331] The notion is fluid and not clearly defined by the ECtHR. The Court does not clearly distinguish between positive obligations, indirect or even direct secondary effects ("Drittwirkung").[332] However, there is broad and well acknowledged literature on the concept of positive obligations and its derivation.[333]

As the framework for this study is data protection, two aspects are of importance in this context: *Jacobs* and *White* describe the first case as a situation where the State must take *some action* to ensure respect for the rights included in Article

[330] Ovey and White (2006), p. 243.

[331] Ovey and White (2006), p. 243. See generally to Article 8 ECHR: Clapham (2006), pp. 387–400; Greer (2006), pp. 215–216, Wiesbrock (1999), pp. 120–123; Dröge (2003), pp. 13–23, 90–100, 123–137, 158–165; Heringa (2006).

[332] To a comparative analysis of the German term "Drittwirkung" and its signification, see Youngs (1998), pp. 95–97.

[333] See generally to positive obligation of Article 8 ECHR: Clapham (2006), pp. 387–400; Greer (2006), pp. 215–216, Wiesbrock (1999), pp. 120–123; Dröge (2003), pp. 13–23, 90–100, 123–137, 158–165.

8 ECHR.[334] Examples for this type of case are cases where the State must create an access right to personal information.[335]

Secondly, the state could be obliged to take protective measures to defend an individual from interferences by other individuals to ensure respect for the rights included in Article 8 ECHR.[336] Examples for this type of situation are the cases where individuals must be protected against unwanted release of personal information originating from public or even private actors.

aa) Fair Balance Test

In positive obligation cases, the textual basis for a state's responsibility under Article 8 ECHR is the duty to respect the rights elaborated in paragraph one of that provision.[337] The notion of respect as used in Article 8 ECHR is not yet identified definitively, especially in so far as positive obligations are concerned. The ECtHR emphasises that "having regard to the diversity of practices followed and the situations obtaining in the Contracting States, the notion's requirements will vary considerably from case to case and the margin of appreciation to be accorded to the authorities may be wider than that applied in other areas under the *Convention*".[338] As regards negative as well as positive obligations, States enjoy a certain margin of appreciation in determining the steps to be taken to ensure compliance with the ECHR, but if the State has failed to apply one particular positive obligation provided by domestic law, it may still fulfil its positive duty by other means.[339] For that reason, in those cases the criterion "in accordance with the law" of the justification test cannot be applied in the same way as in cases of direct interference by the State.[340] Thus the State enjoys a wider margin of appreciation as regards the choice of means.[341]

However, the applicable principles are mostly similar to a negative obligation.[342] In determining whether or not a positive obligation exists, the ECtHR

[334] Ovey and White (2006), p. 243.

[335] Siemen (2006), p. 178.

[336] Ovey and White (2006), p. 243.

[337] Mowbray (2007), p. 585.

[338] *I. v. the United Kingdom*, Application no. 25680/94, judgment of 11 July 2002, para 51.

[339] *Fadeyeva v. Russia*, Application no. 55723/00, judgment of 9 June 2005, para 96.

[340] Ibid.

[341] See *Fadeyeva v. Russia*, Application no. 55723/00, judgment of 9 June 2005, para 96: "Thus, in cases where an applicant complains about the State's failure to protect his or her Convention rights, domestic legality should be approached not as a separate and conclusive test, but rather as one of many aspects which should be taken into account in assessing whether the State has struck a "fair balance" in accordance with Article 8 § 2".

[342] Mowbray (2007), p. 585; Gómez-Arostegui (2005), pp. 153, 157. See also: *Fadeyeva v. Russia*, Application no. 55723/00, judgment of 9 June 2005, para 94; *Powell and Rayner v. the United Kingdom*, Application no. 9310/81, judgment of 21 February 1990, para 41.

pays particular regard to the fair balance that has to be struck between the competing interests of the individual and of the community as a whole.[343] Additionally, even in relation to the positive obligations coming from the first paragraph of Article 8, the aims mentioned in the second paragraph may be of certain significance.[344] As a consequence thereof, in cases where the parties disagree as to whether the measure at issue constitutes an interference with an existing right (negative obligation) or a failure by the State to grant a right which did not previously exist (positive obligation), the ECtHR applies the fair balance test.[345]

bb) Categories of Positive Obligations

Most of the cases in which the ECtHR developed positive obligations concern access rights to personal information included in medical[346] or secret service files. To stay within the limits of the following analysis of the data protection framework of the EU's AFSJ actors, only the access to secret service files including rectification and erasure rights are discussed hereinafter.

(1) Access to Secret Service Files

The central element of cases concerning the access to secret service files is that of balance between the inherent secrecy of the information and the individual's need to understand measures taken against him. As seen above, the ECtHR cautiously

[343] *Powell and Rayner v. the United Kingdom*, Application no. 9310/81, judgment of 21 February 1990, para 41; *Fadeyeva v. Russia*, Application no. 55723/00, judgment of 9 June 2005, para 94.

[344] *Powell and Rayner v. the United Kingdom*, Application no. 9310/81, judgment of 21 February 1990, para 41.

[345] *Dickson v. the United Kingdom*, Application no. 44262/04, judgment of 4 December 2007, paras 69–71: "The Court recalls that, although the object of Article 8 is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference. In addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private and family life. These obligations may involve the adoption of measures designed to secure respect for private and family life even in the sphere of the relations of individuals between themselves. The boundaries between the State's positive and negative obligations under Article 8 do not lend themselves to precise definition. The applicable principles are nonetheless similar. In particular, in both instances regard must be had to the fair balance to be struck between the competing interests [. . .]".

[346] Compare *Gaskin v. the United Kingdom*, Application no. 10454/83, judgment of 7 July 1989; in this context see also: Pitt-Payne (2003), pp. 108–119, 113; *M.G. v. the United Kingdom*, Application no. 39393/98, judgment of 24 September 2002; *K.H. and others v. Slovakia*, Application no. 32881/04, judgment of 28 April 2009; *McGinley and Egan v. the United Kingdom*, Application nos. 21825/93 and 23414/94, judgment of 9 June 1998; *Roche v. the United Kingdom*, Application no. 32555/96, judgment of 19 October 2005 and *Guerra and others v. Italy*, Application no. 14967/89, judgment of 19 February 1998.

approaches such cases by emphasising the state's wide margin of appreciation as regards national security interests.[347]

Whereas in *Leander v. Sweden* the ECtHR emphasised that the right of access to public service is not as such enshrined in the ECHR and consequently it did not recognise a serious interference with *Leander's* rights,[348] another Swedish case in 2006 re-revealed the question whether persons concerned should generally have a right of access to their secret service data files. In *Segerstedt-Wilberg and others v. Sweden*, five applicants contested the refusal of the Swedish authorities to provide them with information concerning their secret service files entries.[349] The ECtHR dealt briefly with this question referring to the *Leander* case: a refusal of full access to a national secret police register is necessary where the State may legitimately fear that the provision of such information may endanger the efficacy of a secret surveillance system designed to protect national security and to combat terrorism.[350] Nevertheless the ECtHR referred to the quality of the law and made clear that in this case, the legal basis guaranteeing the refusal balanced the interest at stake and provided for a clear description of the discretion conferred to the competent authorities.[351] The Court opposed the applicants' opinion that the storage of information in secret police registers for "special reasons" afforded unfettered powers to the police by basing on the argument that no entry could be made exclusively on the

[347] *Leander v. Sweden*, Application no. 9248/81 judgment of 26 March 1987, para 59; *C.G. and others v. Bulgaria*, Application no. 1365/07, judgment of 24 April 2008, para 43.

[348] *Leander v. Sweden*, Application no. 9248/81, judgment of 26 March 1987, paras 59 and 67; nevertheless the risks resulting from an underestimation of the dangers of secret collection, storing and use of personal information was subject to the partially dissenting opinion of judges *Pettiti* and *Russo* in *Leander v. Sweden*; although they do not consider an infringement of Article 8 ECHR in the end, they emphasise, with regard to the right of access to personal information concerning the applicant himself, that: "In the case specifically of registers which, being secret, make it impossible for a citizen to avail himself of the laws and regulations entitling him to have access to administrative documents, it is all the more necessary that there should be an effective remedy before an independent authority, even if that authority is not a judicial body". Already in 1987, in the wake of the electronic era, they add: "Consideration also needs to be given to the dangers of electronic links between the police registers and other States' registers or Interpol's register. The individual must have a right of appeal against an entry resulting from a fundamental mistake, even if the source of the information is kept secret and is known only to the independent authority that has jurisdiction to determine the applicant's appeal". Therefore they conclude that: "[. . .] it is absolutely essential that an independent authority should be able to determine the merits of an entry in the register and even whether there has been a straightforward clerical error or mistake of identity – in which case the national – security argument would fall to the ground". Partially dissenting opinion of judges *Pettiti* and *Russo*, *Leander v. Sweden*, Application no. 9248/81, judgment of 26 March 1987).

[349] *Segerstedt-Wiberg and others v. Sweden,* Application no. 62332/00, judgment of 6 June 2006.

[350] *Segerstedt-Wiberg and others v. Sweden,* Application no. 62332/00, judgment of 6 June 2006, para 102.

[351] *Segerstedt-Wiberg and others v. Sweden,* Application no. 62332/00, judgment of 6 June 2006, paras 79 and 99–104.

basis of an individual's political opinion without his or her consent.[352] Additionally, judicial review of a decision denying the access was assured by several independent review bodies.[353] Under those conditions, the State enjoys a wide margin of appreciation as regards the regulation of access to its secret service files.[354]

In the above mentioned case *C.G. and others v. Bulgaria*, the ECtHR went a step further and clarified that if a secret service file is used to justify restrictive measures against an individual, it must contain information making it possible to verify whether the secret surveillance measures taken were lawfully ordered and executed or not.[355] Whereas in *Leander v. Sweden* the ECtHR still denied the right to access to information which explains why the applicant presented a security risk, in *C.G. and others v. Bulgaria* the Court demands at least an outline of the specific facts serving as a basis for the assessment that the applicant presented a national security risk.[356] It is noteworthy that compared to *Leander v. Sweden*, this judgment shows a certain development towards a right to be informed about the reasons for a decision which is to the detriment of a person concerned even though this information is contained in a secret service file.

Summarising, states are not under a general positive obligation regarding a right of full access to secret service data files,[357] but, there is nevertheless a right to know whether the content of one's own secret service data file was lawfully created if restrictive measures against a person concerned are based on this secret information.

Moreover, the right of access to a secret file can be included in Article 6 ECHR as part of the right to a fair trial.[358] Most importantly this right occurs in cases

[352] *Segerstedt-Wiberg and others v. Sweden,* Application no. 62332/00, judgment of 6 June 2006, para 79.

[353] *Segerstedt-Wiberg and others v. Sweden,* Application no. 62332/00, judgment of 6 June 2006, paras 62–68.

[354] *Segerstedt-Wiberg and others v. Sweden,* Application no. 62332/00, judgment of 6 June 2006, para 103.

[355] *C.G. and others v. Bulgaria*, Application no. 1365/07, judgment of 24 April 2008, para 48.

[356] *C.G. and others v. Bulgaria*, Application no. 1365/07, judgment of 24 April 2008, paras 46 and 47: [. . .] the Court finds it particularly striking that the decision to expel the first applicant made no mention of the factual grounds on which it was made. It simply cited the applicable legal provisions and stated that he "present[ed] a serious threat to national security"; this conclusion was based on unspecified information contained in a secret internal document [. . .]. Lacking even outline knowledge of the facts which had served as a basis for this assessment, the first applicant was not able to present his case adequately in the ensuing appeal to the Minister of Internal Affairs and in the judicial review proceedings.

[357] See also: *Segerstedt-Wiberg and others v. Sweden,* Application no. 62332/00, judgment of 6 June 2006, para 102: "The Court notes that, according to the Convention case-law, a refusal of full access to a national secret police register is necessary where the State may legitimately fear that the provision of such information may jeopardise the efficacy of a secret surveillance system designed to protect national security and to combat terrorism [. . .]".

[358] *Luboch v. Poland*, Application no. 37469/05, judgment of 15 January 2008, paras 49–73.

dealing with lustration proceedings in former communistic regimes.[359] The ECtHR found that it cannot be assumed that a continuing and real public interest remains in imposing restrictions on access to material classified as confidential under former regimes.[360] This finding is motivated by the very nature of lustration proceedings which serve to disclose facts dating back to the communist era and which are not connected to current activities and functions of the security services.[361] In this special case, access had to be granted to assure compliance with the right to a fair trial guaranteed by Article 6 ECHR.[362]

(2) Rectification and Erasure

In the last years, the ECtHR becomes increasingly aware of rectification and erasure rights. Whereas the Court in the 1990s paid little attention to applicants claiming rectification or erasure of personal data, there has been a move towards recognition of those rights in the last years.[363]

In the above mentioned cases *Segerstedt-Wilberg and others v. Sweden* and *Marper v. the United Kingdom*, the ECtHR developed an obligation to erase or rectify personal information contained in public databases or secret service files by acknowledging that the retention of certain information is limited in time and in some cases not necessary in a democratic society anymore. It refers to the core principles of the relevant instruments of the Council of Europe setting limits on the sprawling powers of public authorities to store data. Thereby the ECtHR recognises the right to erase data if they are wrong or no longer needed to safeguard an "actual relevant national security interest".[364] The participation in a political meeting or the entry about resistance to police control during demonstrations 30 years ago are examples of information no longer relevant to national security.[365]

---

[359] *Turek v. Slovakia*, Application no. 57986/00, judgment of 14 February 2006; *Matyjek v. Poland*, Application no. 38184/03, judgment of 24 April 2007; *Luboch v. Poland*, Application no. 37469/05, judgment of 15 January 2008.

[360] *Luboch v. Poland*, Application no. 37469/05, judgment of 15 January 2008, para 61.

[361] *Luboch v. Poland*, Application no. 37469/05, judgment of 15 January 2008, para 61; *Turek v. Slovakia*, Application no. 57986/00, judgment of 14 February 2006; *Matyjek v. Poland*, Application no. 38184/03, judgment of 24 April 2007.

[362] To the right of access as a procedural right, see Siemen (2006), pp. 191–192 discussing *McMichael v. the United Kingdom*, Application no. 16424/90, judgment of 24 February 1995.

[363] For the restricted approach of the ECtHR in the 1990s, see the cases related to transsexuals: *Yvonne Chave neé Jullien v. France*, Application no. 14461/88, admissibility decision of 9 July 1991; *Rees v. the United Kingdom*, Application no. 9532/81, judgment of 17 October 1986; *Cossey v. the United Kingdom,* Application no. 10843/84, judgment of 27 September 1990; *Sheffield and Horsham v. the United Kingdom*, Application nos. 22985/93 and 23390/94, judgment of 30 July 1998.

[364] *Segerstedt-Wiberg and others v. Sweden,* Application no. 62332/00, judgment of 6 June 2006, para 90.

[365] Ibid.

The Court did not take the direct approach of expressly establishing a positive obligation to erasure, instead it chose the path of proportionality by stating that the retention of data has to be proportionate in relation to the purpose of collection and limited in time.[366] In conclusion, states have to enact appropriate measures against the misuse of personal data, including the establishment of erasure and rectification rights.

f) Conclusion: The ECtHR's Case-Law with Regard to Article 8 ECHR – Valuable Support in Searching for European Data Protection Principles in the AFSJ

Taking into account the above observations, the ECtHR is increasingly aware of the data protection elements inherent to its case-law. Whereas earlier interpretations of Article 8 ECHR data protection guarantees were closely attached to the right to private life, recent cases show the development towards a right to data protection as one independent aspect of Article 8. Similar to other guarantees of the ECHR, the scope of this aspect of Article 8 is a wide one. It does not depend on criteria such as the type of the data or the way they were processed. The scope includes all forms of personal information no matter how the data are used. At the same time, it is open to the right to access personal data which plays an increasing role in the ECtHR's jurisprudence.

While the ECtHR sets almost no limits to the scope, it attempts to restrict the application of Article 8 ECHR when examining the interference.

Several categories can be distilled from the ECtHR's case law. In addition to legislation and measures directly restricting the right to data protection, various other actions can interfere with Article 8 ECHR. It is important to underline that each of the following acts constitutes a separate interference with Article 8 ECHR: the storing, the transmission, the release and the retention of data.

Despite the originally restrictive function of the interference criterion, a great number of actions still interfere with Article 8 ECHR. As a consequence, the essential way to distinguish whether an action is in compliance with Article 8 ECHR is to balance the interest of the Member States and the individual's fundamental rights.

In cases dealing with legislation enacted against terrorism, permitting surveillance or collecting and storing of data and the retention of information on past criminal offences, the ECtHR's case law is characterised by the legal pragmatism of prescribing in great detail the kinds of data protection guarantees states have to enact to fulfill the requirements of Article 8 ECHR. Independent supervision, the ability to delete data, and procedural rights such as the obligation to notify are some

[366] See *S. and Marper v. the United Kingdom*, Application nos. 30562/04 and 30566/04, judgment of 4 December 2008, paras 101–126, and *Segerstedt-Wiberg and others v. Sweden,* Application no. 62332/00, judgment of 6 June 2006, paras 90–92.

of detailed principles which the ECtHR has established to keep up with the increasing legislation enacted in the security sector and with steadily more sophisticated technology.

Moreover, the limitation on the categories of individuals against whom surveillance measures may be taken as well as the clear definition of the circumstances and limits of the storing and the use of the information before processing[367] and time limits for storing are essential guarantees following from the respect of Article 8 ECHR. To avoid indiscriminate storing of personal data in governmental databases, the age of the person concerned must be taken into account.[368] It is essential to determine which kind of data are to be stored and for which purposes the data should be used afterwards (purpose limitation principle).[369] This core principle includes the initial determination of the subsequent use of the data and therefore supports the control of the power of data processors.[370] By separating different purposes and, in this way, different powers, the power remains restricted to a predefined and specified purpose.

The existence of independent review and adequate and effective safeguards against abuse, including effective remedies, are key elements to assure compliance with the rule of law.[371] Accessing actors and the persons authorised to consult the files must be defined before the collection of data in security-related data processing.[372]

Because the power of processors increases with the ability to exchange data,[373] the ECtHR clarified in *Weber and Saravia v. Germany* that the types of offences on behalf of which data transmission is permitted must be limited.[374] Further, in order to transmit data to other authorities, the data must be marked and remain connected

[367] *Segerstedt-Wiberg and others v. Sweden,* Application no. 62332/00, judgment of 6 June 2006, paras 88–92; *Liberty and others v. the United Kingdom*, Application no. 58234/00, judgment of 1 July 2008, para 68; *Rotaru v. Romania*, Application no. 28341/954, judgment of 4 May 2000, para 57; *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006, paras 116 and 127.

[368] *S. and Marper v. the United Kingdom*, Application nos. 30562/04 and 30566/04, judgment of 4 December 2008, para 119; *Segerstedt-Wiberg and others v. Sweden,* Application no. 62332/00, judgment of 6 June 2006, paras 89–92.

[369] *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006, para 116; *Rotaru v. Romania*, Application no. 28341/954, judgment of 4 May 2000, para 57; see also: *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, Application no. 62540/00, judgment of 28 June 2007.

[370] Gutwirth (2002), p. 97.

[371] *Rotaru against Romania*, Application no. 28341/95, judgment of 4 May 2000, paras 55–63; *Segerstedt-Wiberg and others v. Sweden,* Application no. 62332/00, judgment of 6 June 2006, para 121.

[372] *Rotaru v. Romania*, Application no. 28341/954, judgment of 4 May 2000, para 57.

[373] De Hert and Gutwirth (2006), in particular p. 30.

[374] *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006, para 129.

to the purposes which had justified their collection and the transmission must be recorded in minutes.[375] Since the *Leander v. Sweden*, explicit and detailed provisions relating to the access procedure, including a list of the authorities to which information may be communicated as well as the circumstances in which such communication may take place and the procedure to be followed are essential criteria applied in transfer cases.[376]According to ECtHR case law, the subsequent notification of individuals subject to surveillance measures is directly linked to the effectiveness of remedies before the courts and therefore to the existence of effective safeguards against the abuse of monitoring powers.[377] Therefore, notification of the individual should be carried out as soon as possible.[378]

As illustrated in the foregoing, over the years, in view of both the rapid pace of technological change and the policies of security lawmakers, the ECtHR describes in sometimes astonishing detail the measures which have to be introduced to assure conformity with the ECHR.

All in all, the weighting of interests as presently conducted by the ECtHR concentrates more and more on the protection of the individual in the broad context of the growing ability to rapidly distribute all kinds of information. In view of the dangers inherent in wrong or damaging information, the ECtHR attempts to take countermeasures by creating generic standards which then serve as a model in similar cases and give the states concrete instructions on how to best protect their citizens in comparable circumstances.

In doing so, the ECtHR shows a growing awareness vis-à-vis the state's reasons to justify interference. Weighting the state's argument against the interests of the individual is carried out with greater thoroughness than the early years of the ECtHR and leads more and more to a rather comprehensive protection of the right to data protection covering a wide range of everyday situations.

In addition to negative obligations, positive obligations in data protection play an increasing role and are closely connected with access, rectification as well as erasure rights.

The development since *Leander v. Sweden*, where the ECtHR strictly denied the right to access secret service information, thus preventing the applicant from investigating the reasons of the decision taken to his detriment, illustrates a movement towards the right to be informed about such reasons, even if such information might be contained in a secret service file. Over 20 years later, in

[375] *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006, paras 121 and 127.

[376] *Leander v. Sweden*, Application no. 9248/81, judgment of 26 March 1987, para 55.

[377] *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006, para 135: "since there is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively".

[378] *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006, para 135.

C.G. and others v. Bulgaria, the Court demands to reveal the existence of specific facts which justified the refusal of access and classified the applicant as a national security risk.[379] Possibilities of independent review of the access demand and a law balancing the interest of the state against those of the individual are today essential requirements to deny the access to information contained in secret service files.[380]

The question of rectification and erasure rights in the context of law enforcement databases or secret service files is the most difficult to answer. The ECtHR does not directly mention a positive obligation, although it clarifies that the retention has to be proportionate in relation to the purpose of collection and limited in time.[381] By putting the question under the umbrella of the proportionality criterion, the Court recognises the right to erase wrong data or data which are no longer necessary to safeguard national security.

All in all, in particular the development in recent years illustrates the great awareness of the ECtHR in respect of the data protection right of individuals. Over the years, the standards of the ECtHR have become much more specific, giving detailed instructions regarding the extent to which states have to change their national legislation to comply with the ECHR. The dangers resulting from growing data processing and storing in large databases will be progressively taken into account. Besides the negative obligation to protect an individual from interferences of the state, positive obligations such as the possible development of an access right to personal data play an increasingly important role.

2. *Data Protection Elements and Restrictions with Regard to Articles 5, 6, 10 and 13 ECHR*

In addition to the protection offered by Article 8 ECHR, there are several data protection elements contained in other articles of the ECHR. Those elements cover, on the one hand, "pure" data protection aspects and on the other, access rights as well as restrictions to data protection.

---

[379] *C.G. and others v. Bulgaria*, Application no. 1365/07, judgment of 24 April 2008, paras 46 and 47: "[. . .] the Court finds it particularly striking that the decision to expel the first applicant made no mention of the factual grounds on which it was made. It simply cited the applicable legal provisions and stated that he "present[ed] a serious threat to national security"; this conclusion was based on unspecified information contained in a secret internal document [. . .]. Lacking even outline knowledge of the facts which had served as a basis for this assessment, the first applicant was not able to present his case adequately in the ensuing appeal to the Minister of Internal Affairs and in the judicial review proceedings."

[380] See cases: *Segerstedt-Wiberg and others v. Sweden,* Application no. 62332/00, judgment of 6 June 2006 and *C.G. and others v. Bulgaria*, Application no. 1365/07, judgment of 24 April 2008.

[381] See *S. and Marper v. the United Kingdom*, Application nos. 30562/04 and 30566/04, judgment of 4 December 2008, paras 101–126, and *Segerstedt-Wiberg and others v. Sweden,* Application no. 62332/00, judgment of 6 June 2006, paras 90–92.

a) Article 5 ECHR

In connection with the right to personal liberty and security as guaranteed by Article 5 ECHR, the Court assessed that the failure to make documents available to the applicant's lawyer constituted a violation of Article 5 (4) ECHR.[382] The refusal of rapid access precluded the opportunity of effectively challenging the statements or views on which the detention decision was based.[383] With regard to the interpretation of the requirements of a "reasonable suspicion" of Article 5 (1) lit c ECHR, which is necessary to arrest a person, the ECtHR stipulated that the use of confidential information to justify a detention decision is in accordance with Article 5 ECHR.[384]

b) Article 6 ECHR

Other procedural guarantees including data protection elements are incorporated in Article 6 ECHR. Article 6 (1) ECHR establishes among others that "everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law". Directly connected to the principle of equality of arms and enshrined in the wider concept of a fair trial, is the right to have an adversarial trial.[385] This means that both parties must be given "the opportunity to have knowledge of and comment on the observations filed and the evidence adduced by the other party".[386] Article 6 (1) ECHR read together with Article 6 (3) lit. d ECHR therefore grants to a certain extent a right to access court files and a right of judicial review exercised by an independent judge.[387]

Limitations to the right to disclosure of all information in the context of a court hearing may arise from interests of national security, the protection of witnesses or secret investigation methods.[388] In those cases, evidence or other information may be withheld to assure protection of other individuals or to safeguard an important

---

[382] *Lamy v. Belgium*, Application no. 10444/83, judgment of 30 March 1989; Article 5 (4) ECHR states: "Everyone who is deprived of his liberty by arrest or detention shall be entitled to take proceedings by which the lawfulness of his detention shall be decided speedily by a court and his release ordered if the detention is not lawful".

[383] *Lamy v. Belgium*, Application no. 10444/83, judgment of 30 March 1989, para 29. See also: Ovey and White (2006), p. 153.

[384] *Murray v. the United Kingdom*, Application no. 14310/88, judgment of 28 October 1994, paras 50–63; Siemen (2006), p. 205.

[385] Ovey and White (2006), p. 176.

[386] *Rowe and Davis v. the United Kingdom*, Application no. 28901/95, judgment of 16 February 2000, para 60; *Ruiz-Mateos v. Spain*, Application no. 12952/87, judgment of 23 June 1993, para 63; *Edwards and Lewis v. the United Kingdom*, Application nos. 39647/98 and 40461/98, judgment of 27 October 2004, paras 46 and 48.

[387] Meyer-Ladewig (2006), Article 6, para 45 a; Siemen (2006), pp. 206–207.

[388] Ovey and White (2006), p. 177; Meyer-Ladewig (2006), Article 6, para 41.

public interest.[389] In some cases, even an intense press campaign can influence the fairness of a trial.[390] Nevertheless information may only be retained if it is strictly necessary.[391]

On several occasions, the Court was further faced with the question whether the admission as evidence of information obtained in breach of Article 8 ECHR (for instance the unlawful use of a covert listening device), conflicts with the requirements of fairness guaranteed by Article 6 (1) ECHR.[392] In only one of the cases, the Court found a violation of Article 6 ECHR: in *Allan v. the United Kingdom*, the applicant was in pre-tail detention and expressed his wish to remain silent during the interrogation.[393] However, the police used the applicant's cellmate to obtain evidence, including taped conversations. Since the ECtHR cannot rule in general on the admissibility of evidence as such, it had to assess whether the proceedings as a whole, including the way in which the evidence was obtained, were fair.[394] In this case, the evidence, obtained in the described way, constituted the principal evidence relied on by the prosecution at the applicant's trail.[395] The Court considered that under such circumstances, besides the violation of Article 8 ECHR, there has also been a breach of Article 6 ECHR.

c) Article 10 ECHR

Article 10 (2) ECHR contains a limitation on the freedom of expression relating to the prevention of the disclosure of information received in confidence. This option, which restricts the freedom of expression, is rarely used. It is invoked in cases where the government wants to control the publication of books or press articles disclosing internal governmental or secret service information or hinder the

[389] Ovey and White (2006), p. 177; see *Rowe and Davis v. the United Kingdom*, Application no. 28901/95, judgment of 16 February 2000, para 61; *Ruiz-Mateos v. Spain*, Application no. 12952/87, judgment of 23 June 1993, para 63; *Edwards and Lewis v. the United Kingdom*, Application nos. 39647/98 and 40461/98, judgment of 27 October 2004, paras 46 and 48; *P.G. and J.H. v. the United Kingdom*, Application no. 44787/98, judgment of 25 September 2001, para 68.

[390] *Craxi v. Italy*, Application no. 34896/97, judgment of 5 December 2002, para 104; Meyer-Ladewig (2006), Article 6, para 60 c.

[391] *Rowe and Davis v. the United Kingdom*, Application no. 28901/95, judgment of 16 February 2000, para 61.

[392] *Khan v. the United Kingdom*, Application no. 35394/97, judgment of 12 May 2000, paras 25–28; *P.G. and J.H. v. United Kingdom*, Application no. 44787/98, judgment of 25 September 2001, paras 37–38; *Allan v. the United Kingdom*, Application no. 48539/99, judgment of 5 November 2002 paras 45–53; *Bykov v. Russia,* Application no. 4378/02, judgment of 10 March 2009, paras 94–105.

[393] *Allan v. the United Kingdom*, Application no. 48539/99, judgment of 5 November 2002.

[394] *Allan v. the United Kingdom*, Application no. 48539/99, judgment of 5 November 2002, para 42.

[395] Ibid, para 45.

publication of information about judicial investigation proceedings.[396] Limitations on the exercise of this right start from the date where the confidential information is in the public sphere (e.g. a banned book is available in another country). From that day on, the disclosure of the information can no longer be subject to punishment.[397]

In addition, despite the fact that on several occasions the Court discussed the question whether the right to freedom of expression of Article 10 ECHR guarantees an access right to information held by the authorities, the ECtHR has held for a long time that this right is not included in the Article.[398] While the Court in 2003 still found it "difficult to derive from the Convention a general right of access to administrative data and documents",[399] recently, the Court advanced towards a broader understanding of the concept of freedom to receive information.[400]

In *Társaság a Szabadságjogokért v. Hungary* the ECtHR explicitly declared that there is a development "towards the recognition of a right of access to information" within the framework of Article 10 ECHR.[401] Hungarian courts refused a non-governmental organisation access to a complaint pending before the constitutional court concerning a parliamentarian's request for examination of amendments to the criminal code in relation to drug-related offences. The government argued that access must be denied because the opinion of the parliamentarian, who lodged the

[396] See the "Spycatcher" cases, where the ban on a book reprint was found to be an interference with Article 10 ECHR: *Observer and Guardian v. the United Kingdom*, Application no. 13585/88, judgment of 26 November 1991 and *Sunday Times v. the United Kingdom*, Application no. 13166/87, judgment of 26 November 1991; *Editions Plon v. France*, Application no. 58148/00, judgment of 18 May 2004; see also: *Weber v. Switzerland*, Application no. 11034/84, judgment of 22 May 1990, where the fine the applicant had to pay for breaching the confidentiality of a judicial investigation was found to be an interference with Article 10 ECHR; to the latter, see also: *Stoll v. Switzerland*, Application no. 69698/01, judgment of 25 April 2006.

[397] Meyer-Ladewig (2006), Article 10, para 29; *Observer and Guardian v. the United Kingdom*, Application no. 13585/88, judgment of 26 November 1991; *Sunday Times v. the United Kingdom*, Application no. 13166/87, judgment of 26 November 1991; *Editions Plon v. France*, Application no. 58148/00, judgment of 18 May 2004.

[398] For background information on Article 10 ECHR, compare Cole et al. (2008), in particular pp. 161–207; *Leander v. Sweden*, Application no. 9248/81, judgment of 26 March 1987, para 74; *Gaskin v. the United Kingdom*, Application no. 10454/83, judgment of 7 July 1989, paras 51–53; *Roche v. the United Kingdom*, Application no.32555/96, judgment of 19 October 2005, paras 171–173; since *Leander v. Sweden*, the ECtHR continuously reiterates that "the freedom to receive information prohibits a Government from restricting a person from receiving information that others wish or may be willing to impart to him and that that freedom cannot be construed as imposing on a state, in circumstances such as those of the present case, positive obligations to . . . disseminate information of its own motion", *Roche v. the United Kingdom*, Application no.32555/96, judgment of 19 October 2005, para 172 and the judgments mentioned above.

[399] *Loiseau v. France*, Application no. 46809/99, admissibility decision of 18 November 2003.

[400] *Társaság a Szabadságjogokért v. Hungary*, Application no. 37374/05, judgment of 14 April 2009, para 35, and *Sdružení Jihočeské Matky v. Czech Republic*, Application no. 19101/03, admissibility decision of 10 July 2006.

[401] *Társaság a Szabadságjogokért v. Hungary*, Application no. 37374/05, judgment of 14 April 2009, para 35.

constitutional complaint, constitutes private data which could not be released without his consent. The ECtHR drew a comparison between the applicant's functions in society and those of the press. Similar to the press, non-governmental organisations would exercise the role of a "social watchdog" by informing the public of political and social matters.[402] To hinder access to information of public interest contradicts this role being essential to the functioning of a democratic society.[403] Therefore, the Court considers that "it would be fatal for the freedom of expression if public figures could censor the press and public debate in the name of their personality rights".[404] Consequently, the refusal breached the applicant's right to have access to information of public interest.[405]

The case *Társaság a Szabadságjogokért v. Hungary* clearly shows the development towards the creation of an access right inherent to Article 10 ECHR to information of public interest granted to the press and other organisations taking part in the shaping of public opinion. This access right refers to the access of documents in the sense of EU Regulation 1049/2001 and should not be confused with the right of access to a file in criminal proceedings and can therefore be distinguished from the individual right to be informed about personal data in the context of Article 8 ECHR.[406]

Another interesting case, further discussed in Chap. B,[407] in the framework of Article 10 ECHR relating to the EU Commission's investigative powers is *Tillack v. Belgium* from 2007[408]: OLAF, the European Anti Fraud Office, being part of the EU Commission, suspected *Tillack*, a German journalist, of having bribed a EU civil servant by paying him 8000 Euros in exchange for confidential information. Thereupon OLAF opened an investigation and lodged a complaint against Mr. *Tillack* with the Belgian judicial authorities which searched his home as well as his workplace seizing his working papers and tools. The applicant later complained to the European Ombudsman who came to the conclusion in his report that OLAF's suspicions based on rumors and that the unit had made incorrect and misleading statements in its submissions to the Ombudsman.[409]

Additionally, the applicant filed a suit under former Article 230 (4) EC Treaty against the EU Commission arguing that the actions of the Belgian police followed from the decision of OLAF to investigate him.[410] The national authorities would

[402] Ibid, para 36.

[403] Ibid, para 38.

[404] Ibid, para 37.

[405] Ibid, paras 38–39.

[406] For the distinction, see White (2009), in particular p. 66.

[407] See Chap. B II 3 b.

[408] *Tillack v. Belgium*, Application no. 20477/05, judgment of 27 November 2007.

[409] Special Report from the European Ombudsman to the European Parliament following the draft recommendation to the European Anti-Fraud Office in complaint 2485/2004/GG.

[410] T-193/04, *Tillack v. Commission*, judgment of 4 October 2006 and C-521/04 P (R), *Tillack v. Commission*, judgment of 19 April 2005, see in more detail: White (2010), in particular p. 90 and White (2009), in particular pp. 64–65.

have had no other choice but to comply with OLAF's request to seize evidence. The EU Commission, on the other side, disagreed with this opinion and referred to it as an autonomous decision of the national authorities to start investigations. The crucial question, however, was whether the sending of information from OLAF to the national authorities constitutes a legally binding act allowing a claim under Article 230 EC. The Court of First Instance agreed with the EU Commission's arguments and reached the conclusion that such a transmission does not give rise to any binding legal effects in relation to Mr. *Tillack*. The final decision to institute investigations lies within the sole responsibility of the national authorities.[411] The European Court of Justice later confirmed the judgment.[412] In consequence, OLAF's investigation reports are not legally binding acts and Mr. *Tillack's* complaint was rejected.

The ECtHR case dealt with Mr. *Tillack's* complaint against the searches of his home and workplace by the Belgian authorities.[413] The Court found that the searches in question amounted to an interference with the applicant's right to freedom of expression, specifically the right of a journalist to protect his sources, and were not justified by the exceptions provided for in Article 10 (2) ECHR. The ECtHR proceeded on the assumption that the right not to reveal one's sources is part of the right to information and has to be treated with the greatest caution, in particular in the applicant's case where the suspicions were based on vague, unconfirmed rumors.[414]

It is worth pointing out that even if the cases deal with different subject matters, Mr. *Tillack* succeeded in obtaining damages from Belgium but failed with his complaint before the European Courts. The problems arising in this context are further analysed in Chap. B II 3 b.

d) Article 13 ECHR

Furthermore, the violation of Article 8 ECHR relatively often follows a breach of Article 13 ECHR which assures the availability of an effective remedy within the national legal order to enforce the substance of the Convention's rights.[415]

While Article 13 ECHR is mostly understood as guaranteeing a remedy only under the condition of a prior ECHR violation, in *Klass v. Germany* the ECtHR

[411] T-193/04, *Tillack v. Commission*, judgment of 4 October 2006.

[412] C-521/04 P (R), *Tillack v. Commission*, judgment of 19 April 2005, para 28.

[413] *Tillack v. Belgium*, Application no. 20477/05, judgment of 27 November 2007.

[414] *Tillack v. Belgium*, Application no. 20477/05, judgment of 27 November 2007, para 65.

[415] *Peck v. the United Kingdom*, Application no. 44647/98, judgment of 28 January 2003, para 99; *Kirov v. Bulgaria*, Application no. 5182/02, judgment of 22 May 2008; *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, Application no. 62540/00, judgment of 28 June 2007; *Rotaru v. Romania*, Application no. 28341/954, judgment of 4 May 2000, para 57; Ovey and White (2006), p. 460.

ruled on the applicability of Article 13 ECHR without demanding the violation of another Convention right.[416] In more recent cases, the ECtHR nevertheless examines Article 13 in conjunction with other provisions of the ECHR.[417]

In *Peck v. the United Kingdom* the ECtHR clearly stipulates that if no efficient remedy exists in national law in case of a breach of Article 8 ECHR, this lack of compensation amounts to a further violation of Article 13 ECHR.[418] In those cases, it is appropriate to examine separately and in addition to Article 8 ECHR, whether domestic law provides an effective remedy as guaranteed by Article 13 ECHR.[419]

A further problem arose in *Segerstedt-Wilberg and others v. Sweden*. The ECtHR had to examine whether the existence of a specific Swedish data inspection board and a so-called record board, a body particularly empowered to monitor on a daily basis the security police's entry and storage of information and to assess compliance with the Swedish Police Data Act, fulfilled the criteria of an effective remedy in cases where individuals seek the erasure or rectification of their police entries.[420] The applicants mainly based their argumentation on the fact that neither the record board nor the data inspection board had the competence to order destruction, rectification or erasure of information kept in the secret police files. The Court accepted the reasoning of the applicant and found in *Germany* addition to the violation of Article 8 ECHR that the Swedish law did not assure direct access to any legal remedy as regards the erasure of the information in question and consequently it did not meet the requirements of an effective remedy guaranteed by Article 13 ECHR.[421] The deficits could have been outweighed by any other possibility to seek compensation, but the Swedish data protection system did not provide for it. In consequence, by invoking Article 13 ECHR, the ECtHR underlines the importance of effective erasure and notification rights which should not only exist on paper, but have to be efficiently enforced in practice. It does not prescribe the details of an effective remedy system, though it stipulates that the absence of the latter violates Article 13 ECHR.

In addition to the requirement of provisions assuring rectification and erasure rights, the right to notification and appeal is often examined within the framework of Article 8 ECHR. Both rights can also be a part of the right to effective

[416] *Klass v. Germany*, Application no. 5029/71, judgment of 6 September 1978, para 63. Ovey and White (2006), p. 460.

[417] See for instance the *Weber and Saravia v. Germany* admissibility decision dealing with the same subject matter as *Klass v. Germany*: *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006, para 156.

[418] *Peck v. the United Kingdom*, Application no. 44647/98, judgment of 28 January 2003, paras 91–114; *Kirov v. Bulgaria*, Application no. 5182/02, judgment of 22 May 2008, paras 48–58.

[419] Where the essence of the principal complaint is the absence of an appropriate remedy required by another provision of the ECHR, it is unnecessary to consider Article 13 ECHR, see Ovey and White (2006), p. 460.

[420] *Segerstedt-Wiberg and others v. Sweden,* Application no. 62332/00, judgment of 6 June 2006, paras 108–122.

[421] Ibid, para 121.

remedy.[422] Even in secret surveillance cases, a limited remedy system has to assure the rights of the persons monitored. Examples can be found in *Klass v. Germany* where individuals believing themselves to be under surveillance could bring an action to the commission overseeing the system of surveillance (or to the German Federal Constitutional Court).[423] The lack of notification of individuals after the termination of surveillance measures additionally violates Article 13 ECHR, as those concerned are unable to seek redress in respect of the use of the secret surveillance measures against them.[424]

e) Conclusion: Procedural Rights Slightly Underpinning the Protection of Article 8 ECHR

All things considered, in addition to the guarantees of Article 8 ECHR, there are several procedural rights including data protection elements contained in Articles 5, 6, 10 and 13 ECHR. In some cases, they complete the protection stemming from Article 8 ECHR, in others they are closely interlinked with the scope of the Article on which they are based.[425] An example of the latter is the access right to court files which refers to the fair trial concept of Article 6 ECHR and can, as a matter of course, only be invoked within the scope of Article 6 ECHR. Insofar as regards the last category, it is difficult to draw generalising data protection principles out of the analysis of other provisions apart from Article 8 ECHR. In this case, the procedural data protection guarantees rather represent additional protection in particular situations than pure data protection rights. They often arise from a further development of another right of the Convention and are "annexed" to it.

The rights enshrined in Article 13, such as the rights to notification, appeal, erasure or rectification represent important guarantees completing the protection of Article 8 ECHR. It remains to be seen whether the development towards the recognition of a right of access to information within the framework of Article 10 ECHR will continue.

Both categories, however, represent vital data protection elements which are essential to develop further the protection under Article 8 ECHR.

---

[422] *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, Application no. 62540/00, judgment of 28 June 2007, paras 96–103; *Kirov v. Bulgaria*, Application no. 5182/02, judgment of 22 May 2008, paras 48–58; *Klass v. Germany*, Application no. 5029/71, judgment of 6 September 1978, paras 69–70; *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006, para 157; *Rotaru v. Romania*, Application no. 28341/954, judgment of 4 May 2000, para 57.

[423] *Klass v. Germany*, Application no. 5029/71, judgment of 6 September 1978, para 70.

[424] *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, Application no. 62540/00, judgment of 28 June 2007, para 101.

[425] See Siemen (2006), p. 210.

3. *Convention No. 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data*

In contrast to the economically oriented OECD Guidelines mentioned in the introduction,[426] the Council of Europe Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data is oriented on a fundamental rights perspective.[427] From the point of view of the Council of Europe, Convention No. 108 is a consistent further development of Article 8 ECHR.[428] After ratification by France, Norway, Sweden, Spain and Germany, the instrument entered into force in 1985. During the first years, it was legally binding only for these five Member States, whereas in the meanwhile, Convention No. 108 has been ratified by 41 States of the Council of Europe.[429] The European Communities acceded Convention No. 108 in June 1999.[430] It is referred to in various EU instruments dealing with the exchange of data on the EU level.[431] While Convention No. 108 is regarded as a "non-self-executing" act by the vast majority of scholars, signifying that no individual rights can be directly deduced from it,[432] it nevertheless represents the first legally binding European instrument in the data protection field and is promoted by some authors and governments to provide a possible basis for an international data protection convention seeing that Convention No. 108 is open to accession to States which are not members of the Council of Europe since July 2008.[433]

---

[426] OECD Recommendation concerning Guidelines governing the protection of privacy and transborder flows of personal data of 23 September 1980.

[427] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981, CETS No. 108. In the following: Convention No. 108; to the history and the details, see Henke (1985–1986).

[428] Simitis (2006), p. 130, para 184.

[429] Albania, Andorra, Austria, Belgium, Bosnia, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Germany, Estonia, Finland, France, Georgia, Greece, Hungary Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxemburg, the former Yugoslav Republic of Macedonia, Malta, Moldova, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Sweden, Switzerland, Serbia, Slovakia, Slovenia, Spain and the United Kingdom (February 2011).

[430] Amendments to Convention No. 108 allowing the accession of the European Communities, 15th June 1999.

[431] Recital (11) of Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of the individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995, L-281/31; Article 14 of Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime, OJ 2009, L-138/4; Article 27 Council Decision of 6 April 2009 establishing the European Police Office, OJ 2009, L-121/37 etc.

[432] Petri (2001), p. 141; Henke (1985–1986), p. 60 et seq. with further references.

[433] See the goals of the French government in: Besson (2008); critical: Kuner (2009), pp. 307–317, p. 313; For the decision to open accession to non-member states, see Council of Europe, Committee of Ministers, 1031st meeting of 2 July 2008, Decision, Item 10.2, (CM/Del/Dec (2008)1031 4 July 2008).

a) The Principles of Convention No. 108

In order to ensure minimum coherence between the Members of Convention No. 108, domestic legislation has to be adapted to general data protection principles which it stipulates. Following the example of the OECD Guidelines, it applies to data processing in the public as well as the private sector and is limited to automatic data processing. Convention No. 108 entails broad common principles including five "basic" data protection standards which represent common core values in European data protection law. For the first time in European history, Convention No. 108 specifies from a fundamental rights point of view, principles referring to the quality of data and to data processing. Data must be:

1. Obtained and processed fairly and lawfully,
2. Stored for specific and legitimate purposes and not used in a way incompatible with those purposes,
3. Adequate, relevant and not excessive in relation to the purposes for which they are stored,
4. Accurate and, where necessary, kept up to date and finally,
5. Preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.[434]

In addition to these five principles, Members of Convention No. 108 are required to establish provisions regarding "special categories" of data and a sanction and remedy system for persons concerned.[435] The notion of "special categories" has an anti-discriminatory function and therefore refers to data revealing racial origin, political opinions, religious or other beliefs, as well as personal data concerning health or sexual life or criminal convictions. According to the Explanatory Report No. 48 of Convention No. 108, further data categories can be added to this list. Nowadays, these data categories are often summarised by using the term "sensitive data". For the processing of these data, member states have to establish "appropriate" security measures. That means that the domestic law of the Member States of Convention No. 108 ultimately determines the level of protection of "sensitive data".

Derogation from the five basic principles is only allowed in accordance with Article 9 Convention No. 108 and must be provided for by national law. It must also constitute a "necessary measure in a democratic society in the interest of: protection state security, public safety, the monetary interest of the state or the suppression of criminal offences" or the protection of the data subjects' rights and freedoms of others.

Transparency is required by Article 8 of Convention No. 108 which sets out the rights of the individuals, consisting of information, rectification and erasure rights. Persons concerned shall be enabled to establish the existence of an automated personal data file, its main purposes, as well as the identity the habitual residence or principal place of business of the controller of the file and have a remedy if a

[434] Article 5 lit a-e Convention No. 108.

[435] Articles 6, 8 and 10 Convention No. 108.

request for confirmation or, as the case may be, communication, rectification or erasure is not complied with.[436]

In addition to these provisions, Convention 108 deals with transborder flows of personal data. While the scope of these provisions is restricted in regards to transfer across national borders of the Convention's Member States, these provisions do not regulate data transfer to third states. According to Article 12 Convention No. 108, it is prohibited to restrict data transfer for the sole purpose of the protection of privacy. Member States should not impose higher data protection standards to the recipient state than provided for in Convention No. 108.[437] However, Convention No. 108 does not replace domestic law – its purpose is restricted to offer "helpful guidance" in case of the implementation of domestic data protection acts. Therefore it is in the competence of the member states to concretise the Convention's provisions through implementation of national law.

b) The Additional Protocol Amending Convention No. 108 Regarding Supervisory Authorities and Transborder Data Flows

Since Convention No. 108 does not regulate the transfer of data to third states, the Council of Europe enacted in November 2001 an additional protocol amending Convention No. 108 regarding supervisory authorities and transborder data flows.[438] According to this protocol, the transfer to third actors is generally permitted under the condition that the third party ensures an adequate level of protection for the intended transfer.[439] Similar to Directive 95/46, the adequacy mechanism provides certain criteria which have to be taken into account when assessing the

[436] See Article 8 lit a and lit d Convention No. 108.

[437] In two cases the convention permits the suspension of the transfer to another member state. Article 12 para 3 lit a and b Convention No. 108 provides: Firstly, in case if the state's legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection. Secondly, when the transfer is made from the state's territory to the territory of a non Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph. In the first case, as there is no common definition of sensitive data for contracting states, member states are in charge of specification of the criteria of sensitive data on their own. In the second case, transfer to another member states remains legitimate as long as the data processing takes place in the recipient member state. There are no regulations for data once received from a contracting party after the processing in the recipient state took place (i.e. transfer of the received data to third states).

[438] Additional Protocol of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, 8 November 2001.

[439] Article 2 Additional Protocol of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, 8 November 2001.

level of protection for each transfer. In addition to an examination of the circumstances of the transfer, in particular the type of data, the following must be taken into account: the purposes and duration of processing for which the data are transferred, the country of origin and the country of final destination, the general and sectoral rules of law applicable in the state or organisation in question and the professional and security rules which are in force there.[440] The adequacy of the data protection rules can be assessed for a whole state or organisation. Despite of the similarity to the adequacy mechanism of Directive 95/46,[441] the Explanatory Report of the Additional Protocol to Convention No. 108 from 2001 makes no explicit reference to it, but in practice the adequacy decisions of the EU Commission might serve as a helpful indication.

Member States, however, can derogate from this provision under the following circumstances: if domestic law provides for it, because of specific interest of the data subject or legitimate prevailing interest (especially important public interest) or if adequate safeguards (i.e. contractual clauses) are provided by the controller responsible for the transfer. In any case, they must respect "the principle inherent in European law that clauses making exceptions are interpreted restrictively, so that the exception does not become the rule".[442]

While the additional protocol to Convention No. 108 entered into force in 2004, no more than 25 Member States of the Convention No. 108 ratified the instrument so far, amongst them only 19 of the 27 EU Member States.[443] This limited participation highlights another weak point of Convention No. 108 when it comes to the possibility of broad interpretation of the general principles, in particular with regard to the implementation in domestic law. As a consequence thereof, the "categorical statement" for limitations on data processing is diminished in its value.[444]

Finally, another problem arises regarding the possibility to challenge a decision violating one of the rights listed in the Convention. Neither Convention No. 108, nor its additional protocol provide for such a possibility. Individuals shall have a right to be heard, but have no substantial right to lodge a complaint. Rather, personal data are protected in an "indirect way", i.e. states are obliged to comply with the provisions, but there is no individual right to file a complaint against misuse of data which could assure more effective protection on a European level.

---

[440] Explanatory Report of the Additional Protocol to Convention No. 108, point 27.

[441] Compare Sect. III 2 e bb.

[442] Article 2 para 2 lit a and b Additional Protocol to Convention No. 108; Explanatory Report of the Additional Protocol to Convention No. 108, point 31; WP 114 of Article 29 Working Party of 25th November 2005.

[443] Ratification in February 2011: Albania, Andorra, Austria, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Estonia, France, Germany, Hungary, Ireland, Latvia, Liechtenstein, Lithuania, Luxembourg, Monaco, Montenegro, Netherlands, Poland, Portugal, Romania, Serbia, Slovakia, Spain, Sweden, Switzerland, Ukraine and the former Yugoslav Republic of Macedonia; EU Member States such as Belgium, Denmark, United Kingdom or Slovenia have not yet ratified the Protocol.

[444] Simitis (2006), p. 121, para 162.

4. *Recommendation No. R (87) 15 Regulating the Use of Personal Data in the Police Sector*

In addition to Convention No. 108, Recommendation R (87) 15 deals with the use of personal data in the police sector.[445] Whereas the binding force of this recommendation might be controversial,[446] it nevertheless specifies certain basic data protection principles in a law enforcement context and, even though it was adopted in 1987, it is still referred to by various EU instruments dealing with the use of personal data in a police context. Examples are the Europol Council Decision, the Schengen instruments and the Prüm Convention.[447]

Recommendation R (87) 15 constitutes one of the most consulted instruments of the Council of Europe elaborating the data protection implications of Article 8 ECHR[448] and the guarantees of Convention No. 108 in this special field of police data exchange by amongst others concretising the derogations made in Article 9 Convention No. 108.[449]

Every 4 years from 1994 to 2002, Recommendation R (87) 15 was reviewed by the Project Group on Data Protection of the Council of Europe's Committee of

[445] Recommendation R (87) 15 of the committee of ministers to member states regulating the use of personal data in the police sector, adopted on 17 September 1987.

[446] To the different wording of the binding force of Recommendation R (87) 15 in the context of Europol, see Petri (2001).

[447] Article 27 and recital 14 Council Decision of 6 April 2009 establishing the European Police Office and replacing the Europol Convention OJ 2009, L-121/37; Articles 115 and 117 Schengen Convention; Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of second generation Schengen Information System, OJ 2007, L-205/63, recital 20; Article 34 Prüm Convention.

[448] Besides Recommendation R (87) 15, there are amongst others: Recommendation No. R (86) on the protection of personal data used for social security purposes of 23 January 1986; Recommendation No. R (89) 2 on the protection of personal data used for employment purposes of 18 January 1989; Recommendation No. R (90) 19 on the protection of personal data used for payment and other related operations of 13 September 1990; Recommendation No. R (95) 4 on the protection of personal data in the area of telecommunication services of 7 February 1995; Recommendation No. R (97) 5 on the protection of medical data of 13 February 1997 etc.

[449] Article 9 of Convention No. 108 – Exceptions and restrictions (1) No exception to the provisions of Articles 5, 6 and 8 of this convention shall be allowed except within the limits defined in this article; (2) Derogation from the provisions of Articles 5, 6 and 8 of this convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of: (a) protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences; (6) protecting the data subject or the rights and freedoms of others; (3) Restrictions on the exercise of the rights specified in Article 8, paragraphs b, c and d, may be provided by law with respect to automated personal data files used for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subjects.

Ministers.[450] Afterwards, review was abandoned as the Project Group agreed that the Recommendation's principles are still relevant and therefore considered that it was not necessary to revise them at present.[451] New developments could be addressed by a teleological interpretation of the existing recommendation. The three reports published until 2002 mainly entail proposals for national legislators how to interpret Recommendation R (87) 15 and how to improve existing data protection rules with regard to current sociological and technological developments.

a) The Principles of Recommendation R (87) 15

The first principle of Recommendation R (87) 15 refers to independent control and supervision which should be established outside the police sector.[452] When introducing new technical means for data processing, two requirements have to be fulfilled: the responsible national supervisory body should be consulted before the introduction, and all reasonable measures have to be taken to ensure that their use complies with the "spirit" of existing data protection legislation.[453] Even though the role of the supervisory body is limited to an advisory one, the prior consultation of this body assures a certain influence on the legislative process as well as the possibility of a public debate before introducing new technologies.[454] Furthermore, notification about permanent automated files to the supervisory body should include the nature of each file declared, the body responsible for its processing, its purposes, the type of data contained in the file and the persons to whom the data are communicated.[455]

The second principle deals with a relatively strict limitation on the use of the data: "the collection of personal data for police purposes should be limited to such as is necessary for the prevention of a real danger or the suppression of a specific criminal offence".[456] The rather severe wording of this principle is restricted however in the following sentence whereupon any exception to this provision is the subject of specific national legislation. Point 43 of the explanatory memorandum to Recommendation R (87) 15 clarifies that this rule expresses a qualitative and quantitative approach by prohibiting open-ended and indiscriminate collection

[450] First evaluation of the relevance of Recommendation R (87) 15 of 1994; Second evaluation of the relevance of Recommendation R (87) 15 of 1998; Third evaluation of Recommendation R (87) 15 of 2002.

[451] Report on the third evaluation of Recommendation R (87) 15 of 2002, Appendix VI, point 4.

[452] Principle 1.1. of Recommendation R (87) 15; With regard to the principles of Recommendation R (87) 15, compare Mayer (2001), pp. 49 and 50.

[453] Principles 1.2. and 1.3. of Recommendation R (87) 15.

[454] See Points 31–35 of the explanatory memorandum of Recommendation R (87) 15.

[455] Principle 1.4. of Recommendation R (87) 15.

[456] Principle 2.1. of Recommendation R (87) 15.

of data by the police. It elucidates the wording of Article 5 (c) of Convention No. 108 which stipulates that personal data must be adequate, relevant and not excessive in relation to the purpose for which they are stored.[457] The explanatory memorandum further specifies that the second principle of Recommendation R (87) 15 attempts to fix the boundaries to the exception provided for in Article 9 (2) lit. a of Convention No. 108 which allows a derogation from the principle that personal data must be adequate, relevant and not excessive in relation to the purpose for which they are stored in respect of the "suppression of criminal offences". The instrument insists that this exception must be limited to the collection of data being necessary for the prevention of a real danger or the suppression of a specific criminal offence, unless the law clearly authorises wider police powers to gather information.[458] Real danger is described as "not being restricted to a specific offence or offender but includes any circumstances where there is reasonable suspicion that serious criminal offences have been or might be committed to the exclusion of unsupported speculative possibilities."[459] By taking into account the *Leander* judgment of the ECtHR, principle two additionally requires the *notification* of the person concerned when data about him have been collected and stored without his knowledge, as soon as the object of the police activities would no longer be jeopardised.[460]

Principle three entails an important provision. In addition to the limitation that stored data have to be accurate and necessary to perform police tasks within the framework of national and international law, principle 3.3. distinguishes between data collected for administrative purposes and data collected for police objectives. It stipulates that both categories should be held in separate files and administrative data should not be subject to rules applicable to police data.[461] Data based on fact and data based on personal opinions and assessments should be clearly distinguished.[462] In the event of unavoidable mixing, point 53 of the explanatory

[457] Point 43 of the explanatory memorandum of Recommendation R (87) 15.

[458] Ibid.

[459] Point 43 of the explanatory memorandum of Recommendation R (87) 15 additionally gives an example to clarify the notion of real danger, real danger means "reasonable suspicion that unspecified drugs were being illegally brought into a country through a port by unidentified private yachts would justify the collection of data on all such yachts using that port, but not all yachts, their owners and passengers using every port in that country".

[460] Principle 2.2. of Recommendation R (87) 15 and Point 45 of the explanatory memorandum of Recommendation R (87) 15.

[461] Point 53 of the explanatory memorandum of Recommendation R (87) 15 clarifies that it would be wrong in principle to allow the special regime for police data, with its particular approach to data protection in the police sector, to extend to data collected for an administrative purpose.

[462] Point 52 of the explanatory memorandum of Recommendation R (87) 15: "Principle 3.2 encourages the implementation of a system of data classification. It is thought that it should be possible to distinguish between corroborated data and uncorroborated data, including assessments of human behaviour, between facts and opinions, between reliable information (and the various

memorandum of Recommendation R (87) 15 insists on the full application of general data protection rules provided for administrative storage.

Principle three therefore recognises the important distinction between data collected by the police and data collected for other purposes, such as administrative requirements. In light of existing attempts and developments in connection with the increasing data exchange between private actors, administrative authorities and police agencies, this principle should be borne in mind. Currently, data protection rules, which were once applicable to data collected in an administrative or economic context (such as PNR, telecommunications or immigration data), change at the very moment where the data are transferred to police authorities. In most cases, the individual will not be informed about the transfer or the associated change in the applicable rules.

The strict approach of provision three is further developed in the *fourth principle* which codifies a severe purpose limitation principle. Data collected and stored by the police should be used exclusively for police purposes, i.e. prevention and suppression of criminal offences or the maintenance of public order.[463] However, the absolute nature of this principle can be modified partly by principle five which deals with the communication of data.[464]

According to *principle five*, transfer of data to public parties depends on a legitimate interest, respectively on the above mentioned police purposes. It is permissible when the communication is undoubtedly in the interest of the data subject, the data subject has given its consent or where there is a clear presumption of such consent as well as to prevent a serious and imminent danger.[465] As principle five attempts to regulate the different forms of transfer while at the same time providing for general principles applicable to all data transfers, only slightly stricter derogations apply to the transfer to private parties.[466] Communication of data to foreign authorities should be restricted to police bodies and should only be allowed if there is a clear legal provision under national or international law.[467] In the absence of such a provision, the communication is must be necessary for the prevention of a serious and imminent danger or essential for the suppression of

shades thereof) and conjecture, between reasonable cause to believe that information is accurate and a groundless belief in its accuracy".

[463] Principle 4. of Recommendation R (87) 15 and Point 55 of the explanatory memorandum of Recommendation R (87) 15.

[464] Point 55 of the explanatory memorandum of Recommendation R (87) 15.

[465] Principles 5.2.i.–5.3.ii. of Recommendation R (87) 15.

[466] Point 56 of the explanatory memorandum of Recommendation R (87) 15; the communication to private parties should only be permissible, if, in a particular case, there exists a clear legal obligation or authorisation, or with the authorisation of the supervisory authority; furthermore communication is exceptionally permissible if, it is undoubtedly in the interest of the data subject, the data subject has given its consent or it exists a clear presumption of such consent as well as to prevent a serious and imminent danger (principles 5.3.i. and 5.3.ii.).

[467] Principle 5.4. of Recommendation R (87) 15.

a serious criminal offence under ordinary law.[468] When communicating the data to foreign police authorities, the data should not be used for purposes other than those specified in the request for communication. [469] The use for other purposes is subject to the prior conclusion of an agreement with the other party.[470] It is worth noting that the transfer of data to third states is not bound to a very strict purpose limitation principle which would have required to link the use of the data to the purpose for which they had been originally collected.

As a result of the Schengen Agreement, the Council of Europe completed principle five by enacting Recommendation 1181 on police co-operation and protection of personal data in the police sector in 1992.[471] Recommendation 1181 proposes the drafting of a Convention enshrining the principles of Recommendation R (87) 15 and applying these principles in the context of data exchange in the police sector between member states and between member states and third countries.[472] The standards of Recommendation 1181 mainly deal with the rights of the individuals and the respect of accuracy of data and the purpose limitation principle.[473] An independent authority outside the police sector equipped with full access to all relevant files should assure compliance with the principles set out in the proposed Convention. Although data exchange between member states and between member states and third countries increased enormously since 1992 and consequently the need for regulation in this field is even greater than in the 1990s, the project of a Convention dealing with principles for police data exchange in this context was never realised.

Principle five additionally regulates the conditions for communication providing for quality control of the data prior to the transfer. Data should be verified at the time of their communication at the latest. Inaccurate or outdated data should not be

[468] Ibid.

[469] Principle 5.5.iii. of Recommendation R (87) 15; Furthermore should the interconnection of files with files held for different purposes be subject to the grant of an authorisation by the supervisory body or should be in compliance with a clear legal provision, Principle 5.6. of Recommendation R (87) 15.

[470] Principle 5.5.iii. of Recommendation R (87) 15.

[471] Recommendation 1181 (1992) 1 on police co-operation and protection of personal data in the police sector of 11 March 1992.

[472] Recommendation 1181, point 7.

[473] Point 7. ii. of Recommendation 1181: a. data should be accurate, relevant, not exceed the purpose for which they are stored and, where necessary, kept up to date; b. they should be screened before they are stored; c. an individual should have the right to know whether personal data concerning him are kept; d. he should have an appropriate right of access to such data; e. he should have the right to challenge such data and, if necessary, have them rectified or erased; f. individuals who are denied access to files relating to them should have a right to appeal to an independent authority which has full access to all relevant files and which can and should weigh the conflicting interests involved; g. there should be an independent authority outside the police sector responsible for ensuring respect of the principles laid down in such a convention; iii. appeal to member states to ensure that data in the police sector may only be exchanged with other member states and with Interpol on the lines provided for in the proposed draft convention.

transferred. If data have been transmitted in spite of this, the communicating body must immediately inform the recipients of the incorrectness of the transferred data.

The *sixth principle* gives individuals a right of access, rectification and erasure. However, it entails certain restrictions such as the performance of the legal task of the police, the protection of the data subject and the rights and freedoms of others.[474] Where access is refused, the individual should have the possibility to appeal to an independent body.

Time limits for the storage and deletion of the data if they are no longer necessary for the purposes for which they were stored are provided for in *principle seven*. Several criteria should be taken into account when fixing the time limit: the need to retain data in light of the conclusion of an inquiry into a particular case, a final judicial decision, in particular an acquittal, rehabilitation, spent convictions, amnesties, the age of the data subject and particular categories of data.[475] In addition to regular checks on the quality of the data, *principle eight* provides for the general establishment of "necessary measures to ensure the appropriate physical and logical security of the data and prevent unauthorised access, communication or alteration".[476]

Especially the age criterion in principle seven could play a central role in future discussions about time limits of vast databases. Bearing in mind the decision *S. and Marper v. the United Kingdom* in which the ECtHR underlined the importance of a time limit to the storage in particular for data of younger persons, this criterion seems to become increasingly important.[477] Stigmatisation effects which can be the consequence of an entry in a police database might have a strong influence on the future life of young people. The United Kingdom violated Article 8 ECHR as it neither provided a time limit for the storage, nor for provisions making a distinction between the nature or gravity of the offence and the age of the suspected person.[478] With the increasing amount of various databases at national as well as at EU level, the time limit of entries and the age criterion provided for in Recommendation R (87) 15 and derived from the ECtHR case law, are important corrective factors to be considered in future projects of large databases.

b) Conclusion: Recommendation R (87) 15 – Essential Data Protection Principles for Police Cooperation at European Level

All in all, Recommendation R (87) 15 entails important and basic data protection principles for the police sector. Far too often those principles are restricted in the

[474] Principle 6.4. of Recommendation R (87) 15.

[475] Principle 7.1. of Recommendation R (87) 15.

[476] Principles 7.2. and 8. of Recommendation R (87) 15.

[477] *S. and Marper v. the United Kingdom*, Application nos. 30562/04 and 30566/04, judgment of 4 December 2008.

[478] Ibid, para 119.

case that a specific national or international law provides for a derogation.[479] However, three aspects deserve special attention:

Stipulated in principle one, comprehensive independent control and supervision established outside the police sector seems to be the most important tool to guarantee compliance with the principles. This principle regulates in detail the tasks necessary to fulfil effective oversight. In accordance with its wording, it refers only to supervisory authorities of the Member States, but bearing in mind the various references of EU instruments to Recommendation R (87) 15 and in light of present day conditions, the same principles should apply to supervisory authorities at the EU level.

Secondly, the strict limitation of the collection of data to police purposes for reasons such as the prevention of a real danger or the suppression of specific criminal offences is certainly more restrictive than the open scopes of today's data exchange mechanisms. Several examples are, amongst others, the Data Retention Directive, the Europol-US agreement on data and related information exchange, as well as the PNR agreement between the EU and the US.[480] More examples are given in Chap. C. A severe application of this principle excludes vague formulations and paraphrases of the purpose which can be found in more and more instruments dealing with the collection of (police) data. The explanatory memorandum expressly clarifies that this provision should prohibit the open-ended and indiscriminate collection of data by the police.[481]

A third important aspect concerns restrictions to the transfer of personal data. The data transferred to other public bodies, private parties and foreign authorities should not be used for purposes other than those specified in the request for communication.[482] This provision applies to all of the EU's police data exchange systems referring to Recommendation R (87) 15. Problems in this context may arise in two situations: Firstly, in particular third states do not always agree to a limited

[479] See e.g. principles 2.1.; 3.1.; 5.4. or 5.6.

[480] Directive 2006/24/EC of the European Parliament and of 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 2006, L-105/54; Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Unites States Department of Homeland Security (DHS), OJ 2007, L-204/18, in the following: EU-US PNR-Agreement of August 2007, OJ 2007, L-204/18; Europol-US Agreement on the exchange of personal data and related information of 2002.

[481] Point 43 of of the explanatory memorandum of Recommendation R (87) 15.

[482] Principle 5.5.iii. of Recommendation R (87) 15; Furthermore should the interconnection of files with files held for different purposes be subject to the grant of an authorisation by the supervisory body or should be in compliance with a clear legal provision, Principle 5.6. of Recommendation R (87) 15.

use of data once received.[483] Secondly, the purpose is described in a very broad manner not specifying the exact use.[484]

5. *Conclusion: Towards Basic ECHR Principles for Security-Related Data Processing*

The analysis of the Council of Europe's instruments, particularly the ECtHR's case law, shows that the protection of personal data is of fundamental importance to an individual's enjoyment of his or her right to respect for private and family life.[485] The protection of personal data within the framework of the Council of Europe has become commonly accepted and much more explicit in recent years. Above all, the case law of the ECtHR assures relatively comprehensive protection which is conducive to extracting principles of general application. When examining the justification of interferences with this right, the discretion conferred to the Member States has become narrower over the years and rights of individuals increasingly predominate over the interests of the State. Instruments such as the Convention No. 108 and Recommendation R (87) 15 complement the protection granted by Article 8 ECHR, even though they are limited in scope and not ratified by all EU Member States. In particular the principles of Recommendation R (87) 15 are of fundamental importance in respect to the references to this instrument made by almost all EU instruments dealing with the exchange of personal data in the police sector.[486]

The exemplary function of the ECtHR's case law is all the more important at the EU level, particularly in view of the previously limited competences of the European Courts in the former third pillar.[487] Seeing that the scope of the ECHR covered

[483] See for instance EU-US PNR-Agreement of August 2007, OJ 2007, L-204/18.

[484] Examples: EU-US PNR-Agreement of August 2007, OJ 2007, L-204/18; Europol-US Agreement on the exchange of personal data and related information of 2002, in particular Article 5 accessible at http://www.europol.europa.eu/index.asp?page=agreements (accessed February 2011) and Eurojust-US Agreement of November 2006, in particular Article 2, accessible at http://www.eurojust.europa.eu/official_documents/eju_agreements.htm (accessed February 2011).

[485] *Z. v Finland*, Application no. 22009/93, judgment of 25 February 1997, para 95; *Peck v. United Kingdom*, Application no. 44647/98, judgment of 28 January 2003, para 78; *L.L. v France* Application no. 7508/02, judgment of 10 October 2006, para 43; *Biriuk v Lithuania*, Application no. 23373/03, judgment of 25 November 2008, para 39; *I v Finland* Application no. 20511/03, judgment of 17 July 2008, para 38; *S. and Marper v the United Kingdom*, Application nos. 30562/04 and 30566/04, judgment of 4 December 2008, para 103; *C.C. v. Spain*, Application no. 1425/06, judgment of 6 October 2009, para 31; see also: Breitenmoser (1986), p. 245; Kugelmann (2003), p. 16 et seq.; Meyer-Ladewig (2006), Article 8, para 11; Moreham (2008), pp. 44–79.

[486] Exemplarily: Article 27 Council Decision of 6 April 2009 establishing the European Police Office, OJ 2009, L-121/37 etc.

[487] Compare Lenaerts (2010), in particular pp. 261–264.

the respect of fundamental rights in the law enforcement sector since its beginnings, the jurisdiction of the ECtHR could develop important principles over the last years while not being inhibited by the legal structure of the EU.

Whereas the analysis of the case law has shown that in general the ECtHR admits a wide margin of discretion to the Member States when national security is at stake, the interests of the parties however have to be reasonably balanced. Moreover, to be in accordance with the law, the measure in question must be "foreseeable", which means formulated with sufficient precision to enable an individual to regulate his conduct.[488] In the judgments related to governmental data collection and the implementation of surveillance measures in the framework of Article 8 ECHR, certain criteria stand out and must be fulfilled in order to guarantee proportionality and thus strive for a balance between the interests at stake. These criteria include the limitation on the categories of individuals against whom surveillance measures may be taken as well as the clear definition of the circumstances and limits of the storing and the use of the information before processing.[489] Time limits for storing are essential and the age of the person concerned must be taken into account to avoid indiscriminate storing of personal data in governmental databases.[490] Prior to surveillance measures and the collection of data in security-related data processing, it is crucial to determine which kind of data are to be stored and for which purposes the data should be used afterwards (purpose limitation principle).[491] Independent review and adequate and effective safeguards against abuse, including effective remedies, must exist to assure compliance with the rule of law.[492] Detailed provisions concerning the persons authorised to consult the files, the nature of the files, the procedure to be followed

[488] *Sunday Times v. the United Kingdom*, Application no. 6538/74, judgment of 26 April 1979, para 49; *Liberty and others v. the United Kingdom*, Application no. 58234/00, judgment of 1 July 2008, para 68; *Silver v. the United Kingdom*, Application no. 5947/72 and others, judgment of 25 March 1983, paras 85–88.

[489] *Segerstedt-Wiberg and others v. Sweden,* Application no. 62332/00, judgment of 6 June 2006, paras 88–92; *Liberty and others v. the United Kingdom*, Application no. 58234/00, judgment of 1 July 2008, para 68; *Rotaru v. Romania*, Application no. 28341/954, judgment of 4 May 2000, para 57; *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006, paras 116 and 127.

[490] *S. and Marper v. the United Kingdom*, Application nos. 30562/04 and 30566/04, judgment of 4 December 2008, para 119; *Segerstedt-Wiberg and others v. Sweden*, Application no. 62332/00, judgment of 6 June 2006, paras 89–92.

[491] *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006, para 116, *Rotaru v. Romania*, Application no. 28341/954, judgment of 4 May 2000, para 57; see also *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, Application no. 62540/00, judgment of 28 June 2007.

[492] *Rotaru against Romania*, Application no. 28341/95, judgment of 4 May 2000, paras 55–63; *Segerstedt-Wiberg and others v. Sweden,* Application no. 62332/00, judgment of 6 June 2006, para 121.

or the use that might be made of the information thus obtained are essential requirements which have to be fulfilled before ordering surveillance.[493]

In *Weber and Saravia v. Germany*, the ECtHR clarified amongst other, that the Bundesverfassungsgericht (German Federal Constitutional Court) only adequately counterbalanced an interference, provoked by the collection and transmission of security-related personal data to another authority, by strictly limiting the types of offences on behalf of which data transmission was permitted.[494] The restriction referred to the order of the Bundesverfassungsgericht that the law in question could only be applied and data could only be transmitted, if specific facts – as opposed to mere factual indications – aroused the suspicion that someone had committed one of the limited offences listed in a special article of challenged act.[495] In order to transmit data to other authorities, there is a requirement that the data be marked and remain connected to the purposes which had justified their collection[496] and that the transmission be recorded in minutes.[497] Explicit and detailed provisions relating to the hand out procedure, including a list of the authorities to which information may be communicated as well as the circumstances in which such communication may take place and the procedure to be followed were already important criteria applied in transfer cases, since the *Leander v. Sweden* case.[498]

With regard to the subsequent notification of individuals subject to surveillance measures, the ECtHR emphasises that this question is closely linked to the effectiveness of remedies before the courts and therefore to the existence of effective safeguards against the abuse of monitoring powers.[499] Again, in the case *Weber and Saravia v. Germany*, the ECtHR adds: "As soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, [. . .], information should be provided to the persons concerned".[500]

What often appears to be lost in the discussion about a common legislative data protection standard at the EU level is the absolutely central role played by ECtHR in Europe. The activity of the ECtHR in the context of national security and the prevention of disorder or crime the latter circumstances is of fundamental importance and plays a elementary role also in view of the instruments which have to be

[493] *Rotaru v. Romania*, Application no. 28341/954, judgment of 4 May 2000, para 57.

[494] *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006, para 129.

[495] Ibid, para 127.

[496] Ibid, para 121.

[497] Ibid, para 127.

[498] *Leander v. Sweden*, Application no. 9248/81, judgment of 26 March 1987, para 55.

[499] *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006, para 125: "since there is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively".

[500] *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006, para 135.

implemented at the EU level in former third pillar matters as demanded by Article 16 (2) TEU.[501] The Court creates an overarching standard and often has a role model character for both EU courts.[502] Due to the increasingly intense connection between EU law and the ECHR mentioned in the introduction (para I), the rules laid down by the ECtHR can be seen as a minimum data protection standard within the EU. Consequently, the European legislator can not step back and lag behind the criteria previously developed by the ECtHR.

Within the limits of the EU's competences, this responsibility applies as well in positive obligation cases as regards access, rectification and erasure rights. The case law regarding positive obligations visibly demonstrates that the ECtHR undoubtedly proceeds on the assumption that there are positive obligations to secure respect for private life by means of a system of data protection rules and safeguards.[503] Additionally, it has become less reluctant concerning the individual's right for a better understanding of the decisions which are taken to his or her detriment.

Finally, the combination of the different instruments of the Council of Europe – predominantly the case law of the ECtHR – assures the most comprehensive data protection approach in security-related data processing in Europe. The ECtHR specifies fundamental data protection principles when processing, storing and using personal information, thereby it increasingly abandons its case-by-case approach by stipulating more general principles which could be afterwards applied in similar cases and which serve as guiding principles for the EU and the Member States when enacting or reviewing their data protection legislation. This basic standard will be later used to assess the existing as well as the proposed instruments and measures of the actors in the AFSJ of the EU.

III European Union Standards

After having illustrated the ECHR data protection standards in security related data processing, the EU principles merit further attention. It is worth noting in advance that the EU data protection rules are to a great extent diversified and that the AFSJ

[501] Article 16 (2) TEU: "The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities. The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union".

[502] Compare with regard to the model character of the ECtHR case-law for Europol: Esser (2008); Case C-465/00, *Rechnungshof v. Österreichischer Rundfunk and Others*, judgment of 20 May 2003, para 10 and 19.

[503] *I. v. Finland*, Application no. 20511/03, judgment of 17 July 2008, para 37; *Segerstedt-Wiberg and others v. Sweden,* Application no. 62332/00, judgment of 6 June 2006 etc.

consists of a patchwork of different applicable rules making it difficult to illustrate the data protection instruments and principles in this area. However, it is worth noting that the EU's development of fundamental rights protection arose out of a case concerning the protection of private life interests.[504] The former pillar structure considerably influenced the scopes of the existing data protection instruments[505] as well as it limited the competence of the European Courts. As the power of the EU Courts in former Titles V and VI (common foreign security policy and police and judicial cooperation in criminal matters) of the EU Treaty was curtailed[506], far less case law with reference to security related data processing exists when comparing it to the ECHR. The few existing decisions are further elaborated in the following.

Another heritage of the former pillar structures relates to the fact that the main piece of legislation in EU data protection law, Directive 95/46, is not applicable to security related data processing. However, its principles represent fundamental data protection values and are often used as the framework of reference when adopting new data protection legislation in the EU. Thus, the following section focuses in a first section on the scopes of the instruments in force and analyses in a second section the principles applying to the whole or only to a part of the AFSJ. Differences between the scope and the guarantees of the diverse sources are duly considered. Included in the first section is the discussion of the important changes in relation to data protection brought by the entry into force of the Lisbon Treaty.

1. Main Data Protection Instruments in the AFSJ and Their Scope

a) Former First Pillar Protection

The Council of Europe developments in private life concerns and data protection rights influenced the efforts taken at EU level to adopt harmonised data protection standards. Even though, in contrast to the fundamental rights basis of the ECHR, the economic aspect of introducing unified standards to establish an internal market played an important role when adopting the key instrument of legislation regarding

[504] The *Stauder v. City of Ulm* case concerned a community scheme for the distribution of butter at reduced prices on the disclosure of the name of the recipient. *Stauder* complaint against the disclosure of his name and the Court of Justice interpreted that the community's scheme was not requiring such disclosure. The respect of Stauder's fundamental right to privacy constituted a general principle of community law and set forth to itself to annul an EC rules which went contrary to such principle, see Case 29–69, *Erich Stauder v. City of Ulm*, judgement of 12 November 1969.

[505] The scopes of the instruments are limited to specific contexts and different data protection principles apply in different situations; compare also Van den Wyngaert (2004), in particular p. 295; for a general overview of the AFSJ structure refer to Borchardt (2010), pp. 570–596.

[506] Compare Lenaerts (2010) in particular pp. 261–264.

data protection in Community law, the Data Protection Directive 95/46 in October 1995. The legal basis of Article 95 EC Treaty[507] (Article 114 TFEU) assured the participation of the European Parliament trough the co-decision procedure. Although having its roots in the harmonisation of the internal market, Directive 95/46 has a strong fundamental rights approach and was supposed to give "substance to and amplify" the principles contained in the Council of Europe Convention No. 108.[508]

Directive 95/46 covers data processing by automatic and non automatic means[509] by the Member States in (former) first pillar policies (for instance the VIS) and created the Article 29 Data Protection Working Party which examines questions relating to the interpretation of Directive 95/46 with the aim of contributing to a uniform application of the Directive.[510] Due to its pioneer character, the definitions and principles of Directive 95/46 are often a reference instrument for data protection provisions in other EU instruments. Later, the protection of personal data within the first pillar of the EU was reinforced by the adoption of the Directive on the protection of privacy in the telecommunications sector.[511] In 1997, the Amsterdam Treaty added Article 286 EC Treaty (Article 16 TFEU) which extended the application of the data protection principles contained in Directive 95/46 to personal data processed by European Community institutions and bodies. Based on this Article, Regulation 45/2001 was adopted which guarantees data protection in an EU-internal former first pillar context and established the European Data Protection Supervisor (EDPS)[512] as the authority responsible for overseeing data processing of the institutions an bodies at

[507] With regard to Article 95 EC Treaty, compare Bieber et al. (2006), pp. 264–268.

[508] Recital (11) of Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of the individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995, L-281/31, in the following: Directive 95/46, OJ 1995, L-281/31; the two approaches (fundamental rights and internal market) are reflected in the title of the Directive referring to the free flow of data as well as to the protection of individuals.

[509] Article 3 (1) Directive 95/46 covers not only data processing by automatic and non automatic means of personal data which form part of a filing system or are intended to form part of a filing system, it includes also data processing otherwise than by automatic means.

[510] Article 29 and 30 of Directive 95/46. OJ 1995, L-281/31.

[511] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector OJ 1998 L-24/1; replaced by 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 (Directive on privacy and electronic communications) OJ 2002, L-201/37 and amended by Directive 2006/24/EC of the European Parliament and of 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 2006, L-105/54.

[512] Hereafter referred to as EDPS.

Community level.[513] As a result of their first pillar status, AFSJ databases such as the VIS, Eurodac and partially the SIS (II) are monitored by the EDPS. Such as Directive 95/46, Regulation 45/2001 does not apply to legal persons.[514]

b) Scope of Directive 95/46 and Regulation 45/2001

Directive 95/46 as well as Regulation 45/2001 are pure (former) first pillar instruments. Regulation 45/2001 therefore exclusively relates to "the processing of personal data by all Community 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 Community law".[515] Directive 95/45 equally excludes Titles V and VI former TEU (common foreign and security policy and police and judicial cooperation) from the scope of Directive 95/46.[516]

Over the course of time, the scope of Directive 95/46 was further clarified by the case law of the Court of Justice. Initially ruling that the rights of Directive 95/46 go further than the mere exercise of economic activities (*Österreichischer Rundfunk/Lindqvist*[517]), the Court of Justice later restricted the Directive's scope to pure first pillar subjects by confirming the inapplicability of Directive 95/46 in cases of processing data for law enforcement purposes (*PNR case*).[518] The cases determining the scope of Directive 95/46 are briefly discussed in the following in chronological order.

In *Österreichischer Rundfunk,*[519] the Court of Justice not only underlined that the provisions of Directive 95/46 were to be interpreted in the light of Article

[513] European Parliament and Council Regulation (EC) 45/2001 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 2001, L-8/1 (referred to as Regulation 45/2001, OJ 2001, L-8/1 in the following).

[514] See case T-189/03, *Bank Austria Creditanstalt AG v. Commission*, judgment of 30 May 2006, para 95.

[515] Article 3 (1) Regulation 45/2001, OJ 2001, L-8/1, Article 3 (2) of Regulation 45/2001 adds that the "Regulation shall apply 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".

[516] Article 3 (2) Directive 95/46. OJ 1995, L-281/31.

[517] Case C-465/00, *Rechnungshof v. Österreichischer Rundfunk and Others*, judgment of 20 May 2003; Case C-101/01, *Lindqvist* of 6 November 2003.

[518] Joined cases C-317/04 and C-318/04, *Parliament v. Council*, judgment of 30 May 2006.

[519] In *Rechnungshof v. Österreichischer Rundfunk and Others* the Austrian Constitutional and Supreme Court requested a preliminary ruling on the questions: first, whether Directive 95/46 precludes national legislation requiring a public body (the ORF, a broadcasting organisation governed by public law) to collect and communicate data on income for the purpose of publishing the names and incomes of state employees and second, whether the provisions precluding national the legislation are directly applicable, in the sense that the persons obliged to disclose may rely on them to prevent the application of national provisions. The answer to the first question was that

8 ECHR[520] and that the Article 8 ECHR guarantees form part of the general principles of Community law,[521] the Court additionally emphasised that the Directive applies to a wide range of data processing cases without the need to prove in each specific case the connection to the internal market.[522]

The *Lindqvist* case[523] highlighted the wide scope of data protection in the (former) first pillar matters by restricting the scope of the exceptions provided for by Article 3 (2) of Directive 95/46. The exceptions apply to "the processing of personal data outside the scope of Community law, such as Titles V and VI of the Treaty on European Union[524] 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" as well as to processing "by a natural person in the course of a purely personal or household activity".[525] The Court of Justice underlined that, according to the first indent of Article 3 (2) Directive 95/46, the processing of data ouside of the scope of Community law only applies to those activities by the state mentioned by way of example in Article 3 (2) Directive 95/46 unrelated to the fields of an activity of individuals[526]: the "exception applies only to the activities which are expressly listed there or which can be classified in the same category (*ejusdem generis*)".[527] The Court of Justice

"Articles 6(1)(c) and 7(c) and (e) of Directive 95/46 do not preclude national legislation such as that at issue in the main proceedings, provided that it is shown that the wide disclosure not merely of the amounts of the annual income above a certain threshold of persons employed by the bodies subject to control by the Rechnungshof but also of the names of the recipients of that income is necessary for and appropriate to the objective of proper management of public funds pursued by the legislature, that being for the national courts to ascertain" and to the second question: "Article 6 (1)(c) and 7(c) and (e) of Directive 95/46 are directly applicable, in that they may be relied on by an individual before the national courts to oust the application of rules of national law which are contrary to those provisions", case C-465/00, *Rechnungshof v. Österreichischer Rundfunk and Others*, judgment of 20 May 2003, paras 94 and 101.

[520] Case C-465/00, *Rechnungshof v. Österreichischer Rundfunk and Others*, judgment of 20 May 2003, paras 10, 71 et seq.

[521] To the concepts of general principles, refer to Herdegen (2010), pp. 166–170.

[522] Case C-465/00, *Rechnungshof v. Österreichischer Rundfunk and Others*, judgment of 20 May 2003, para 42.

[523] In *Lindqvist*, Mrs. Lindqvist was charged with criminal violations of Swedish data protection law because she had published, on grounds of charitable and religious reasons, on the internet names, jobs, telephone numbers, medical problems etc. of her colleagues although she removed data in case somebody objected, case C-101/01, *Lindqvist*, judgment of 6 November 2003.

[524] Title V (Common Foreign and Security Policy) and Title VI (Police and Judicial Cooperation) former TEU.

[525] Article 3 (2) Directive 95/46.

[526] Case C-101/01, *Lindqvist*, judgment of 6 November 2003, paras 42–43.

[527] Ibid, para 43.

further held that the scope of Directive 95/46 includes the loading of personal data on a website as it constitutes processing by automatic means.[528]

In light of this relatively wide interpretation of the scope of Directive 95/46, the *PNR judgement* in 2006 was unexpected by many scholars.[529] The case dealt with a request for annulment by the European Parliament of a Council as well as a Commission Decision allowing for the transfer of flight passenger data (passenger name record (PNR)) from airlines to US American security authorities. The two decisions taken together approved the conclusion of an agreement with the USA in this regard (EU-US PNR agreement) and based on the first pillar legal basis of Article 95 EC Treaty (Article 114 TFEU) implying the application of Directive 95/46.

In contrast to the foregoing case-law, the Court of Justice came to a restrictive interpretation of the scope of Directive 95/46 and ruled that, although the data are collected and transferred by an economic operator (the airlines), the use and the purpose of processing of the data, and not the purpose initially justifying their collection, should decide about the legal basis allowing for conclusion of the EU-US PNR Agreement. It stipulated: "the transfer of PNR data [...] constitutes processing operations concerning public security and the activities of the State in areas of criminal law".[530] Therefore, the PNR data transfers were regarded as security-related third pillar data processing, excluding three important things: the participation of the European Parliament in the legislative process, the possibility to challenge fundamental rights violations before the Court of Justice and finally, the application of the data protection guarantees of Directive 95/46 to the PNR transfers.

By extending the exemption entailed in Article 3 (2) Directive 95/46 to the transfer of data of economic actors when they fall under a framework established by public security authorities,[531] the *PNR judgement* of the Court raises important questions regarding the protection of data collected by economic actors and later used for law enforcement purposes. The Court however decided not to address these questions.[532]

---

[528] Ibid, para 19.

[529] Hijmanns and Scirocco (2009), in particular p. 1503.

[530] Joined cases C-317/04 and C-318/04, *Parliament v. Council*, judgment of 30 May 2006, para 56; the Court added: "While the view may rightly be taken that PNR data are initially collected by airlines in the course of an activity which falls within the scope of Community law, namely sale of an aeroplane ticket which provides entitlement to a supply of services, the data processing which is taken into account [...] is, however, quite different in nature", as a result, the PNR transfers did not concern "data processing necessary for a supply of services, but data processing regarded as necessary for safeguarding public security and for law-enforcement purposes", see Joined cases C-317/04 and C-318/04, *Parliament v. Council*, judgment of 30 May 2006, para 57.

[531] Joined cases C-317/04 and C-318/04, *Parliament v. Council*, judgment of 30 May 2006, para 58.

[532] Compare Chap. D III 2 a.

The distinction between law enforcement data and data serving other purposes was confirmed in *Heinz Huber v. Germany* delivered by the Court of Justice in December 2008.[533] The Court clarified that data collected for a register serving public security, defence and fight against crime purposes do not profit from the protection of Directive 95/46.[534] Processing of personal data for the purposes of the application of legislation relating to the right of residence and for statistical purposes however falls within the scope of application of Directive 95/46.[535]

The understanding of the scope of Directive 95/46 in law enforcement related activities was again subject in the data retention case, *Ireland v. Parliament and Council* in 2009, where the choice of the legal basis of the Data Retention Directive 2006/24 was at stake.[536] Comparable to the *PNR case*, the Data Retention Directive, which harmonises the obligations of electronic providers to store and hold available traffic data for the (possible) later use for crime prevention purposes, was adopted on the basis of Article 95 EC Treaty (Article 114 TFEU).

Taking into account the EU-US PNR Agreement case, Ireland, supported by Slovakia, challenged the first pillar legal basis and asked the central question whether Directive 2006/24 should not have been based on a third pillar legal basis, because it regulates the data retention for law enforcement purposes, or whether the Parliament and the Council chose Article 95 EC Treaty as the correct legal basis. Article 95 EC Treaty can be generally invoked "when disparities exist between national rules which are such as to obstruct the fundamental freedoms or to create distortions of competition and thus have a direct effect on the functioning of the internal market".[537]

The Court rejected Ireland's argument and ruled that Directive 2006/24 regulates operations which "are independent of the implementation of any police and judicial cooperation in criminal matters"[538] and exclusively relate to the harmonization of the activities of service providers in the relevant sector of the internal market.[539] Despite of Article 1 of Directive 2006/24 which expressly states that it harmonises the Member States' provisions concerning the obligation of electronic communication service providers to store the "traffic and location data on both legal entities and natural persons" and "the related data necessary to

[533] Case C-524/06, *Heinz Huber v. Germany*, judgment of 16 December 2008, discussed in Sect. III 2 a aa.

[534] Case C-524/06, *Heinz Huber v. Germany*, judgment of 16 December 2008, para 45.

[535] Ibid.

[536] Case C-301/06, *Ireland v. Parliament and Council*, judgment of 10 February 2009; Directive 2006/24/EC of the European Parliament and of 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 2006, L-105/54.

[537] Case C-301/06, *Ireland v. Parliament and Council*, judgment of 10 February 2009, para 63.

[538] Ibid, para 83.

[539] Ibid, para 84.

identify the subscriber or registered userclient data" processed by them, "in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime",[540] the Court decided against Ireland. It distinguished between the retention and the storing of the data and its subsequent use and the access to them.[541] Only the retention and the storing determined the legal basis. Consequently, the Court of Justice approved the first pillar choice of Article 95 EC Treaty as the correct legal basis for the directive.

The two judgments taken together do not necessarily result in a consistent legal approach to law enforcement access to data collected for economic purposes[542] and have aroused substantiated criticism.[543] However, the case-law is kept legally simple and might bring more clarity on the dividing line between (former) first pillar data processing protected by Directive 95/46 and (former) third pillar data processing excluded from the Directive's scope.[544] The result is that on the one hand, instruments directly obliging private actors to transfer their data to law enforcement authorities are excluded from the scope of Directive 95/46 and on the other hand, instruments not directly regulating the access from law enforcement authorities, but the retention of economic data (even if they are intended to be subsequently used for other than economic purposes) can be included in the Directive's scope.

Finally, in *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy* the Court of Justice clarified once more that data serving an economic purpose fall under the protection of Directive 95/46. It stipulates: "The scope of application of Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data extends to the processing of personal data which consists in transferring onward on CD-ROM, in order for them to be used for commercial purposes, data on the earned and unearned income and the assets of natural persons which has been collected from documents in the public domain held by the tax authorities and processed for publication and which has already been published in the media. The scope of application of the directive also extends to the processing of such data for the purposes of a text-messaging service whereas mobile telephone users can, by sending a text message containing details of an individual's name and municipality of residence to a given number, receive those data."[545]

---

[540] Article 1 (1) and (2) Directive 2006/24/EC of the European Parliament and of 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 2006, L-105/54.

[541] Case C-301/06 *Ireland v. Parliament and Council*, judgment of 10 February 2009, para 84.

[542] Discussed in the Chap. D III 2.

[543] Simitis (2009); Hijmanns and Scirocco (2009).

[544] Hijmanns and Scirocco (2009), in particular p. 1506.

[545] Case C-73/07, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy*, judgment of 16 December 2008, summary of the judgment, para 3.

Summarising, the scope of Directive 95/46 is relatively comprehensibly defined in Article 3 of Directive 95/46. One issue requiring special attention so far relates to the interpretation of the exemptions with regard to the retention of data later used for law enforcement purposes. As long as the instrument only requires the retention of the data, without regulating the access to them, Directive 95/46 remains applicable. If an instrument directly obliges private actors to transfer their data to law enforcement authorities, the exemption of Article 3 (2) Directive 95/46 is applicable.

c) Framework Decision Governing Data Processing in Police and Cooperation

Data processing in former third pillar matters was for a long time exclusively governed by the aforementioned public international law instruments of the Council of Europe (Convention No. 108, Recommendation R (87) 15 and the ECHR standard).[546] After years of discussions and debates, the Data Protection Framework Decision 2008/977/JHA on personal data processed in the framework of police and judicial cooperation in criminal matters (FDPJ) was finally adopted in November 2008 with the intention to cover data processing in (former) third pillar matters.[547] Its provisions had to be transposed into national law by November 2010. The FDPJ is based on Article 30 (1) (b) EU Treaty (replaced by Articles 87 and 88 TFEU) requiring that collection and transfers of law enforcement information shall be subject to appropriate data protection measures.

The opportunity to create a legal data protection framework in the (former) third pillar was however missed.[548] This is mainly due to the restricted scope of the instrument which is neither applicable to the data processing of most of the AFSJ law enforcement agencies, such as Europol and Eurojust,[549] nor to other AFSJ

[546] With regard to the beginnings of the cooperation in criminal law, see Cullen and Jund (2002), pp. 23–34; with regard to the necessity to strengthen the judiciary in the EU, compare Braum (2009a).

[547] 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 2008, L-350/60 (in the following referred to as FDPJ, OJ 2008, L-350/60), equivalent to Directive 95/46, the processing refers to automatic and non-automatic processing of personal data, Article 2 (a) FDPJ.

[548] Hijmanns and Scirocco (2009), in particular pp. 1493–1496.

[549] Europol considers in recital (12) of Council Decision of 6 April 2009 establishing the European Police Office, OJ 2009, L-121/37: "A Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters will be applicable to the transfer of personal data by Member States to Europol. The relevant set of data-protection provisions in this Decision will not be affected by that Framework Decision and this Decision should contain specific provisions on the protection of personal data regulating these matters in greater detail because of the particular nature, functions and competences of Europol"; the equivalent at Eurojust is recital (13) Council Decision 2009/426/JHA of 16 December 2008 on

exchange systems, i.e. the SIS or the CIS.[550] The reason for this inapplicability is explained in Recital 39 FDPJ and relates to the fact that the aforementioned data exchange systems were adopted under Title VI of the TEU and "constitute a complete and coherent set of rules covering all relevant aspects of data protection".[551] Additionally excluded from the scope is the internal processing of the Member States in police and criminal matters. The FDPJ exclusively applies in a cross-border context, although for instance not in case of the Treaty of Prüm[552] establishing cross-border DNA information exchange between Member States.

Hijmans and *Scirocco* rightly raise the question how these limitations work in practice.[553] At the time of collection of the data by the Member State, the subsequent possible cross-border transfer of such data will often not be foreseeable. The standards of the FDPJ therefore do not have general application. In addition to the scope, there are several other shortcomings, discussed below, and principally involving the level of protection (e.g. specific conditions enacted prior to the FDPJ take precedence over the provisions of the FDPJ[554]) and the lack of specific rules in police and criminal cooperation.[555]

d) The Impact of the Lisbon Treaty on the AFSJ

The entry into force of the Lisbon Treaty influenced the aforementioned EU data protection framework in several ways. One of the major changes relates to the abolition of the pillar structure putting an end to the structural separation between

---

the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime, OJ 2009, L-138/4, stating that: "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 is applicable to the processing by the Member States of the personal data transferred between the Member States and Eurojust. The relevant set of data protection provisions of Decision 2002/187/JHA will not be affected by Framework Decision 2008/977/JHA and contains specific provisions on the protection of personal data regulating these matters in more detail because of the particular nature, functions and competences of Eurojust".

[550] FDPJ, OJ 2008, L-350/60, recital 39.

[551] FDPJ, OJ 2008, L-350/60, recital 39.

[552] The Treaty of Prüm was signed in May 2005 by seven Member States (Belgium, Germany, Spain, France, Luxembourg, the Netherlands and Austria), outside of the framework of the EU-Treaty and contains provisions about enhanced cross-border cooperation, particularly in combating terrorism and cross-border crime; in the meanwhile the provisions of the treaty have been transposed in EU law by Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ 2008, L-210/1.

[553] Hijmanns and Scirocco (2009), in particular p. 1494.

[554] Article 28 FDPJ, OJ 2008, L-350/60.

[555] See Sect. III 2.

"European Community" actions and "European Union" activities, a development which will largely influence data protection policy in the AFSJ.[556]

aa) Article 16 TFEU and Its Delayed Effects on the AFSJ

One important change for data protection law in the EU relates to the introduction of Article 16 TFEU stipulating a special legal basis which provides a subjective right to data protection being also applicable in the AFSJ.[557] Prominently placed in Title II on "provisions of general application", Article 16 provides in its paragraphs one and two that "everyone has the right to the protection of personal data concerning them" and that "compliance with these rules shall be subject to the control of independent authorities".[558] The European Parliament and the Council will "lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data".[559]

Although the wording of Article 16 TFEU might be of very general nature, it expressly recognises for the first time in European history at primary law level the need for rules on data protection, not only as it regards data processing within the European Institutions (former Article 286 EC Treaty), but also as regards processing by Member States. Requiring independent supervision and prescribing the ordinary legislative procedure, where Parliament and Council act as co-legislators, democratic principles are respected to a greater extent than before.[560] Article 16 TFEU applies to all data processing in public and private matters, including the AFSJ.

[556] For the general changes in the AFSJ, compare the excellent overview by Müller-Graff (2009); for an overview of the historical development of the AFSJ, see Streinz (2005), pp. 377–383; Schaper (2009), pp. 27–66.

[557] Scirocco (2008); a brief comment on Article 16 TFEU can be found in Lenz and Borchardt (2010), Commentary with regard to Article 16 TFEU, pp. 363–377; Geiger et al. (2010), pp. 211 and 212; Fischer (2010), pp. 221 and 222.

[558] Article 16 (1) and (2) TFEU.

[559] Full text of Article 16 TFEU: (1) Everyone has the right to the protection of personal data concerning them; (2) The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities. The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.

[560] Replacing Article 251 EC, which lays down the current co-decision procedure, the *ordinary legislative procedure* in Article 294 TFEU assures compulsory participation of the European Parliament, as well as of the Council acting by a qualified majority in the legislative process.

Its paragraph (2) however refers to Article 39 TEU.[561] This reference could nonetheless darken the expectations of the European Parliament and data protection authorities as regards a harmonised data protection approach to all former pillars, as it provides that in the common foreign and security policy (former second pillar), solely the Council will "adopt a decision laying down the rules relating to the protection of individuals with regard to the processing of personal data by the Member States when carrying out activities".[562] Consequently, the decision making procedure in this area will not include the European Parliament where data processing by Member States is concerned. According to the provision's wording, Article 16 TFEU seems however to remain fully applicable as regards data processing by European Institutions in the common foreign and security policy.[563]

Although, when turning to the effects of Article 16 TFEU on the AFSJ, despite of the clear advantage of having only one reference data protection standard disregarding the former (first or third) pillar specifics at first glance, there are regrettably several restrictions applying to the coherent application of Article 16 TFEU in the AFSJ. The obligation of Article 16 TFEU on the European Parliament and the Council to lay down the rules relating to data protection includes the AFSJ. However, various transitional provisions delay the effects of the full enforcement of Article 16 TFEU in this area. They are illustrated in the following.

Declaration 20 annexed to the Lisbon Treaty shows a certain hesitation as regards the application of Article 16 TFEU when it touches upon national security. The Declaration restrains Article 16 TFEU insofar as where rules on protection of personal data are be adopted on the basis of Article 16 which "could have direct implications for national security", due account needs "to be taken of the specific characteristics of the matter".[564] Declaration 21 goes even further and states that "the Conference acknowledges that specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 of the TFEU Union may prove necessary because of the specific nature of these fields".[565] It becomes clear from reading these Declarations that the Member States reserved a "back door" in national security matters as well as in police and judicial cooperation to enact other data protection rules in the AFSJ than those being possibly applicable to former first pillar matters.

Moreover, certain Member States exclude in a complicated way the application of Article 16 TFEU in specific cases. Protocol No. 21 annexed to the Lisbon Treaty

[561] Article 16 (2) TFEU stipulates that "the rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union".

[562] Article 39 TEU.

[563] Hijmanns and Scirocco (2009) in particular p. 1515 and Scirocco (2008).

[564] Declaration 20 of the Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, OJ 2010, C-83/335.

[565] Compare Declaration 21 of the Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, OJ 2010, C-83/335 (emphasis added).

provides for derogations for the United Kingdom and Ireland. Article 6 (a) of Protocol No. 21 states that both countries shall not be bound by the rules adopted on the basis of Article 16 TFEU "which relate to the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of that Treaty[566] where the United Kingdom and Ireland are not bound by the rules governing the forms of judicial cooperation in criminal matters or police cooperation which require compliance with the provisions laid down on the basis of Article 16".[567] This means if the United Kingdom or Ireland do not participate in specific aspects of police and judicial cooperation, they do not have to protect data in these areas either.[568]

A very complicated exception procedure applies additionally to Denmark. Article 2 (a) of Protocol No. 22 on the position of Denmark[569] refers to Article 2 of Protocol No. 22 and excludes that none of the provisions of Title V of Part Three of the TFEU[570] ("[...] no measure adopted pursuant to that Title, no provision of any international agreement concluded by the Union pursuant to that Title, and no decision of the Court of Justice of the European Union interpreting any such provision or measure or any measure amended or amendable pursuant to that Title [...]") shall be binding upon or applicable in Denmark.[571] This Article shall also apply in respect of the rules laid down on the basis of Article 16 TFEU which relate to the processing of personal data by the Member States.[572] As the United Kingdom and Ireland, Article 7 of the annex to Protocol No. 22 clarifies that Denmark is not bound by the rules of Article 16 when they relate to Chapter 4 or Chapter 5 of Title V of Part Three of the TFEU.[573]

Another important obstacle leading to a delay in the full application of the guarantees set out by Article 16 TFEU is stipulated in Protocol No. 36 on transitional provisions.[574] Its Title VII relates to transitional provisions concerning acts

[566] Chapter IV and V of Title V of Part III of the TFEU relate to judicial cooperation in criminal matters and police cooperation.

[567] Article 6 (a) Protocol No. 21 annexed to the Lisbon Treaty on the position of the United Kingdom and Ireland in respect of the Area of Freedom, Security and Justice, OJ 2010, C-83/201.

[568] With regard to the opt-outs compare Monar (2009), in particular pp. 773–776.

[569] Protocol No. 22 annexed to the Lisbon Treaty on the position of Denmark, OJ 2010, C-83/201.

[570] Title V of Part III of the TFEU includes the AFSJ.

[571] Article 2 Protocol No. 22 annexed to the Lisbon Treaty on the position of Denmark, OJ 2010, C-83/201.

[572] Ibid.

[573] Article 7 of the annex of Protocol No. 22 annexed to the Lisbon Treaty on the position of Denmark, OJ 2010, C-83/201 stipulates that: "Denmark shall not be bound by the rules laid down on the basis of Article 16 of the Treaty on the Functioning of the European Union which relate to the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of that Treaty where Denmark is not bound by the rules governing the forms of judicial cooperation in criminal matters or police cooperation which require compliance with the provisions laid down on the basis of Article 16".

[574] Protocol No. 36 annexed to the Lisbon Treaty on transitional provisions, OJ 2010, C-83/201.

adopted on the basis of Titles V and VI of the former TEU (common foreign and security policy and police and judicial cooperation in criminal matters) prior to the entry into force of the Lisbon Treaty. Article 9 of the Protocol No. 36 provides that the legal effects of the acts adopted before the entry into force of the Lisbon Treaty shall be preserved until those acts are repealed, annulled or amended.[575] A deadline to adapt the old instruments to the new Treaty provisions, for instance in case they do not comply with Article 16 TFEU, is not given.[576]

With respect to acts in the field of police cooperation and judicial cooperation in criminal matters adopted before the entry into force of the Treaty of Lisbon, the powers of the Commission under Article 258 TFEU (the Commission's right to enact infringement proceedings) as well as the limited powers of the Court of Justice under Title VI of the former TEU shall remain the same.[577] In this case, the transitional measure shall cease to have effect 5 years after the date of entry into force of the Treaty of Lisbon.[578]

The result of these transitional provisions is that the rules and instruments adopted prior to the Lisbon Treaty (as long as they are not modified) as well as the former situation as regards the curtailed power of judicial control in the former third pillar matters (for a maximum period of 5 years) remain untouched.[579] Having this in mind, from the perspective of the Member States, one understands the enormous legislative activity having taken place shortly prior to the entry into force of the Lisbon Treaty which led to the adoption of partially questionable decisions in terms of data protection in former third pillar matters.[580] Many instruments in the AFSJ (Europol and Eurojust Decisions, including their implementing measures, Decision allowing for law enforcement access to the VIS etc.[581]) were quickly adopted before the new provisions stipulated in the

[575] Article 9 Protocol No. 36 annexed to the Lisbon Treaty on transitional provisions, OJ 2010, C-83/201 states that: "The legal effects of the acts of the institutions, bodies, offices and agencies of the Union adopted on the basis of the Treaty on European Union prior to the entry into force of the Treaty of Lisbon shall be preserved until those acts are repealed, annulled or amended in implementation of the Treaties. The same shall apply to agreements concluded between Member States on the basis of the Treaty on European Union".

[576] A five years deadline is only mentioned in Article 10 (3) Protocol No. 36 referring exclusively to the powers of the Commission and the European Court of Justice.

[577] Article 10 (1) Protocol No. 36 annexed to the Lisbon Treaty on transitional provisions, OJ 2010, C-83/201.

[578] Ibid.

[579] Only Member States that made a declaration according to Article 35 (2) former TEU accepting the jurisdiction of the European Court of Justice, can continue to request a preliminary ruling relating to the validity or interpretation of an instrument enacted in this area before the entry into force of the Lisbon Treaty.

[580] This point is further discussed in the analysis of the legal basis of the AFSJ actors, in particular in Chap. B II 1 and B II 2.

[581] This is further discussed in the analysis of the legal basis of the AFSJ actors in Chaps. B II 1, B II 2 and C II 2.

Lisbon Treaty, providing for more democratic control as well as for improved legislative procedures, entered into force. In consequence, even instruments not complying with the data protection guarantees of Article 16 TFEU in the AFSJ, will remain applicable until they are modified, repealed or annulled. This affects for instance instruments such as the FDPJ which is inapplicable to domestic data processing in police and judicial matters.

Taking the above-mentioned into account, the (legal) dimension of Article 16 TFEU in terms of its exemplary effect should nevertheless not be underestimated. Its position in the principles of general application underlines the respect of data protection principles in future legislation, including proposals in the AFSJ. *Hijmans* and *Scirocco* highlight the possible direct effect Article 16 (1) TFEU could have[582] and conclude this will limit the margin of appreciation of the legislature and would lead to the possibility to invoke this right before a court. The mandate of the Parliament (and the Council) to enact data protection rules in the AFSJ will hopefully accelerate the development towards effective and harmonised data protection rules in the AFSJ.

Finally, even though Article 16 TFEU constitutes an enormous step towards the recognition of essential data protection principles in the AFSJ, its guarantees have to be specified to help enforcing the rights of the individuals in the AFSJ. The interpretation of such broad principles, as carried out by the ECtHR in recent years with regard to data protection, could support this process in a valuable way.

bb) Important Changes in Respect of the Entire AFSJ

Keeping the mentioned restrictions in mind, with respect to the entire AFSJ, regulated in Title V, Articles 67–89 TFEU, the Lisbon Treaty brings a number of important developments briefly summarised in the following[583]:

– The introduction of the ordinary legislative procedure in the entire AFSJ reinforces the long demanded democratic control by strengthening the role of the European Parliament. In contrast to the former third pillar, Council and Parliament act as co-legislators in the AFSJ. Article 87 (2) (a) expressly states that the European Parliament and the Council shall act together in accordance with the ordinary legislative procedure to establish measures concerning "the collection, storage, processing, analysis and exchange of relevant information" in police cooperation.

[582] The authors compare the direct wording of Article 16 (1) TFEU with the direct wording in Article 18 (1) EC Treaty (the right of the EU citizen to move and reside freely within the territory of the Member States, now Article 21 TFEU) to which the Court acknowledged a direct effect and conclude that Article 16 (1) is formulated in the same precise manner allowing also to concede a direct effect to it, see Hijmanns and Scirocco (2009), in particular pp. 1517–1518; with regard to the direct effect of EU primary law, compare Herdegen (2010), pp. 164–166.

[583] A good overwiev on the changes in the AFSJ is made by: Niemeier (2010); Müller-Graff (2009); Callies (2010), pp. 431–452.

- The expansion of the decisions taken by qualified majority in the Council and the reinforcement of the right of initiative of the Commission raise hopes that decisions less frequently base on the lowest common denominator in data protection matters. However, Article 76 TFEU (general provisions in the AFSJ) maintains the right of initiative of the Member States with regard to acts ensuring administrative cooperation in the AFSJ, although a threshold of one quarter of the Member States applies.
- Article 82 (3) and 83 (3) TFEU concerning judicial cooperation however introduce a so-called emergency brake[584]: Where a member of the Council considers that a draft directive would affect fundamental aspects of its criminal justice system, it may request that the draft directive be referred to the European Council. In that case, the ordinary legislative procedure shall be suspended. After discussion, and in case of a consensus, the European Council shall, within 4 months of this suspension, refer the draft back to the Council, which shall terminate the suspension of the ordinary legislative procedure.[585]
- Articles 86 (1), 87 (3) and 89 (1) TFEU additionally provide for unanimity decisions of the Council when it comes to the adoption of a European Public Prosecutor's Office, when measures concerning the operational cooperation between police authorities should be established and when the conditions and limitations regarding the extent to which national enforcement agencies can operate on the territory of another Member State are laid down.
- The reinforcement of the role of national Parliaments stipulated in Articles 12 TEU and 69 TFEU in the AFSJ leads to additional democratic accountability. Article 12 (c) TEU explicitly mentions the role of the national Parliaments in the framework of the AFSJ by taking part in "the evaluation mechanism for the implementation of the Union policies in that area" and "through being involved in the political monitoring of Europol and the evaluation of Eurojust's activities".[586] Articles 85 (1) and 88 (2) TFEU specify these tasks by referring to the involvement of the national Parliaments in the legislative process determining Eurojust's and Europol's structure, operation, field of action and tasks. The control of Eurojust's and Europol's activities by the EP and the national Parliaments will therefore increase and shall be established in the future in form of Regulations amending the current Council Decisions.
- The removal of the restrictions relating to the judicial control by the Court of Justice[587] and the possibility to enact infringement proceedings[588] in the area of

[584] Hijmanns and Scirocco (2009), in particular p. 1522.

[585] Articles 82 (3) and 83 (3) TFEU.

[586] Article 12 (c) TEU.

[587] Compare case C-160/03, *Spain v. Eurojust*, judgment of 15 March 2005, in which the Court confirmed that the acts of (former) third pillar bodies (in this case, Eurojust) did not fall within its competence.

[588] Articles 258 and 259 TFEU.

police and judicial cooperation, considerably increase procedural legitimacy and will certainly support the enforcement of decisions taken in the AFSJ.[589]

- After the transition period has expired, judicial control of the AFSJ's actors, in particular the control of the AFSJ agencies will be considerably improved by the Lisbon Treaty. The former restricted area of actions (infringement proceedings, action for annulment, complains for failure to act) which may be brought before the European Union Courts will be extended to the AFSJ.[590]
- It is also worth pointing out that the competences of the European Ombudsman which include the investigation of maladministration of the activities of EU institutions, bodies and agencies[591] will refer to bodies such as Europol and Eurojust. Every citizen of the EU or any natural or legal person residing (or having its registered office) in a Member State can address its complaint to this body.
- A further and very important improvement concerns the adoption of international Agreements in the AFSJ. They will be subject to a reinforced democratic control. According to Article 218 (6) (a) (v) TFEU the European Parliament has to give its consent to international agreements in all fields where the ordinary legislative procedure applies. Consequently, the European Parliament will have the possibility to examine in the area of police and judicial cooperation, if a third state (or organisation) agreement complies with satisfying data protection standards as well as to block such agreements in case they fail to ensure a sufficient level of protection. Such agreements will additionally fall within the competence of the Courts of the EU, establishing the opportunity to obtain an opinion of the Court on the compatibility of envisaged provisions of the agreement with the Treaties.[592]
- The establishment of the permanent standing committee, COSI (Comité de sécurité intérieur) in Article 71 TFEU coordinating the internal security policy

[589] The protocol (No 36) on transitional provisions delays can delay the entry into force of some of the provisions mentioned above, especially Article 9 and 10.

[590] Article 263 (1) TFEU provides for the possibility of legal review of the acts of EU bodies, offices and agencies "intended to produce legal effects vis-à-vis third parties" (action for annulment) and Article 265 (1) TFEU regulates the action for a failure to act for the mentioned actors. Article 267 (1) (b) TFEU which permits preliminary rulings on the validity and interpretation of acts of the institutions, bodies, offices and agencies, paves the way for a reinforced external control in the future. And, although Article 263 (5) TFEU restricts the review of the legality of the legal acts by stipulating that "acts setting up bodies, offices and agencies of the Union may lay down specific conditions and arrangements concerning actions brought by natural or legal persons against acts of these bodies, offices or agencies intended to produce legal effects in relation to them", the general situations of individuals concerned has been significantly ameliorated, not least because Article 16 TFEU is now applicable to the entire data processing of the AFSJ.

[591] Article 228 (1) TFEU.

[592] Hijmanns and Scirocco (2009), in particular p. 1522.

could contribute to a more harmonised approach to decisions taken in the AFSJ, including harmonised proposals on data protection in this area.[593]

Especially with regard to the former third pillar area, decision making under the Lisbon Treaty will in future pave the way for the adoption of a hopefully satisfying general fundamental rights framework in the AFSJ.[594] Prior to the adoption of the Treaty, the Council's unanimity power with bare consultation rights of the European Parliament in this area, often resulted in compromises on the "lowest common denominator" hindering the implementation of clear and effective data protection provisions.[595] The transitional provisions applying in the AFSJ however represent the concerns of the Member States regarding the transfer of powers to the EU in this special area and will delay the positive effects of Article 16 TFEU for some time.

Therefore, regardless of the adoption of the Lisbon Treaty, the current legal framework of data protection provisions in the EU is (still) characterised by the former pillar structure. It will take some time to overcome the traditional separation between the protection of personal data in former Community matters and police and judicial cooperation matters. However, the chances to improve the current framework are better than ever before.

All things considered, despite these shortcomings, the adoption of the Lisbon Treaty was an important step forward towards the respect of data protection rights in the AFSJ. The mandate of the Parliament and the Council to adopt data protection rules will require a thorough analysis of the existing data protection framework in the AFSJ and may lead in future to a general framework for data protection in this area. The elements laid down in Article 16 clearly need specification. The analysis of the data protection systems in the current AFSJ carried out in Chap. B may provide some assistance in this respect.

e) Charter of Fundamental Rights and Guarantees of the ECHR

In addition to Article 16 TFEU, the new statuses of the European Charter of Fundamental Rights[596] (Charter) and the ECHR enforce the role of data protection as a fundamental right. Additionally, the new Article 6 (1) TEU clearly concedes binding value to the Charter by stating that the Charter "shall have the same legal value as the Treaties".[597] The same article read together with Protocol No. 8 annexed to the Lisbon Treaty additionally lays down the Union's obligation to

[593] The first meeting of COSI took place in March 2010, further meetings are planned.

[594] Scirocco (2008).

[595] Scirocco (2008); the analysis of instruments prior to the adoption of the Lisbon Treaty is carried out in Sect. III.

[596] A general overview of the Charter gives Craig and De Burca (2008), pp. 412–417.

[597] For details and the historical background, compare Wentrup Große (2003), pp. 31–47; Gebauer (2007); Pache (2009); Heusel (2002); Kokott and Sobotta (2010).

accede to the ECHR.[598] Both instruments refer to the necessity of protection of personal data, whereas the Charter specifies in a slightly more detailed manner than Article 8 ECHR, the core values of the European data protection consensus.

As mentioned in the introduction, Article 8 (1) of the Charter ascertains that "everyone has the right to the protection of personal data concerning him or her". Its paragraph (2) specifies that "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 must have the right of access and the right of rectification.[599] Compliance with these rules shall be subject to control by an independent authority.[600]

The Charter is applicable to the institutions, bodies, offices and agencies of the EU and the Member States when they are implementing EU law.[601] Data protection is therefore recognised as a fundamental right in the entire European Union, regardeless of the former pillar strucutures.[602] Thus the Charter and the guarantees of its Article 8 are the first provision extending the respect of data protection rights also to former second and third pillar matters. Fomer third pillar agencies such as Europol and Eurojust are therefore subject to the provisions of the Charter.[603]

Comparable to the restrictions applying to Article 16 TFEU, certain Member States exclude the application of the Charter to them. Protocol No. 30 limits the extension of the rights of the Charter in Poland and in the United Kingdom.[604] As with regard to Article 16 TFEU, both countries may retrieve their submission under the Charter's regime, although Poland – in contrast to the United Kingdom – has not excluded the application of the data protection provisions of Article 16 TFEU in the AFSJ. Consequently, there is some contradiction in Poland's approach as regards data protection guarantees. From the remaining applicability of Article 16 TFEU follows however that Poland will necessarily accept the instruments enacted based on Article 16 TFEU.

It is worth noting that data protection is stipulated as a right in itself and is not annexed to the right to private life which is additionally mentioned in Article 7 of the Charter. Data protection is to be understood as an element of the right to private

[598] Article 6 (2) TEU and Protocol No. 8 annexed to the Lisbon Treaty relating to Article 6 (2) of the Treaty on European Union on the accession of the Union to the European Convention on the Protection of Human Rights and Fundamental Freedoms, OJ 2010, C-83/201.

[599] Article 8 (2) Charter of Fundamental Rights, OJ 2010, C-83/02.

[600] Article 8 (3) Charter of Fundamental Rights, OJ2010, C-83/02; for a general overview of the guarantees of Article 8 of the Charter, see Rengeling and Szczekalla (2004), § 16, pp. 453–496; Callies and Ruffert (2007), pp. 2563–2568.

[601] Article 51 (1) 52 of the Charter of Fundamental Rights, OJ 2010, C-83/02; Jarass (2010), Article 8, para 3; for details compare Wentrup Große (2003), pp. 44 and 49.

[602] Meyer (2011), Article 8, para 1.

[603] The relevance of the Chater for the activities of Europol and OLAF is emphasised by Paeffgen (2006), in particular p. 78.

[604] Protocol No. 30 annexed to the Lisbon Treaty on the application of the Charter of Fundamental Rights of the European Union to Poland and to the United Kingdom, OJ 2010, C-83/201.

life which is however particulary important and it therefore needs to be mentioned in a proper article.[605] Article 8 of the Charter is consequently described as the *lex specialis* of Article 7 of the Charter.[606]

The guarantees inherent to Article 8 of the Charter are based on Article 286 EC Treaty, Directive 95/46, Article 8 ECHR and Convention No. 108.[607] The explanation of the Praesidium specifies that the right to the protection of personal data is to be exercised under the conditions of Directive 95/46 and may be limited under the general conditions set out by Article 52 of the Charter. The article lays down that the limitations on the rights and freedoms of the Charter "must be provided for by law and respect the essence of those rights and freedoms".[608] "Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interests recognised by the Union or the need to protect the rights and freedoms of others".[609]

Article 52 of the Charter additionally underlines the close connection of the rights stipulated in the Charter and the rights of the ECHR. In so far as the Charter contains rights which correspond to the rights of the ECHR, "the meaning and the scope of those rights shall be the same as those laid down by the Convention [ECHR]".[610] With regard to the data protection guarantees in EU law, the recent judgment of the European Court of Justice in the case *Schecke v. Land Hessen*[611] confirmed the close relationship between Article 8 ECHR and Article 8 of the Charter. The case concerned the legality of several regulations in the area of the common agricultural policy[612] which obliged national authorities to publish a set of personal data belonging to beneficiaries of EU agricultural subsidies in order to improve the transparency of the Union's financial support system. In Germany, the

[605] Meyer (2011), Article 8, para 6.

[606] Meyer (2011), Article 8, para 13; Jarass (2010), Article 8, para 4.

[607] Note from the Praesidium of the Convention, Explanation on the Charter of Fundamental Rights of the European Union, Draft Charter of Fundamental Rights, CHARTE 4473/00 CONVENT 49 of 11 October 2000; Jarass (2010), Article 8, para 1.

[608] For a deepened understanding of Article 52 (3) of the Charter and of the influence of the ECHR on the Charter of Fundamental Rights, Ziegenhorn (2009); Schneiders (2010).

[609] Article 52 (1) of the Charter of Fundamental Rights, OJ 2010, C-83/02; with regard to Europol and its possibility to justify interferences with regard to Article 8 of the Charter, compare Kistner-Bahr (2010), pp. 227–232.

[610] Article 52 (3) of the Charter of Fundamental Rights, OJ 2010, C-83/02.

[611] Joined cases C-92/09 and C-93/09, *Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen*, judgement of 9 November 2010.

[612] Council Regulation (EC) No 1290/2005 of 21 June 2005 on the financing of the common agricultural policy, OJ 2005, L-209/1, as amended by Council Regulation (EC) No 1437/2007 of 26 November 2007, OJ 2007, L-322/1 and Commission Regulation (EC) No 259/2008 of 18 March 2008 laying down detailed rules for the application of Regulation No 1290/2005 as regards the publication of information on the beneficiaries of funds deriving from the European Agricultural Guarantee Fund (EAGF) and the European Agricultural Fund for Rural Development (EAFRD), OJ 2008, L-76/28.

Federal Office for Agriculture and Food therefore made names, postcodes and amounts received public on a (searchable) website. The farmers and agricultural firms concerned claimed that the publication requirement violated their rights to private life of Article 7 of the Charter and to the protection of personal data of Article 8 of the Charter.

The Court states that: "Finally, according to Article 52 (3) of the Charter, in so far as it contains rights which correspond to rights guaranteed by the Convention, the meaning and scope of those rights are to be the same as those laid down by the Convention. Article 53 of the Charter further states that nothing in the Charter is to be interpreted as restricting or adversely affecting the rights recognised inter alia by the Convention".[613] More specifically, in the context of the legal standards following from the new Articles 7 and 8 of the Charter, the Court stipulates that: "[. . .] it must be considered that the right to respect for private life with regard to the processing of personal data, recognised by Articles 7 and 8 of the Charter, concerns any information relating to an identified or identifiable individual [. . .] and the limitations which may lawfully be imposed on the right to the protection of personal data correspond to those tolerated in relation to Article 8 of the Convention".[614]

Without going into the details of the *Schecke* case, it is worth noting the Court applies the ECtHR method and examines first, the existence and second, the justification of an interference with the rights to private life and data protection stipulated in the Charter. In essence, the Court observes that the publication of the data of the beneficiaries of EU subsidies "with no distinction being drawn according to the duration, frequency or nature and amount of the aid received" did not succeed in striking the right balance between the interests involved.[615] Institutions are obliged to balance, before disclosing information relating to individuals, "the European Union's interests in guaranteeing transparency of its actions and the infringements of the rights recognised by Articles 7 and 8 of the Charter".[616] The respective provisions of the regulations were for that reason declared void.

As follows from the foregoing, the data protection principles and guarantees of Article 8 ECHR and Directive 95/46, which are specified in the case law of the EU Courts and the ECtHR, are therefore of utmost importance when the principles mentioned in Articles 7 and 8 of the Charter should be further clarified by the EU Courts in future. For that reason, the case law of the ECtHR was illustrated in detail above.

This statement and the intended accession to the ECHR will therefore change the acceptance of the right to data protection in future European Union fields of action.[617] European Union Institutions will be directly bound by the provisions of the ECHR and their acts will be subject to critical scrutiny of the ECtHR. Besides,

[613] Joined cases C-92/09 and C-93/09, *Volker and Markus Schecke GbR and Hartmut Eifert* v. *Land Hessen*, judgement of 9 November 2010, para 51.

[614] Ibid, para 52.

[615] Ibid, paras 79–89.

[616] Ibid, para 85.

[617] With regard to the general changes, compare Lock (2010), pp. 777–798.

Article 6 (3) states that fundamental rights, "as guaranteed by the ECHR" and "as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's law".[618]

Even though in *Rechnungshof v. Österreichischer Rundfunk and Others*, the European Court of Justice already recognised that the provisions of Directive 95/46 were to be interpreted in the light of Article 8 ECHR and that the guarantees of Article 8 ECHR form part of the general principles of Community law, European Union Courts will have to respect the principles laid down in the ECHR more than ever before. Thus far the ECtHR could only assess EU law indirectly by ruling on the implementation of EU law in a Member State. When the EU accedes to the ECHR, individual challenges of the acts of EU institutions and even of judicial decision of the European Union Courts before the ECtHR become possible. Although the accession is important, it will not lead to a substantial change of the case law of the EU Courts in data protection matters.[619] As stipulated above, the ECHR and the guarantees of the ECHR and the case law of the ECtHR are already incorporated into EU law (*Rechnungshof v. Österreichischer Rundfunk and Others*).

2. *EU Data Protection Principles in the AFSJ*

The following section focuses on the brief analysis of the existing data protection principles in the EU which are relevant in the AFSJ context.[620] There is no conclusive or definite set of EU data protection principles.[621] Therefore the following section orientates on the main piece of legislation in the EU, Directive 95/46. As demonstrated above, it has to be recalled that the scope of Directive 95/46 is however limited and does not refer to security-related data processing in the AFSJ. Its principles, which are a further development of the principles of Convention No. 108, are nevertheless worth mentioning, taking into consideration that they lay down the foundations of EU data protection rules and that they are applicable to instruments such as the VIS or Eurodac. The other instruments including data protection provisions relevant in the AFSJ are Regulation 45/2001 and the FDPJ. Regulation 45/2001, covering data processing at the Community institutions and bodies, mirrors most of the principles of Directive 95/46. The FDPJ equally bases on the Directive's principles, although it refers to them in a very mitigated way as the following analysis will demonstrate.

---

[618] For a detailed analysis of the meaning of the term "general principles" of EU law, refer to Schneiders (2010), pp. 44–95.

[619] Hijmanns and Scirocco (2009), in particular p. 1523.

[620] It will not consider all the details of the history of EU data protection law. This would go beyond the interest of this research. For an excellent overview of the origins of Directive 95/46, see Dammann and Simitis (1997); for a general overview of EU data protection law, refer to Siemen (2006).

[621] Brouwer (2008a), p. 204.

a) Quality Standards

Quality standards of European data protection rules are central to the processing of personal data. They are enumerated in Article 6 of Directive 95/46 and mainly contain the principles of Article 5 Convention No. 108. Personal data must be "processed fairly and lawfully, collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; accurate and, where necessary, kept up to date". Further, "every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified; kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed".

These criteria are specified in the aforementioned case law of the Court of Justice, which takes into account particularly the principle of proportionality[622] and the respect of fundamental rights as stipulated in Article 6 EU Treaty, especially Article 8 ECHR.[623]

aa) Lawfulness and Fairness

The requirement to process personal data lawfully is not only mentioned in Directive 95/46,[624] but also in Regulation 45/2001 and the FDPJ.[625] It signifies that data processing is based on the condition of lawfulness and requires from the Member States the enforcement of existing data protection rules as well as the enactment of new rules, if necessary.[626] Some criteria for making data processing legitimate are

[622] For details, see Koch (2003); Von Arnauld (2008) and Case C-275/06, *Productores de Música de España Promusicae vs. Telefónica de España*, judgment of 29 January 2008, paras 68–70. In *Promusicae vs. Telefónica de España* the Court of Justice stipulated that when transposing intellectual property directives, Member States must interpret them in a form "which allows a fair balance to be struck between the various fundamental rights protected by the Community legal order. Further, when implementing the measures transposing those directives, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with those directives but also make sure that they do not rely on an interpretation of them which would be in conflict with those fundamental rights or with the other general principles of Community law, such as the principle of proportionality" (para 70).

[623] Case C-465/00, *Rechnungshof v Österreichischer Rundfunk and Others*, judgment of 20 May 2003, paras 66, 70, 71, 93 and 99. The Directive refers to the European Convention on Human Rights to "give substance to and amplify" the principles contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic processing of Personal Data (recitals 10 and 11 of Directive 95/46, OJ 1995, L-281/31).

[624] Article 6 (1) (a) Directive 95/46, OJ 1995, L-281/31.

[625] Article 3 (1) FDPJ, OJ 2008, L-350/60 and Article 4 (1) (a) Regulation 45/2001, OJ 2001, L-8/1.

[626] Dammann and Simitis (1997), Article 6, para 2.

further detailed in Article 7 of Directive 95/46 and Article 5 of Regulation 45/2001.[627] Data processing is for instance legitimate, if the data subject has unambiguously given his consent, the processing is necessary in order to protect the vital interests of the data subject or the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed.[628] There is no requirement that the data processing must in any case have a legal basis, but it must always be in accordance with the applicable law. It is worth reminding that the ECtHR's case law, however, provides for stricter criteria with regard to the legal basis of data processing to ensure foreseeability.[629]

Nonetheless, the Court of Justice also stipulated certain criteria relating to the lawfulness of data processing. In *Huber v. Germany*, the Court of Justice makes clear that the concept of necessity in Article 7 of Directive 95/46 cannot have a meaning which varies between the Member States.[630] It has its own independent meaning in Community law and "must be interpreted in a manner which fully reflects the objective of that directive".[631]

---

[627] "Member States shall provide that personal data may be processed only if: (a) the data subject has unambiguously given his consent; or (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or (d) processing is necessary in order to protect the vital interests of the data subject; or (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1)", (compare Article 7 Directive 95/46, OJ 1995, L-281/31) and Article 5 Regulation 45/2001, OJ 2001, L-8/1: "Personal data may be processed only if: (a) processing is necessary for the performance of a task carried out in the public interest on the basis of the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or in the legitimate exercise of official authority vested in the Community institution or body or in a third party to whom the data are disclosed, or (b) processing is necessary for compliance with a legal obligation to which the controller is subject, or (c) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract, or (d) the data subject has unambiguously given his or her consent, or (e) processing is necessary in order to protect the vital interests of the data subject".

[628] Article 7 (a) (d) and (e) Directive 95/46, OJ 1995, L-281/31.

[629] Compare Sect. II 1 d aa (3) and *Valenzuela Contreras v. Spain*, Application no. 27671/95 judgment of 30 July 1998, para 57; *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006, para 95; *Huvig v. France*, Application no. 11105/84, judgment of 24 April 1990, para 34, and *Kruslin v. France*, Application no. 11801/85, judgment of 24 April 1990, para 35.

[630] Case C-524/06, *Heinz Huber v. Germany*, judgment of 16 December 2008, para 52.

[631] Case C-524/06, *Heinz Huber v. Germany*, judgment of 16 December 2008, para 52.

Mr. Huber, an Austrian national who resided in Germany, requested the deletion of personal data stored in the German Central Register of Foreign Nationals (Ausländerzentralregister, AZR). The AZR is a centralised register used for statistical purposes which contains personal data, similar to the VIS,[632] relating to foreign nationals who are resident in Germany on a basis which is not purely temporary.[633] Besides the statistical purposes, these data may additionally be used for security, police and judicial purposes.[634] Germany claimed therefore to use *Mr. Huber's* data "for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed" in accordance with Article 7 (e) of Directive 95/46.

Due to the restricted scope of Directive 95/46 mentioned above,[635] only data relating to the right of residence and to statistical purposes were subject to the Court of Justice proceedings.[636] The Court of Justice examined different questions relating to the existence and the use of the content of this database.[637] While the case additionally had a strong emphasis on the discriminatory function of the database,[638] with regard to the questions whether such treatment was compatible with the requirement of necessity under Article 7(e) of Directive 95/46, the Court of Justice concluded that:

> A system for processing personal data relating to Union citizens who are not nationals of the Member State concerned, [...] having as its object the provision of support to the

[632] Data stored in the AZR are: the name of the authority which provided the data, the reference number allocated by the Bundesamt; the grounds of registration; surname, surname at birth, given names, date and place of birth, sex and nationality; previous and other patronymics, marital status, particulars of identity documents, the last place of residence in the country of origin, and information supplied on a voluntary basis as to religion and the nationality of the spouse or partner; particulars of entries into and exits from the territory, residence status, decisions of the Federal Employment Agency relating to a work permit, refugee status granted by another state, date of death; decisions relating, inter alia, to any application for asylum, any previous application for a residence permit, and particulars of, inter alia, any expulsion proceedings, arrest warrants, suspected contraventions of the laws on drugs or immigration, and suspected participation in terrorist activities, or convictions in respect of such activities; and search warrants (Case C-524/06, *Heinz Huber v. Germany*, judgment of 16 December 2008, para 20).

[633] Case C-524/06, *Heinz Huber v. Germany*, judgment of 16 December 2008, para 19.

[634] Case C-524/06, *Heinz Huber v. Germany*, judgment of 16 December 2008, paras 19–29.

[635] Compare Sect. III 1 b.

[636] Case C-524/06, *Heinz Huber v. Germany*, judgment of 16 December 2008, para 45.

[637] The questions referred to whether: (1) the general processing of personal data of foreign citizens of the Union in a central register of foreign nationals is compatible with the prohibition of discrimination on grounds of nationality against citizens of the Union who exercise their right to move and reside freely within the territory of the Member States (Article 12(1) EC Treaty, in conjunction with Articles 17 EC and 18(1) EC Treaty)? (2) such processing is compatible with the prohibition of restrictions on the freedom of establishment of nationals of a Member State in the territory of another Member State (first paragraph of Article 43 EC Treaty)? (3) such treatment is compatible with the requirement of necessity under Article 7(e) of Directive 95/46?

[638] Gonzalez Fuster et al. (2010).

> national authorities responsible for the application of the law relating to the right of residence does not satisfy the requirement of necessity laid down by Article 7(e) of Directive 95/46 [...], interpreted in the light of the prohibition on any discrimination on grounds of nationality, unless:
> – it contains only the data which are necessary for the application by those authorities of that legislation, and
> – its centralised nature enables the legislation relating to the right of residence to be more effectively applied as regards Union citizens who are not nationals of that Member State.
>
> It is for the national court to ascertain whether those conditions are satisfied in the main proceedings. The storage and processing of personal data containing individualised personal information in a register such as the Central Register of Foreign Nationals for statistical purposes cannot, on any basis, be considered to be necessary within the meaning of Article 7(e) of Directive 95/46.[639]

It is Interesting to note, with regard to the processing of personal data for crime fighting purposes, that the Court of Justice emphasised the discriminatory effect of a database containing only data of non-German EU citizens whereas a similar register on German citizen was not in place. The Court of Justice followed the opinion of Advocate General *Poiares Maduro* who pointed out that "the existence of two separate data processing systems casts an unpleasant shadow over Union citizens, whom the German Government monitors much more strictly and systematically than German citizens".[640] The Court concluded that the fight against crime necessarily involves the prosecution of crimes and offences committed, irrespective of the nationality of their perpetrators, but, "it follows that as regards a Member State, the situation of its nationals cannot, as regards the objective of fighting crime, be different from that of Union citizens who are not nationals of that Member State and who are resident in its territory".[641] Therefore the difference in treatment between non-German EU citizens and German citizens which arises in consequence of systematic processing of personal data relating only to Union citizens, who are not nationals of the Member State concerned for the purposes of fighting crime, constituted a discrimination which is prohibited by Article 12 (1) EC Treaty (now Article 18 TFEU).[642]

Summarising, besides the pure data protection issue of Article 7 (e) Directive 95/46, the Court of Justice put emphasis on the important question of the discriminatory effect on a specific group of persons whose data are stored in a database used for crime fighting purposes.[643] The judgement additionally takes into account that the purpose of processing of the data is changing (data are originally collected for

[639] Case C-524/06, *Heinz Huber v. Germany*, judgment of 16 December 2008, para 82.

[640] Opinion of Advocate General Poiares Maduro, delivered on 3 April 2008 in case C-524/06, *Heinz Huber v. Germany*, judgment of 16 December 2008, para 15.

[641] Case C-524/06, *Heinz Huber v. Germany*, judgment of 16 December 2008, paras 78 and 79.

[642] Case C-524/06, *Heinz Huber v. Germany*, judgment of 16 December 2008, para 80.

[643] Compare also: Martin (2009), pp. 95–108.

statistical purposes and later used for other purposes) and warns against the suspicion which may arise out of the inclusion in this specific database.[644]

Against this background, it is worth noting that the FDPJ does not provide any specifications with regard to the lawfulness of the processing. This might be partly due to the fact that one of the most important requirements of lawfulness relates to the consent of the individual for the processing.[645] This criterion can reasonably only be used restrictively in a law enforcement context. Nonetheless, even in context of the FDPJ, lawfulness requires the respect of both, of basic principles such as the rule of law as well as of fundamental data protection principles subsequently specified in the FDPJ.

The criterion of a fair processing is only stipulated in Directive 94/45 and Regulation 45/2001.[646] It underlines the importance of the lawfulness of the processing. Even in absence of clear rules on data processing, the possibility to qualify data processing as illegal should not be excluded because of the applicability of unclear rules on the lawfulness.[647] Regrettably, this criterion is not mentioned in the FDPJ.

bb) Purpose Limitation

As already illustrated in the framework of the Council of Europe's instruments, purpose limitation is central to data protection law. It guarantees transparency and is therefore an important aim of Directive 95/46.[648] Data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes".[649] Regulation 45/2001 and the FDPJ include similar provisions.[650] The purpose must be clearly defined before the processing which should exclude, on the one hand, processing for unspecified and unknown purposes and, on the other hand, the possibility to subsequently change the original purpose.[651] This is, at the first glance, a quite restrictive provision which

[644] Compare Gonzalez Fuster et al. (2010).

[645] Article 7 (a) Directive 95/46, OJ 1995, L-281/31 and Article 5 (d) Regulation 45/2001, OJ 2001, L-8/1.

[646] Mentioned in Article 6 (1) (a) Directive 95/46, OJ 1995, L-281/31 and Article 4 (1) (a) Regulation 45/2001, OJ 2001, L-8/1.

[647] The reason for this criterion is that the use of secret devices, for instance telephone tapping, should be excluded, compare Dammann and Simitis (1997), Article 6, para 3.

[648] According to Article 6 (1) (b), data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards".

[649] Article 6 (1) (b) Directive 95/46, OJ 1995, L-281/31.

[650] Article 3 (1) FDPJ, OJ 2008, L-350/60 and Article 4 (1) (b) Regulation 45/2001, OJ 2001, L-8/1.

[651] Compare Ehmann and Helfrich (1999), Article 6, paras 6–15.

nevertheless allows for some derogation. Directive 95/46 for instance does not specify which purposes are incompatible with the original purpose and Regulation 45/2001 and the FDPJ allow for broad exceptions. Regulation 45/2001 allows changing the original purpose if "the change of purpose is expressly permitted by the internal rules of the Community institution or body".[652]

The most far reaching derogation from this principle is however contained in the FDPJ. Further processing for another purpose is permitted in so far as:

(a) It is not incompatible with the purposes for which the data were collected;
(b) The competent authorities are authorised to process such data for such other purpose in accordance with the applicable legal provisions; and
(c) Processing is necessary and proportionate to that other purpose.[653]

According to Article 11 FDPJ, when complying with the aforementioned principles, processing of data received or made available by another Member State may be additionally further processed for the following purposes:

(a) The prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties other than those for which they were transmitted or made available;
(b) Other judicial and administrative proceedings directly related to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties;
(c) The prevention of an immediate and serious threat to public security; or
(d) Any other purpose only with the prior consent of the transmitting Member State or with the consent of the data subject, given in accordance with national law.[654]

As follows from the reading of these exceptions, FDPJ allows for broad derogations from the purpose limitation principle. Solely the consent of the transmitting authority of the Member States is sufficient to fundamentally change the initial purpose of processing. The individual whose data are processed is completely left out of this decision. This shift towards the exclusive decision right of the authority processing the data with regard to the whereabouts and the subsequent use of the data clearly reverses the aim of the purpose limitation principle, which is also the protection of the individual against data processing for unspecified and unknown purposes.[655] To what extent this far reaching

[652] Article 6 (1) Regulation 45/2001, OJ 2001, L-8/1.

[653] Article 3 (2) FDPJ, OJ 2008, L-350/60; additionally, just as in Directive 95/46, data processing for historical, statistical or scientific purposes is allowed if the Member States provide for appropriate safeguards, such as making the data anonymous.

[654] Article 11 FDPJ, OJ 2008, L-350/60.

[655] For critical remarks on this provision, compare De Busser (2009), pp. 103–105, and third opinion of the EDPS on the proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, OJ 2007, C-139/1 (in the following: EDPS opinion on the FDPJ, OJ 2007, C-139/1), paras 20–25.

exemption is still in compliance with the foreseeability criterion developed by the ECtHR and its case law regarding the collection of data in security-related data processing[656] is very questionable.

cc) Adequate and Not Excessive in Relation to the Purposes for Which the Data Are Collected and/or Further Processed

Data processing for adequate and not excessive purposes in relation to the original purpose of collection is provided for in Article 6 (1) (c) Directive 95/46, in Article 4 (1) (c) Regulation 45/2001 and in Article 3 (1) FDPJ.[657] The provisions restrict the amount of processed data and subject the way of their processing to the purpose for which the data were collected.[658] As we have seen before, the requirement of purpose limitation is however largely derogated from in the FDPJ. Article 11 of the FDPJ, mentioned above, therefore contradicts the limitation of the purpose provided for in Article 3 (1) FDPJ when it allows for processing for "any other purpose". Although Article 3 (1) FDPJ represents a prerequisite for the application of Article 11 FDPJ,[659] the contradiction between these Articles is obvious.

dd) Data Must Be Accurate and Where Necessary, Kept up to Date

The accuracy of the data relates to the requirement that the data must represent correct and truthful facts.[660] Related to the accuracy are the completeness and the up to date nature of a set of data. Article 6 (1) (d) Directive 95/46 and Article 4 (1) (d) Regulation 45/2001 thus add that "every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or

[656] Compare *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006, para 116; *Rotaru v. Romania*, Application no. 28341/954, judgment of 4 May 2000, para 57; see also: *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, Application no. 62540/00, judgment of 28 June 2007.

[657] Article 6 (1) (c) Directive 95/46, OJ 1995, L-281/31; Article 4 (1) (c) Regulation 45/2001, OJ 2001, L-8/1 and Article 3 (1) FDPJ, OJ 2008, L-350/60.

[658] Dammann and Simitis (1997), Article 6, para 11.

[659] Article 11 provides that: "Personal data received from or made available by the competent authority of another Member State may, *in accordance with the requirements of Article 3(2)*, be further processed only for the following purposes other than those for which they were transmitted or made available [. . .]"(emphasis added).

[660] Dammann and Simitis (1997), Article 6, para 13.

rectified".[661] This second requirement symbolises both, first, incomplete data can lead to an inaccurate set of data and, second, when assessing the accuracy of processing, the purpose for which the data were collected must be taken into account.[662] While Directive 95/46 and Regulation 45/2001 explicitly refer to the accuracy and the up to date nature of data, the FDPJ only indirectly mentions these two obligations.

Article 4 (1) FDPJ provides that police and judicial "data shall be rectified if inaccurate and, where this is possible and necessary, completed or updated". As the wording of Article 4 (1) FDPJ already suggests, the enforcement of accuracy and completeness appears to be less restrictive than the formulations used in Directive 95/46 and Regulation 45/2001. The personal data shall not only be completed and updated when this is necessary, it must also be possible. The decision when it appears to be possible is left to the authority processing the data and therefore risks to be applied in a rather subjective way.

The provisions relating to the transmission to other Member States in the FDPJ are however slightly more restrictive. They do not include a subjective criterion and provide that "the competent authorities shall take all reasonable steps to provide that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available".[663] Although important in police work, the FDPJ unfortunately does not entail a provisions – similar to principle 3 Recommendation R (87) 15 – which refers to the accuracy of the data and distinguishes, on the one hand, between data collected for administrative purposes and data collected for police objectives and, on the other hand, between data based on facts and data based on opinions or personal assessments.[664] The EDPS in its opinion on the FDPJ rightly points to the risk that the difference between evidences, facts and opinions or assessments (soft intelligence) disappears when transferring such data to another authority.[665]

No distinction is further made between the different categories of data subjects such as criminals, suspects, victims or witnesses. When recalling the ECtHR's case law in *S. and Marper v. the United Kingdom* where the ECtHR clearly insists on a different treatment of data of convicted and not convicted persons,[666] the introduction of a provision taking such separation into consideration would have been advantageous in order to harmonise essential data protection rules in EU and ECHR law.

---

[661] Article 6 (1) (d) Directive 95/46, OJ 1995, L-281/31; Article 4 (1) (d) Regulation 45/2001, OJ 2001, L-8/1.

[662] Dammann and Simitis (1997), Article 6, para 15.

[663] Article 8 (1) FDPJ, OJ 2008, L-350/60.

[664] Compare above, Sect. II 4 a.

[665] EDPS opinion on the FDPJ, OJ 2007, C-139/1, para 32.

[666] *S.* and *Marper v. the United Kingdom*, Application nos. 30562/04 and 30566/04, judgment of 4 December 2008, para 122, to the stigmatisation of innocent individuals, see Gonzalez Fuster et al. (2010).

ee) Time Limit

According to Directive 95/46 and Regulation 45/2001, data "must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed".[667] The FDPJ provides that "personal data shall be erased or made anonymous when they are no longer required for the purposes for which they were lawfully collected or are lawfully further processed".[668] If at the time of expiry of the time limit the data are needed for "a current investigation, prosecution of criminal offences or the enforcement of criminal penalties", this obligation shall not apply.[669]

In both cases, the time limit is intrinsically linked to the purpose of collection or processing and therefore assures some degree of foreseeability for persons concerned, at least, as long as the purpose of processing remains unchanged. The main difference between both formulations however is the use of *shall* in the FDPJ instead of *must* in Directive 95/46 and Regulation 45/2001. The use of *shall* indicates a slightly mitigated obligation to erase data or to make them anonymous. Combined with the exhaustive possibilities to derogate from the purpose limitation principle, the time limit in the FDPJ still raises some questions. In case the purpose is changing during the processing, the time limit can easily be adapted to the new purpose. Theoretically, the time limit can be indefinitely extended. This possibility highlights the close relationship between the purpose and the duration of the storage and shows the practical effects which a derogation from the purpose limitation principle may have.

b) Special Categories of Data

The provisions prohibiting the processing of "sensitive or special categories of data" have the same anti-discriminatory function as the provision on sensitive data in Convention No. 108 and refer for that reason to almost the same categories.[670] Directive 95/46 and Regulation 45/2001 explicitly prohibit to process data revealing racial or ethnic origin, political opinions, religious or philosophical

[667] Article 6 (1) (e) Directive 95/46, OJ 1995, L-281/31; Article 4 (1) (e) Regulation 45/2001, OJ 2001, L-8/1.

[668] Article 4 (2) FDPJ, OJ 2008, L-350/60.

[669] Article 9 (1) FDPJ, OJ 2008, L-350/60.

[670] Directive 95/46 and Regulation 45/2001 additionally mention data on ethnic origin and trade union membership.

beliefs, trade-union membership or personal data concerning health or sex life.[671] Data processing relating to criminal offences, convictions or security measures "shall be carried out only under the control of official authority, or if suitable safeguards are provided under national law [...]"[672] or, in case of processing by the EU, "only if authorised by the Treaties establishing the European Communities or other legal instruments adopted on the basis thereof or, if necessary, by the European Data Protection Supervisor, subject to appropriate specific safeguards".[673] Although data themselves (as such) can not be sensitive, contextual criteria, which may make personal data sensitive data according to the context in which they are processed, such as economic, social or psychological circumstances of processing, are not included.[674]

Several exceptions nonetheless apply to this general prohibition. For instance, when the data subject has given its consent or the processing is necessary for a medical diagnosis, necessary for the purposes of complying with the specific rights and obligations of the controller in the field of employment law or the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.[675]

The latter exception was recently evaluated in a case before the General Court. In *Esch-Leonhardt and Others v. ECB,*[676] the General Court dismissed an application for annulment of a decision to include in the applicants' personnel files a letter concerning their use of the internal electronic mail system for transmitting union information. The background of the case is briefly summarised: the director of the human resources at the ECB prohibited the applicants, who were members of trade unions, to distribute trade union information to their colleagues by using the internal ECB e-mail system. The respective e-mail was thereupon added to the personal files of the applicants. Against this decision, the applicants enacted legal

[671] Article 8 (1) Directive 95/46, OJ 1995, L-281/31; Article 10 (1) Regulation 45/2001, OJ 2001, L-8/1.

[672] Article 8 (5) Directive 95/46, OJ 1995, L-281/31, data relating to administrative sanctions or judgments in civil cases *may be* also processed under the control of an official authority.

[673] Article 10 (5) Regulation 45/2001, OJ 2001, L-8/1.

[674] Compare for criticism on this provision, Dammann and Simitis (1997), Article 8, para 3 and for general criticism on the term "sensitive data", compare Simitis (1999).

[675] Further exceptions refer amongst others to the processing of data in the framework of organisations such as trade unions or non-profit-seeking organisations, or the processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his or her consent, or the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims, compare Article 8 (2) and (3) Directive 95/46, OJ 1995, L-281/31; Article 10 (2) and (3) Regulation 45/2001, OJ 2001, L-8/1.

[676] T-320/02, *Esch-Leonhardt and Others v. ECB*, judgment of 18 February 2004.

proceedings by basing themselves on Articles 2 (a), (b) and (c)[677] and Article 10 (1) of Regulation 45/2001.[678]

Due to the facts that, in both cases the applicants themselves declared in the respective e-mail to be members of the trade-union and that a shortened version, blacking out the trade union membership, of the respective e-mail would not have been sufficient to a proper management of the personal files, the General Court dismissed the application for annulment and concluded that the exception provided for in Article 10 (2) (b) Regulation 45/2001[679] is applicable.

In contrast to the detailed provisions of Directive 95/46 and Regulation 45/2001, the FDPJ does not stipulate a similar list including the exceptions. It simply reverses the general prohibition of the processing of sensitive data into the opposite. Article 6 FDPJ permits the processing of data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and personal data concerning health or sex life when the processing is "strictly necessary and when the national law provides adequate safeguards". Although the FDPJ is an instrument in police and judicial cooperation, it does not refer to data relating to criminal offences, convictions or security measures. Questions arising out of the fast changing technology in the framework of the processing of biometric data including DNA – subject of the ECtHR case *S. and Marper v. the United Kingdom*, discussed above – are not even mentioned.

c) Rights of the Individual

aa) Information, Notification and Transparency

One of the elements of a fair processing of data is the information provided to the data subject. Knowing that one's personal data are processed guarantees transparency

[677] Article 2 (a), (b), (c) of Regulation 45/2001 entails the definitions of the instrument (Article 2 (a) '*personal data*' shall mean any information relating to an identified or identifiable natural person hereinafter referred to as '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 or her physical, physiological, mental, economic, cultural or social identity; (b) '*processing of personal data*' hereinafter referred to as '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, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction; (c) '*personal data filing system*' hereinafter referred to as 'filing system' shall mean any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis (emphasis added)).

[678] Article 10 (1) Regulation 45/2001explicitly prohibits to process data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership or personal data concerning health or sex life.

[679] The processing relates to data which are manifestly made public by the data subject.

and enables the person concerned to assess its own position and to adapt its behaviour to a given situation.[680] Foreseeability and the control of the use of personal information play an essential role in data protection law. Moreover, as the ECtHR in *Weber and Saravia v. Germany* emphasised, the question of information of the individual concerned is directly linked to the effectiveness of remedies before the courts and for that reason to the existence of effective safeguards against the abuse of governmental monitoring powers.[681]

Directive 95/46 and Regulation 45/2001 distinguish two situations with regard to information rights: first, data which have been obtained from the data subject and second, data which have been obtained by other means.[682] In both cases, information has to be provided irrespective of whether the individual applies for access to the data.[683] The information includes (a) the identity of the controller and of his representative, (b) the purposes of the processing for which the data are intended and (c) any further information[684] in so far as such further information is necessary having regard to the specific circumstances in which the data are collected and to guarantee fair processing in respect of the data subject.[685] Information on the categories of data must be additionally provided in the case that the information is not obtained from the data subject.[686]

Regulation 45/2001 adds information on the legal basis of the processing operation for which the data are intended, the time-limits for storing the data and the right to have recourse at any time to the EDPS and the origin of the data, except where the controller cannot disclose this information for reasons of professional secrecy[687] in so far as such further information is necessary, having regard to the

[680] Dammann and Simitis (1997), Article 10, para 1; Ehmann and Helfrich (1999), Article 10, paras 25–28.

[681] *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006, para 135: "since there is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively".

[682] Articles 10 and 11 Directive 95/46, OJ 1995, L-281/31; Articles 11 and 12 Regulation 45/2001, OJ 2001, L-8/1.

[683] Articles 10 and 11 Directive 95/46, OJ 1995, L-281/31; Articles 11 and 12 Regulation 45/2001, OJ 2001, L-8/1.

[684] Such as the recipients or categories of recipients of the data, the existence of the right of access to and the right to rectify the data concerning the individual concerned.

[685] Articles 10 (1) and 11 (1) Directive 95/46, OJ 1995, L-281/31; Articles 11 (1) and 12 (1) Regulation 45/2001, OJ 2001, L-8/1; in the event that the information is obtained from the data subject, additional information on the fact whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply must be given.

[686] Article 11 (1) Directive 95/46, OJ 1995, L-281/31; Articles 12 (1) Regulation 45/2001, OJ 2001, L-8/1.

[687] Information on the origin of the data is only provided if the information is not obtained from the data subject.

specific circumstances in which the data are collected and to guarantee fair processing in respect of the data subject.[688]

Derogations exist in the event of processing for statistical purposes, historical or scientific research.[689] When the information is not obtained from the data subject, the information does not to be given, if the "provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law".[690] Although the provision on the disproportionate effort allows for a certain discretion,[691] Member States must nonetheless provide appropriate safeguards in these cases.

In contrast to Directive 95/46 and Regulation 45/2001, a clear obligation to provide the data subject with information on the processing does regrettably not exist in the FDPJ. The wording of the provision on the information of the data subject appears to be more a possibility rather than an obligation.[692] Recital (26) FDPJ mentions that "[. . .] it may be necessary to inform data subjects regarding the processing of their data [. . .]". Article 16 further details that "Member States shall ensure that the data subject is informed regarding the collection or processing of personal data by their competent authorities, in accordance with national law".[693] Member States may additionally ask another Member State not to inform the data subject about data transferred from this first Member State to the other.[694]

None of the FDPJ provisions stipulates a clear obligation to inform the person concerned about the processing.

bb) Access

The right to obtain access to personal data serves similar purposes as the right to be informed about the data processing. Control about the whereabouts of personal data plays a crucial role. Similar to the access right in Convention No. 108, Directive 95/46 and Regulation 45/2001 include different aspects of the access right. Individuals have the right to obtain information from the controller relating to the confirmation as to whether or not data related to him or her are being processed; information at least as to the *purposes* of the processing operation, the categories

[688] Article 12 (1) (f) Regulation 45/2001, OJ 2001, L-8/1.

[689] Articles 10 (2) and 11 (2) Directive 95/46, OJ 1995, L-281/31; Articles 11 (2) and 12 (2) Regulation 45/2001, OJ 2001, L-8/1.

[690] Article 11 (2) Directive 95/46, OJ 1995, L-281/31; Articles 12 (2) Regulation 45/2001, OJ 2001, L-8/1.

[691] Compare also Chap. B II 1 d cc.

[692] EDPS opinion on the FDPJ, OJ 2007, C-139/1, para 37.

[693] Article 16 (1) FDPJ, OJ 2008, L-350/60.

[694] Article 16 (2) FDPJ, OJ 2008, L-350/60.

of data concerned, the recipients[695] or categories of recipients to whom the data are disclosed, communication in an intelligible form of the data undergoing processing and of any available information as to the source of data and knowledge of the logic involved in any automated decision process concerning him or her.[696] Regulation 45/2001 additionally provides that the controller of the data has to provide the requested information within a 3 month period.[697] The detailed wording of the aforementioned provisions should assure that the Member States, when transposing the Directive into national law, respect the different aspects of the access right and do not chose a very broad access provision susceptible to different interpretations.[698]

Recent case-law on the right of access in the framework of Directive 95/46, such as *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer,*[699] confirms that Member States indeed enjoy a certain margin of discretion in implementing the access right of Directive 95/46, which is, however, limited by proportionality elements. In *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer* the Court made clear that the access rights of Directive 95/46 not only relates to the present but also to the past. In this case, *Mr. Rijkeboer* requested in 2005 the College to notify him of all instances in which data relating to him from the local authority personal records had, in the 2 years preceding the request, been disclosed to third parties.[700] The College complied with the request only partially by notifying *Mr. Rijkeboer* that only the data relating to a period of 1 year preceding his request could be released.[701] Data dating from more than 1 year prior to his request had been, according to Dutch law, erased automatically.[702]

The question referred to the Court was whether pursuant to the access right of Directive 95/46, an individual's right of access to information on the recipients or the content of the data communicated may be limited to a period of 1 year preceding his request for access.[703] The Court concluded that, "it is for Member States to fix a time-limit for storage of information and to provide for access to information

[695] It should be noted that the term "recipients" in the framework of Directive 95/46 and Regulation 45/2001 does not include "authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients" (Article 2 (g) of Directive 95/46, OJ 1995, L-281/31 and Regulation 45/2001, OJ 2001, L-8/1).

[696] Article 12 (a) Directive 95/46, OJ 1995, L-281/31; Article 13 (a) to (d) Regulation 45/2001, OJ 2001, L-8/1.

[697] Article 13 Regulation 45/2001, OJ 2001, L-8/1.

[698] Dammann and Simitis (1997), Article 12, para 3.

[699] Case C-553/07, *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer*, judgment of 7 May 2009.

[700] Ibid, para 23.

[701] Ibid, para 24.

[702] Ibid, para 25.

[703] Ibid, para 31.

which constitutes a fair balance between, on the one hand, the interest of the data subject in protecting his privacy, in particular by way of his rights to object and to bring legal proceedings and, on the other, the burden which the obligation to store that information represents for the controller".[704] Nonetheless, in the present case, the rules limiting the storage of information on the recipients and the content of the data related to a period of 1 year and correspondingly limited access to that information. Basic data however were stored for a much longer period, which did not constitute a fair balance, "unless it can be shown that longer storage of that information would constitute an excessive burden on the controller".[705]

Compared to the detailed provisions of Directive 95/46 and Regulation 45/2001, the right of access in the FDPJ is limited to information on the confirmation from the controller or from the national supervisory authority as to whether or not data relating to him have been transmitted or made available, information on the recipients or categories of recipients to whom the data have been disclosed and communication of the data undergoing processing or at least confirmation from the national supervisory authority that all necessary verifications have taken place.[706] Information relating to the purpose of processing, the source or the communication in an intelligible form are not provided.[707] In addition to the already limited information, various exceptions apply. Member States may restrict the access right (a) to avoid obstructing official or legal inquiries, investigations or procedures, (b) to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or for the execution of criminal penalties, (c) to protect public security, (d) to protect national security, (e) to protect the data subject or the rights and freedoms of others.[708] When restricting the access, the measure must be necessary and proportional and Member States must take the legitimate interests of the person concerned into account.[709] In all of these cases the person concerned "shall be advised that he may appeal to the competent national supervisory authority, a judicial authority or to a court".[710]

cc) Erasure, Blocking, Deletion and Notification to Third Parties

In addition to the right of access, Directive 95/46, Regulation 45/2001 and FDPJ contain the right to erasure, blocking and deletion of data whose processing do not comply with the provisions of the relevant instrument, in particular because of the

[704] Ibid, para 70.
[705] Idem.
[706] Article 17 (1) FDPJ, OJ 2008, L-350/60.
[707] For criticism, compare EDPS opinion on the FDPJ, OJ 2007, C-139/1, para 37.
[708] Article 17 (2) FDPJ, OJ 2008, L-350/60.
[709] Ibid.
[710] Ibid.

incomplete or inaccurate nature of the data.[711] Where Directive 95/46 gives Member States a wide discretion relating to the implementation of these rights and remains rather vague as regards the concrete content of such provisions, Regulation 45/2001 offers more detailed rules. The right to obtain the blocking of data should for instance apply where (a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy, including the completeness, of the data, (b) the controller no longer needs them for the accomplishment of its tasks but they have to be maintained for purposes of proof, or (c) the processing is unlawful and the data subject opposes their erasure and demands their blocking instead.[712] Nonetheless, also in the framework of Directive 95/46, certain criteria apply. The rectification is closely related to the accuracy of the data (Article 6 (1) (d) Directive 95/46) and refers to the truthfulness of the data, which, in turn, depends on the context in which the data are stored.[713]

The FDPJ includes similar provisions and specifies that Member States shall lay down whether the person concerned may request its rights directly at the controller or through the intermediary of the national DPA.[714] Unlike the foregoing rather limited provisions with regard to the protection of the individual, the FDPJ stipulates further guarantees in case the controller refuses rectification, erasure or blocking. Each "refusal must be communicated in writing to the data subject who must be informed of the possibilities provided for in national law for lodging a complaint or seeking judicial remedy".[715]

To complete the protection of the individual, Directive 95/46 and Regulation 45/2001 provide for a sort of "aftercare". The person concerned has the right to obtain from the controller the notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in line with the relevant instruments, unless this proves impossible or involves a disproportionate effort.[716] The FDPJ does not provide for an individual right of the person concerned to ask for the notification to third parties, but in case that incorrect data have been transmitted or data have been unlawfully transmitted, the recipient of the data "must be notified without delay".[717] The individual is however not notified.

---

[711] Article 12 (b) Directive 95/46, OJ 1995, L-281/31; Articles 14, 15 and 16 Regulation 45/2001, OJ 2001, L-8/1 and Articles 4 and 18 FDPJ, OJ 2008, L-350/60.

[712] Compare Article 15 (1) (a) to (c) Regulation 45/2001, OJ 2001, L-8/1.

[713] Dammann and Simitis (1997), Article 12, para 15.

[714] Articles 4 and 18 FDPJ, OJ 2008, L-350/60.

[715] Article 18 (1) FDPJ, OJ 2008, L-350/60, in addition "Upon examination of the complaint or judicial remedy, the data subject shall be informed whether the controller acted properly or not. Member States may also provide that the data subject shall be informed by the competent national supervisory authority that a review has taken place. If the accuracy of an item of personal data is contested by the data subject and its accuracy or inaccuracy cannot be ascertained, referencing of that item of data may take place", Article 18 (1) and (2) FDPJ, OJ 2008, L-350/60.

[716] Article 12 (c) Directive 95/46, OJ 1995, L-281/31; Article 17 Regulation 45/2001, OJ 2001, L-8/1; to criticism related to the term "disproportionate effort", compare Chap. B II 1 d cc.

[717] Article 8 (2) FDPJ, OJ 2008, L-350/60.

dd) The Right to Object

The right to object to the processing of personal data in Directive 95/46 and in Regulation 45/2001 is divided into two cases.

The first case concerns the possibility to object with regard to data processing on compelling grounds relating to the particular situation of the data subject "at least" in cases as described in Article 7 (e) and (f) of Directive 95/46. These provisions refer to data processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed or to the processing necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed.[718] In relation to Regulation 45/2001 the right to object is formulated in a broader way involving in general the objection to data processing on compelling grounds relating to the particular situation of the data subject.[719] Excepted cases are situations in which the processing is necessary for compliance with a legal obligation to which the controller is subject, or necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract or the data subject has unambiguously given his or her consent.[720] The second case in which objection is possible concerns the right to oppose data processing for the purposes of direct marketing.[721] Directive 95/46 and Regulation 45/2001 include similar provisions.

Taking the relatively secret nature of police and judicial data processing into account, it is not particular astonishing that the FDPJ does not involve a right to object. However, in this context, it is important to highlight that security related data processing does not only involve data on criminals. Data of possible suspects, victims and witnesses are equally processed. With regard to the protection of this particular sensitive group of persons, the complete exclusion of the right to object the data processing in certain situation for data processed in the framework of police and judicial data processing seems less obvious.[722] It is likely that there are situations where a victim or witness might oppose (on compelling grounds relating to his particular situation the processing) of his personal data, for instance rape victims. Situations in which a victim or witness may have legitimate grounds to object should therefore also be considered in a police and judicial context.

[718] Article 7 (e) and (f) Directive 95/46, OJ 1995, L-281/31.

[719] Article 18 (a) Regulation 45/2001, OJ 2001, L-8/1.

[720] Ibid.

[721] Article 14 (b) Directive 95/46, OJ 1995, L-281/31; Article 18 (b) Regulation 45/2001, OJ 2001, L-8/1.

[722] Against the right to object in security related data processing, see Alonso Blas (2010), Issue 11, No. 2, pp. 233–250.

ee) Legal Prohibition on Automated Decision Making

The danger of a misuse of automatic means when making a decision, including the assessment of the personality of a person, should be encountered by a more or less strict ban on automated individual decisions. The risk of automatic decisions relates to the fact that their result might seem objective at the first glance (because no subjective impressions are considered) and therefore decision makers may tend to trust the alleged objective result more than another result which might base on subjective criteria. Therefore, Directive 95/46, Regulation 45/2001 and FDPJ protect individuals against decisions which base solely on automatic processing of data.[723] Individuals equipped with personal responsibility and not computers should be accountable for the (possibly detrimental) decision on other persons.[724]

Considerable exceptions however exist. Directive 95/46 and Regulation 45/2001 prohibit automated decision making. An exception applies if the decision is authorised by law.[725] FDPJ generally permits automated decisions if they are authorised by law.[726] In all cases the law must lay down "measures to safeguard the legitimate interests of the data subject",[727] but further guarantees in order to ensure the quality of the protective measures are not necessary. Compared to the provisions in Directive 95/46 and Regulation 45/2001, the wording of Article 7 FDPJ, which regulates automated decision making, raises concern. Instead of the general approach chosen by Directive 95/46 and Regulation 45/2001 to prohibit automated decisions, the FDPJ generally permits them.[728] This wording does not put real obstacles for Member States to enact legislation permitting automated decision making.

[723] Article 15 Directive 95/46, OJ 1995, L-281/31; Article 19 Regulation 45/2001, OJ 2001, L-8/1 and Article 7 FDPJ, OJ 2008, L-350/60.

[724] Dammann and Simitis (1997), Article 15, para 2.

[725] Article 15 (2) (b) Directive 95/46, OJ 1995, L-281/31; Article 19 Regulation 45/2001, OJ 2001, L-8/1; Directive 95/46 additionally allows for automatic decision making when entering into or fulfilling a contract, compare Article 15 (2) (a) Directive 95/46; in case of Regulation 45/2001 automatic decisions are permitted if authorised by national or Community legislation.

[726] Article 7 FDPJ, OJ 2008, L-350/60.

[727] Article 15 (2) (b) Directive 95/46, OJ 1995, L-281/31; Article 19 Regulation 45/2001, OJ 2001, L-8/1 and Article 7 FDPJ, OJ 2008, L-350/60.

[728] Article 7 FDPJ, OJ 2008, L-350/60 stipulates: "A decision which produces an adverse legal effect for the data subject or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to the data subject shall be permitted only if authorised by a law which also lays down measures to safeguard the data subject's legitimate interests".

ff) Independent Supervision and Article 29 Data Protection Working Party

Supervision is an essential requirement to guarantee the effective enforcement of data protection requirements.[729] Independence of this supervision is therefore acore element contributing to this aim. Directive 95/46 and the FDPJ include further specifications with regard to the powers with which the supervisory authorities should be equipped. In addition to consultation duties[730] foreseen in Directive 95/46, investigative powers,[731] effective powers of intervention[732] and powers to engage in legal proceedings or to bring infringements to the attention of the judicial authorities where the national provisions adopted pursuant to the Directive 95/46 or the FDPJ have been violated are included in both instruments (Directive 95/46 and FDPJ). The supervisory bodies shall hear claims lodged by persons and shall inform the person concerned about the outcome of the claim.[733] Decisions taken by the supervisory authorities may be appealed against through the courts.[734] Directive 95/46 additionally provides for the drawing up and the publishing of an activity report.[735]

Regulation 45/2001 establishes the EDPS as the independent supervisory authority responsible for monitoring the data processing carried out by the Community institutions and bodies. Detailed provisions lay down the legal framework of the EDPS. Its appointment, its powers and duties, conditions for the performance of its duties, staff and financial resources and guarantees relating to its independence are subject to Articles 41–48 of Regulation 45/2001. According to Article 46 of Regulation 45/2001 the duties of the EDPS involve, amongst others, the investigation of complaints, the conduction of inquiries, the prior checking of processing notified to the EDPS, the monitoring of the application of the provisions of Regulation 45/2001 and of relevant developments and the cooperation with national DPAs.[736]

In addition, the EDPS disposes of important powers stipulated in Article 47 of Regulation 45/2001. It may, inter alia, order the rectification, blocking, erasure or

[729] Article 28 Directive 95/46, OJ 1995, L-281/31; Articles 41–48 Regulation 45/2001, OJ 2001, L-8/1 and Article 25 FDPJ, OJ 2008, L-350/60.

[730] Article 28 (2) Directive 95/46, OJ 1995, L-281/31.

[731] Investigative powers are powers such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties (Article 28 (3) Directive 95/46 and Article 25 (2) (a) FDPJ).

[732] Intervention powers are powers such as, for example, that of delivering opinions before processing operations 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, or that of referring the matter to national parliaments or other political institutions (Article 28 (3) Directive 95/46 and Article 25 (2) (b) FDPJ).

[733] Article 28 (4) Directive 95/46, OJ 1995, L-281/31 and Article 25 (3) FDPJ, OJ 2008, L-350/60.

[734] Article 28 (3) Directive 95/46, OJ 1995, L-281/31 and Article 25 (2) (c) FDPJ, OJ 2008, L-350/60.

[735] Article 28 (4) Directive 95/46, OJ 1995, L-281/31.

[736] Compare Article 46 Regulation 45/2001, OJ 2001, L-8/1 and Hijmans (2006).

destruction of the data processed in breach with Regulation 45/2001, impose a ban on the processing, intervene in actions before the Court of Justice or refer the matter to the institution or body concerned, and if necessary to the Parliament, the Council and the Commission.[737] The EDPS additionally advises on policy affecting data protection matters and cooperates with national DPAs to guarantee consistent protection of personal data interests. Over the years, the EDPS has become an important actor in the field of European data protection law.[738] In the AFSJ, former first pillar databases, such as Eurodac and the VIS are monitored by the authority. Supervision of the SIS II is intended in future.[739]

The criterion of independence was recently subject to an infringement action against Germany which transposed Article 28 (1) of Directive 95/46 (which stipulates that the national DPAs shall act with complete independence in exercising their functions) by subjecting the national DPAs at federal level, responsible for supervising the processing of data outside the public sector, to state scrutiny.[740] Supported by the EDPS, the Commission considered this supervisory model as an infringement of the independence requirement of Directive 95/46 and decided to bring the action before the Court of Justice. Germany argued that the DPAs are not exposed to external influences, but rather to an "administration's internal monitoring mechanism, implemented by the authorities attached to the same administrative machinery".[741]

Against these relatively vague arguments, the Court came to a clear statement and interpreted the terms "with complete independence" in a broad way. It pointed out that "the mere risk that the scrutinising authorities could exercise a political influence over the decisions of the supervisory authorities is enough to hinder the latter authorities' independent performance of their tasks. First, as was stated by the Commission, there could be 'prior compliance' on the part of those authorities in the light of the scrutinising authority's decision-making practice. Secondly, for the purposes of the role adopted by those authorities as guardians of the right to private life, it is necessary that their decisions, and therefore the authorities themselves, remain above any suspicion of partiality".[742]

Due to this interpretation, the Court of Justice held that the German legal framework to regulate data processing oversight outside the public sector was not consistent with the independence requirement of Article 28 (1) of Directive 94/46. The unambiguous statement in favour of an undoubtful interpretation of the term "complete independence" requires the Member States to establish a legal

[737] Compare the powers listed in Article 47 Regulation 45/2001, OJ 2001, L-8/1.

[738] An excellent overview of the functions of the EDPS gives Hijmans (2006).

[739] Compare Chap. B III 1 e bb.

[740] Case C-518/07, *Commission v. Germany*, judgment of 9 March 2010, para 10; annotations with regard to this case are made by Schild (2010); Bull (2010); Roßnagel, (2010); Petri and Tinnefeld (2010).

[741] Case C-518/07, *Commission v. Germany*, judgment of 9 March 2010, para 16.

[742] Case C-518/07, *Commission v. Germany*, judgment of 9 March 2010, para 36.

framework for national DPAs which remains entirely free from any external influence, including indirect influence. Any other interpretation would have left room for discretion of the Member States and would have permitted other Member States to equally subject their DPAs to whatsoever form of supervision.

In addition to independent supervision, Directive 95/46 established the Article 29 Data Protection Working Party which coordinates the cooperation of the national DPAs at EU level.[743] The Working Party is composed of a representative of the national DPA and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission.[744] The group acts independently and has advisory status. Over the years, it offered valuable support in interpreting the application of Directive 95/46.[745] The tasks of the Article 29 Data Protection Working Party are stipulated in Article 30 Directive 95/46. They relate to the promotion of a uniform application of the general principles of Directive 95/46 through the cooperation between national DPAs. In addition, the group advises the Commission on questions of data protection and on the level of protection in the EU and in third states, makes recommendations to the EU institutions and the public on data protection matters and gives opinions on codes of conducts drawn up at Community level.[746]

gg) Security

Security requirements should protect the personal data against destruction, loss, alteration or unauthorised access or disclosure. Article 17 Directive 95/46 requires to establish "appropriate technical measures" to protect personal data against all unlawful forms of processing.[747] The level of security must be appropriate to the risks represented by the processing and the nature of the data to be protected.[748] Further details of the kind of measures which should be taken are stipulated in Regulation 45/2001 and FDPJ. Article 22 Regulation 45/2001 and Article 22 FDPJ stipulate 11 measures which shall be implemented to protect personal data in automated data processing systems: Equipment access control[749] and control of

[743] Article 29 Directive 95/46, OJ 1995, L-281/31.

[744] Article 29 (2) Directive 95/46, OJ 1995, L-281/31.

[745] The opinions and document of the Article 29 Data Protection Working Party can be found on the webpage: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm (accessed February 2011).

[746] Compare Article 30 (1) (a)–(d) of Directive 95/46, OJ 1995, L-281/31 and http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm (accessed February 2011).

[747] Article 17 (1) Directive 95/46, OJ 1995, L-281/31.

[748] Article 17 (2) Directive 95/46, OJ 1995, L-281/31.

[749] Which means to deny unauthorised persons access to data-processing equipment used for processing personal data.

data media,[750] storage,[751] users,[752] data access,[753] communication,[754] input,[755] and transport[756] should improve security. Recovery,[757] reliability[758] and integrity[759] of the data processing add additional protection.[760]

hh) Accountability

Remedies, liability and sanctions play an important role for the effective enforcement of data protection rights. In case that a person has suffered damage as a result of an unlawful processing operation or of any act incompatible with the instruments in force, he must be entitled to receive compensation from the controller or another authority.[761] The person concerned must dispose of a right to a judicial remedy for the breach of the right guaranteed to him.[762] Directive 95/46, Regulation 45/2001 and FDPJ indiscriminately grant these rights to "any person", irrespectively of the categories of persons concerned.[763] Any natural person or individual consequently may invoke these rights in front of national or European Courts. At European level, at least in the framework of Regulation 45/2001, an individual may lodge a

[750] Includes the prevention of unauthorised reading, copying, modification or removal of data media.

[751] Member States should prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data.

[752] Which means to prevent the use of automated data-processing systems by unauthorised persons using data communication equipment.

[753] Member States must ensure that persons authorised to use an automated data-processing system only have access to the data covered by their access authorisation.

[754] Member States must guarantee that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data communication equipment.

[755] Control of the input means to ensure that it is subsequently possible to verify and establish which personal data have been input into automated data-processing systems and when and by whom the data were input.

[756] Transport control means to prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media.

[757] Recovery should ensure that installed systems may, in case of interruption, be restored.

[758] Reliability ensures that the functions of the system perform, that the appearance of faults in the functions is reported.

[759] Integrity means that stored data cannot be corrupted by means of a malfunctioning of the system.

[760] Compare Articles 22 (2) (a)–(j) of Regulation 45/2001, OJ 2001, L-8/1 and FDPJ, OJ 2008, L-350/60.

[761] Article 23 (1) Directive 95/46, OJ 1995, L-281/31, Article 32 (4) Regulation 45/2001, OJ 2001, L-8/1 and Article 19 (1) FDPJ, OJ 2008, L-350/60.

[762] Article 22 Directive 95/46, OJ 1995, L-281/31, Articles 22 (1) and (2) Regulation 45/2001, OJ 2001, L-8/1 and Article 20 FDPJ, OJ 2008, L-350/60.

[763] Dammann and Simitis (1997), Article 22, para 2; Brouwer (2008), p. 221.

complaint with the EDPS.[764] Actions against decisions of the EDPS may be brought before the Court of Justice.[765] Sanctions to be imposed in case of infringement of the data protection provisions of Directive 95/46, Regulation 45/2001 and FDPJ should additionally ensure the full and effective implementation of these instruments.[766]

d) Exceptions

Despite the relatively comprehensive protection described above, Directive 95/45 and Regulation 45/2001 include various restrictions to the rights included in both instruments[767]: (a) the prevention, investigation, detection and prosecution of criminal offences, (b) an important economic or financial interest of a Member State or of the European Communities, including monetary, budgetary and taxation matters, (c) the protection of the data subject or of the rights and freedoms of others, (d) the national security, public security or defence of the Member States and (e) the monitoring, inspection or regulatory task connected, even occasionally, with the exercise of official authority in the cases referred to in (a) and (b).[768] Article 13 (2) Directive 95/46 further restricts the right to access, rectification, erasure and blocking "where there is clearly no risk of breaching the privacy of the data subject" when data are processed solely for purposes of scientific research or are kept in personal form for a period which does not exceed the period necessary for the sole purpose of creating statistics.[769] Regulation 45/2001 however insist on the requirement of informing the data subject of the principal reason on which the application of the restriction is based and of his right to have recourse to the EDPS.[770]

When invoking such restrictions, Member States, Community institutions and bodies must however establish that the measures are necessary.[771] A general

[764] Article 32 (2) Regulation 45/2001, OJ 2001, L-8/1.

[765] Ibid.

[766] Article 24 Directive 95/46, OJ 1995, L-281/31, Article 49 Regulation 45/2001, OJ 2001, L-8/1 and Article 24 FDPJ, OJ 2008, L-350/60.

[767] Concerned are the rights relating to the quality of the data, the information rights, access, rectification, erasure and blocking as well as the publicizing of processing operations and the erasure of traffic and billing data (Articles 6 (1), 10, 11 (1), 12 and 21 of Directive 95/46, OJ 1995, L-281/31 and Articles 4 (1), 11, 12 (1), 13 to 17 and 37 (1) of Regulation 45/2001, OJ 2001, L-8/1).

[768] Article 13 (1) Directive 95/46, OJ 1995, L-281/31 and Article 20 (1) Regulation 45/2001, OJ 2001, L-8/1; Article 13 (1) Directive 95/46 adds the monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in case of public security.

[769] Article 13 (2) Directive 95/46, OJ 1995, L-281/31.

[770] Article 20 (4) Regulation 45/2001, OJ 2001, L-8/1.

[771] Article 13 (1) Directive 95/46, OJ 1995, L-281/31 and Article 20 (1) Regulation 45/2001, OJ 2001, L-8/1.

exemption for specific authorities or bodies would therefore neither be in accordance with Directive 95/46,[772] nor with Regulation 45/2001.

Exceptions for the processing of personal data solely for journalistic purposes or the purpose of artistic or literary expression "if they are necessary to reconcile the right to privacy with the rules governing freedom of expression" may additionally be provided.[773] Activities may be classified as "journalistic" if their sole objective is the disclosure to the public domain of information, opinions or ideas, irrespective of the medium used to distribute them.[774]

Exceptions in the framework of the FDPJ are not specified in one general provision as in Directive 95/46 or Regulation 45/2001. They are regulated in the relevant Articles which grant rights to individuals and which were already discussed above.

e) Transfer of Personal Data

Provisions on the transfer of personal data can be found in all three instruments. Depending on the scope of the instruments,[775] different rules on the transfer of personal data apply. Directive 95/46 exclusively refers to the protection of data in the framework of the transfer from Member States to third parties in an economic context, Regulation 45/2001 involves the transmission between Community institutions, bodies and/or other recipients outside the Community order and FDPJ includes rules on the transfer of data to authorities of third states, international

[772] Dammann and Simitis (1997), Article 13, para 4.

[773] Article 9 Directive 95/46, OJ 1995, L-281/31.

[774] For the exception as regards the processing for journalistic purposes, compare case C-73/07, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy*, judgment of 16 December 2008, in which the Court of Justice interpreted the exception as regards the processing for journalistic purposes according to Article 9 of Directive 95/46, which governs the relationship between the protection of such data and freedom of expression, as follows: Article 9 Directive 95/46 is to be interpreted "as meaning that an activity in which data on the earned and unearned income and the assets of natural persons are: (1) collected from documents in the public domain held by the tax authorities and processed for publication, (2) published alphabetically in printed form by income bracket and municipality in the form of comprehensive lists, (3) transferred onward on CD-ROM to be used for commercial purposes, and, (4) processed for the purposes of a text-messaging service whereby mobile telephone users can, by sending a text message containing details of an individual's name and municipality of residence to a given number, receive in reply information concerning the earned and unearned income and assets of that person, must be considered as activities involving the processing of personal data carried out 'solely for journalistic purposes', within the meaning of that provision, if the sole object of those activities is the disclosure to the public, irrespective of the medium which is used to transmit them, of information, opinions or ideas. Whether that is the case is a matter for the national court to determine. In any event, those activities are not limited to media undertakings and may be undertaken for profit-making purposes" (para 65 of the judgment).

[775] Compare above Sect. III 1.

bodies or the transfer to private parties in Member States.[776] The following analysis will show that while the transfer of personal data in the context of Directive 95/46 and Regulation 45/2001 is regulated in an exhaustive manner, the rules of the FDPJ fall considerably behind as regards the protection of individual rights in the context of third state data transfer. Having in mind that in the AFSJ as well as in the former first pillar increasingly more data are transferred to third states, the provisions regulating third state data transfer are demonstrated slightly more detailed than the aforementioned rules.

aa) Transfer to Recipients Governed by Directive 95/46 and Regulation 45/2001

Until the entry into force of the Amsterdam Treaty in 1997, which added Article 286 EC Treaty (Article 16 TFEU) to the Community order, the data processing of the institutions and bodies of the Community was not subject to official regulation. First Regulation 45/2001 stipulated rules on the data processing of the Community institutions and bodies. As already seen above, its rules mirror the rules of Directive 95/46 and are equally limited to former first pillar institutions and bodies. It is worth remembering, that, even after the adoption of the Lisbon Treaty, the rules of Regulation 45/2001 are not applicable to the data processing of former third pillar actors or databases, such as Europol, Eurojust or the CIS.[777]

Regulation 45/2001 distinguishes between transmission of data by the Community institutions or bodies and other recipients.

In the first case, personal data processing of the recipient is entirely covered by the rules of Regulation 45/2001 (for instance data processing at OLAF) and data shall only be transferred "if the data are necessary for the legitimate performance of tasks covered by the competence of the recipient".[778] Consequently, the sending party must ensure (1) that the recipient has the appropriate competence and (2) that the transfer is necessary. This assessment should be made on a case-by-case basis.[779] The recipient is bound by the purpose of the transfer when processing the data.[780] When data are transferred following a request from the recipient, both, the recipient and the controller are responsible for the legitimacy of the transfer.[781] Additional safeguards relating to the lawfulness of the transfer include the requirement that the controller should verify the competence of the recipient and make

[776] Articles 25 and 26 Directive 95/46, OJ 1995, L-281/31, Articles 7–9 Regulation 45/2001, OJ 2001, L-8/1 and Articles 13 and 14 FDPJ, OJ 2008, L-350/60.

[777] Compare above Chap. B III 1.

[778] Article 7 (1) Regulation 45/2001, OJ 2001, L-8/1.

[779] EDPS, opinion on a notification for prior checking received from the data protection officer at the European Anti-Fraud Office on Criminal assistance cases, Brussels, 12 October 2007 (Case 2007–203), p. 8.

[780] Article 7 (3) Regulation 45/2001, OJ 2001, L-8/1.

[781] Ibid.

a provisional evaluation of the necessity of the transfer of the data.[782] The recipient must ensure that the necessity of the transfer of the data can be subsequently verified.[783]

In the second case (other recipients), data are either transferred to other recipients subject to Directive 95/46 or to other recipients not subject to Directive 95/46. If Directive 95/46 is applicable to the data processing of the recipient, the latter must establish that the data are necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority, or the recipient establishes the necessity of the transfer and there is no reason to assume that the data subject's legitimate interests might be prejudiced.[784]

Transfer of personal data to recipients who are not governed by the regime of Directive 95/46 necessarily requires more protection. It is analysed in the next section.

bb) Third State Transfer in the Framework of Directive 95/45 and Regulation 45/2001

In contrast to the transfer to recipients governed by Directive 95/46 and Regulation 45/2001, transfer to third states is however regulated in much more detail. Chapter IV of Directive 95/46 and Article 9 of Regulation 45/2001 govern the conditions of the transmission of data to a third state in an economic context.[785] Third state data transfer occupies an increasingly important place in EU data sharing. To avoid that the protection guaranteed in the EU is not considerably weekend when transferring the data to third states and to avoid the by-passing of EU data protection rules by establishing data processing servers in countries applying a low level of data protection, both instruments provide for the so called "adequacy mechanism".

(1) Adequate Level of Protection

In general, according to Articles 25 (1) and (2) of Directive 95/46 and Article 9 of Regulation 45/2001, the transfers to a third state of personal data may take place only if the third state in question ensures an adequate level of protection. To assess the adequacy, the following procedure takes place:

First, the national DPA of the country which intends to transfer the data considers if the third country ensures – or does not ensure – an adequate level of

[782] Article 7 (2) Regulation 45/2001, OJ 2001, L-8/1, if doubts arise as to this necessity, the controller shall seek further information from the recipient.

[783] Article 7 (2) Regulation 45/2001, OJ 2001, L-8/1.

[784] Ibid.

[785] Third States are states that are neither Member States of the EU nor members of the European Economic Area (EEA); besides of the Member States of the EU, Iceland, Liechtenstein and Norway are members of the EEA.

protection.[786] If the national DPA considers that the third country does not ensure an adequate level of protection, according to Article 25 (3) Directive 95/46 the Member State is obliged to inform the European Commission or the EDPS (the latter only in case of Regulation 45/2001).[787] Second, when the Commission agrees that the third country does not ensure an adequate level of protection, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.[788]

In general, Article 25 (2) of Directive 95/46 and Article 9 (2) of Regulation 45/2001 establish the criteria to be applied when evaluating the level of protection provided by a third state. The adequacy of the level shall be assessed in the light of *all* the circumstances surrounding a data transfer operation. Particular consideration shall be given to the nature of the data,[789] the purpose and duration of the proposed processing operation,[790] the country of origin and country of final destination,[791] the rules of law, both general and sectoral, in force in the third country in question and the rules and security measures which are complied with in that country.[792] The indication of "the rules and security measures which are complied with in that country" refers to economic self-regulation measures outside of the legal order that nevertheless have a binding force for the members of the organisation concerned.[793] Therefore, legal commentators postulate that Directive 95/46 follows a practice-oriented and functional approach.[794]

---

[786] The control could also be ensured by the processor itself (e.g. in Germany, § 4 b II, V BDSG).

[787] Article 9 (3) of Regulation 45/2001, OJ 2001, L-8/1.

[788] Article 25 (4) of Directive 95/46, OJ 1995, L-281/31.

[789] Especially the content of the data [e.g. sensitive data, and the possibility of the identification of the person concerned; compare Dammann and Simitis (1997), Article 25, para 10, and Engel (2003), accessible at Dissertationen of the Freie Universität Berlin online: http://www.diss.fu-berlin.de/diss/receive/FUDISS_thesis_000000001587 (accessed February 2011), pp. 110–111 (referred to as Engel (2003)].

[790] The long duration of the data demands a more intensive protection of data subjects as a short processing time, compare Engel (2003) p. 112.

[791] The indication of the country of origin is very important in the context of the import of data from a non-European country into the EU. The indication shall prevent that the data protection authorities do not make high demands to the level of protection in case of the re-import of the data into the third country. The indication of the country of final destination shall ensure that data protection authorities do not makehigh demands to the level of protection to a transit country, compare Engel (2003), pp. 112–113; *Dammann*/*Simitis* assume that transit countries, as well as the country of final destination, which could be different from the direct receiving country should be also considered, compare Dammann and Simitis (1997), Article 25, para 10.

[792] Article 25 (2) of Directive 95/46, OJ 1995, L-281/31; Article 9 (2) of Regulation 45/2001, OJ 2001, L-8/1.

[793] Document adopted by the Article 29 Working Party, WP 12 of 24 July 1998 on the transfers of personal data to third countries: applying Articles 25 and 26 of the EU data protection directive, pp. 11 et seq.

[794] Siemen (2006), p. 299; Brühann (2007), Article 25, para 15; Engel (2003), pp. 115 et seq.

The wording "in the light of all the circumstances surrounding a data transfer operation" suggests that the third country is not obliged to guarantee an adequate level of protection in general, but adequate guarantees must be given in the specific case of the transfer.[795] Nevertheless the Commission can adopt a decision whereupon the entire country guarantees an adequate protection of personal data.[796] Moreover, it shall be given "particular" consideration to certain circumstances, i.e. that other criteria apart from the mentioned ones could also influence the adequacy decision. Further criteria to assess the level of adequacy are not contained in Directive 95/46 or Regulation 45/2001. Such criteria are however of utmost importance considering the far reaching consequence of an adequacy decision of the Commission. A country providing an adequate level of protection profits from economic and convenient advantages when it comes to data transfer. Personal data of EU citizens may then be easily transmitted to the respective country. With regard to these advantages and the implications on the rights of individuals, it seems to be crucial to interpret in detail the meaning of the notion "adequate". When taking into account that, pursuant to its recital 11, Directive 95/46 shall give substance to and amplify the provisions contained in the Convention No. 108, it seems to be reasonable to draw a comparison between the wording used in Convention No. 108 and the wording of Directive 95/46.[797]

(2) Recourse to Convention No. 108

Pursuant to Article 12 (3) (a) of Convention No. 108, referring to the transfer of data across the borders of the member states of the Convention, the transfer of data across national borders is permitted if the receiving party provides an equivalent protection. The abovementioned additional protocol of May 2001[798] governs the transfer of data to third states. Its Article 2 (1) stipulates: "Each Party shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention only if that State or organisation ensures an adequate level of protection for the intended data

[795] Dammann and Simitis (1997), Article 25, para 9; Engel (2003), p. 89–90.

[796] View Commission decision with regard to: Switzerland, Hungary, Canada, Argentina, Guernsey and the Isle of Man, http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm (accessed February 2011).

[797] Recital 11 of the Directive 95/46: "Whereas the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data".

[798] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and Transborder Data Flows, 8 November 2001, entered into force the 1st of July 2004.

transfer".[799] When comparing the two formulations, the different wording is remarkable. The clear distinction between the words adequate and equivalent indicates that there must be a different standard regarding on the one hand the transfer of data to member states of the Convention No. 108 and on the other hand as regards the transfer to third states. It follows that a full equivalence of the level of protection between the EU and third states is not required to transfer data to another country. Instead, a lower level of protection – compared to the level of protection of the member states of the Convention – could be sufficient to guarantee an adequate level of protection in terms of the Convention No. 108 and its additional protocol.[800] Due to the close relationship between Directive 95/46 and Convention No. 108 mentioned above,[801] both adequacy criteria could be interpreted congruently. Consequently, according to this comparison, adequate does mean that the level of protection must be necessarily equivalent.

Siemen explains this conclusion also by the fact that the Explanatory Report of the Additional Protocol of 23 May 2003 interprets the adequacy of the level of protection in "the light of all the circumstances surrounding a data transfer".[802] The same wording is used in Article 25 (2) of Directive 95/46. Therefore the identical wording of the Directive 95/46 and the Explanatory Report of the Additional Protocol additionally indicates an identical understanding of both instruments.[803] *Dammann/Simitis* assume that the wording "adequate" has been chosen for flexibility reasons. With regard to potential negotiations with a third country about the guaranteed level of protection, the wording leaves a wide margin.[804] *Engels* argues in the same way and pleads for an interpretation of the wording adequacy in the sense of "functionally adequate".[805] She proposes that the protection of the personal right of the person concerned should correspond to the circumstances of the transfer.

In conclusion, it can be assumed that the wording adequate level of protection shall be interpreted in the light of the surroundings of the transfer, i.e., that in

[799] Article 2 (1) of the additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and Transborder Data Flows, 8 November 2001, entered into force the 1st of July 2004 (emphasis added).

[800] Dammann and Simitis (1997), Article 25, para 8; Siemen (2006), p. 299.

[801] See Sect. III 1 a.

[802] Explanatory report to the additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and Transborder Data Flows, 8 November 2001, entered into force the 1st of July 2004, ETS No. 181, para 26.

[803] Dammann and Simitis (1997), Article 25, para 8; Siemen (2006), pp. 300–301.

[804] Dammann and Simitis (1997), Article 25, para 8.

[805] Engel (2003), p. 91.

general Directive 95/46 accepts a lower level of protection in the third country compared to the level in the EU.[806] However, when balancing the different interests at stake the "core principles" of Directive 95/46 and Regulation 45/2001 relating to the quality standards and the individual rights must be preserved.[807]

(3) Basic Principles of the Article 29 Data Protection Working Party Regarding the Data Transfer to Third States

Due to its advisory function towards the European Commission, the Article 29 Data Protection Working Party developed guidelines to improve the coherent application of the provisions regulating the transfer of data to third states.[808] In the meantime, various documents of the Article 29 Data Protection Working Party regarding the transfer of data to third states exist.[809] These principles are briefly analysed in following.

The working papers of the Article 29 Data Protection Working Party may not be formally binding, but they are important with regard to the practical application of Directive 95/46. The Commission often refers to the arguments of the Article 29 Data Protection Working Party when substantiating its own decisions.[810] To ensure an adequate protection, the Article 29 Data Protection Working Party establishes six core data protection content principles followed by procedural requirements. Compliance with these principles "could be seen as a minimum requirement for protection to be considered adequate".[811]

---

[806] Dammann and Simitis (1997), Article 25, para 8; Siemen (2006), p. 299; Engel (2003), p. 93. Tinnefeld et al. (1995), pp. 110 and 122.

[807] Dammann and Simitis (1997), Article 25, para 8.

[808] Document adopted by the Article 29 Working Party, WP 4 of 26 June 1997, first orientations on the transfer of personal data to third countries – possible ways forward in assessing adequacy.

[809] Document adopted by the Article 29 Working Party, WP 12 of 24 July 1998 on the transfers of personal data to third countries: applying Articles 25 and 26 of the EU data protection directive, combined the working papers WP 4 of 26 June 1997, first orientations on the transfer of personal data to third countries – possible ways forward in assessing adequacy, WP 7 of 14 January 1998 on the judging of industry self regulation: when does it make a meaningful contribution to the level of data protection in a third country?, WP 9 of 22 April 1998 on preliminary views on the use of contractual provisions in the context of transfers of personal data to third countries and WP 114 of 25 November 2005 on a common interpretation of Article 26 (1) of Directive 95/96.

[810] Compare Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland, OJ L-215/1, 25 August 2000; Commission Decision of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina, OJ L- 168/19, 5 July 2003 and Commission Decision of 21 November 2003 on the adequate protection of personal data in Guernsey, OJ L-308/27, 25 November 2003.

[811] Document adopted by the Article 29 Working Party, WP 12 of 24 July 1998 on the transfers of personal data to third countries: applying Articles 25 and 26 of the EU data protection directive, p. 5.

The content principles are summarised in six essential points:

(1) The purpose limitation principle[812]
(2) The data quality and proportionality principle[813]
(3) The transparency principle[814]
(4) The security principle[815]

[812] The only exemptions to the purpose limitation principle should be the grounds listed in Article 13 of the Directive 95/46: a restriction to the purpose principle is permitted if "such a restriction constitutes (a) a necessary measure to safeguard national security, (b) defence, (c) public security, (d) the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for regulates professions, (e) an important economic or financial interest of a Member State or of the EU, (f) a monitoring, inspection or regulatory function connected with the exercise of official authority in cases referred to in (c), (d) and (e) or (g) the protection of the data subject or the rights and freedoms of others, compare Document adopted by the Article 29 Working Party, WP 12 of 24 July 1998 on the transfers of personal data to third countries: applying Articles 25 and 26 of the EU data protection directive, p. 6.

[813] The principle of *data quality* (2) should ensure that data ought to be accurate and, where necessary, kept up to date. The *proportionality principle* (2) guarantees that the data are "adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed"; these two principles should guarantee the regularly verification of the stored data, i.e., that the protection of the person concerned extends beyond the first control of; since, according to Article 2 (b) of Directive 95/46, the storage of data is also a form of data processing, *Engel* assumes that these two principles in conjunction with the purpose limitation entail the obligation to delete the data when the original purpose of the processing changes afterwards, compare (2003), pp. 97–98.

[814] The *transparency principle* (3) contains that individuals should be provided with information as to the purpose of the processing and the identity of the data controller in the third country, and other information insofar as this is necessary to ensure fairness; the only exemptions permitted should be in line with Articles 11 (2) (exceptions for statistical purposes or for the purposes of historical or scientific research) and 13 of Directive 95/46 (includes exceptions for national security, (b) defence, (c) public security, (d) the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for regulates professions, (e) an important economic or financial interest of a Member State or of the EU, (f) a monitoring, inspection or regulatory function connected with the exercise of official authority in cases referred to in (c), (d) and (e) or (g) the protection of the data subject or the rights and freedoms of others.), compare Document adopted by the Article 29 Working Party, WP 12 of 24 July 1998 on the transfers of personal data to third countries: applying Articles 25 and 26 of the EU data protection directive, p. 6; the transparency principle should permit the person concerned to assess the risk of data processing in the third country, compare Simitis(2000), in particular pp. 472 and 477.

[815] The *security principle* (4) required that "technical and organisational security measures should be taken by the data controller that are appropriate to the risks presented by the processing". Any person operating under the authority of the data controller, including a processor, must not process data except on instructions from the controller. This principle is to counteract the fast technical development by developing normative limits to retain control about automated data processing. The need for technical security measures increases with regard to the rapid development in the information and communication technology. As compliance with this principle depends indeed on the development of automated data security systems, it is difficult to asses the level of protection regarding this criteria, compare Document adopted by the Article 29 Working Party, WP 12 of 24 July 1998 on the transfers of personal data to third countries: applying Articles 25 and 26 of the EU data protection directive, p. 6 and Simitis (2000), in particular p. 478.

(5) The rights of access, rectification and opposition[816] and
(6) Restrictions on onward transfers.[817]

The principles are strongly influenced by the provisions of Directive 95/46, but the Article 29 Data Protection Working Party stresses that the list "should not be set in stone".[818] In some cases "there will be a need to add to the list, while for others it may even be possible to reduce the list of requirements".[819] To specific types of processing, additional principles have to be applied.

In case of the processing of sensitive data, for instance, for those categories listed in Article 8 of Directive 95/46, "additional safeguards should be in place, such as a requirement that the data subject gives his/her explicit consent for the processing".[820] Also in case of the transfer of data for the purpose of direct marketing, "the data subject should be able to 'opt-out' from having its data used for such purposes at any stage".[821] Lastly, "where the purpose of the transfer is the taking of an automated decision in the sense of Article 15 of Directive 95/46, the individual should have the right to know the logic involved in this decision, and other measures should be taken to safeguard the individual's legitimate interest".[822]

[816] The *rights of access, rectification and opposition* (5) should ensure "the right to obtain a copy of all data relating to the data subject that are processed, and a right to rectification of those data where they are shown to be inaccurate". In certain situations the data subject should also be able to object to the processing of the data relating to him/her. The only exceptions to these rights should be in accordance with Article 13 of the Directive 95/46. This principle is closely related to the transparency principle and requires a reliable, regularly and comprehensible information accessible to the data subject, compare Document adopted by the Article 29 Working Party, WP 12 of 24 July 1998 on the transfers of personal data to third countries: applying Articles 25 and 26 of the EU data protection directive, p. 6; Dammann and Simitis (1997), introduction, p. 80 and Simitis (1997), in particular 281.

[817] The *transfer of personal data to other third states* (6) means that transfer to states different from the first recipient country should be only permitted if the other third state (the recipient of the onward transfer) ensures an adequate level of protection. The only exceptions permitted should be in line with Article 26 (1) of the Directive 95/46, compare Document adopted by the Article 29 Working Party, WP 12 of 24 July 1998 on the transfers of personal data to third countries: applying Articles 25 and 26 of the EU data protection directive, p. 6.

[818] Document adopted by the Article 29 Working Party, WP 12 of 24 July 1998 on the transfers of personal data to third countries: applying Articles 25 and 26 of the EU data protection directive, p. 5.

[819] Ibid.

[820] Document adopted by the Article 29 Working Party, WP 12 of 24 July 1998 on the transfers of personal data to third countries: applying Articles 25 and 26 of the EU data protection directive, p. 7. Article 8 of Directive 95/46 concerns for example data revealing racial or ethic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life, or data relating to offences, criminal convictions or security measures.

[821] Document adopted by the Article 29 Working Party, WP 12 of 24 July 1998 on the transfers of personal data to third countries: applying Articles 25 and 26 of the EU data protection directive, p. 7.

[822] Ibid.

In general, the principles of the Article 29 Data Protection Working Party are not as detailed as the provisions of the Directive 95/46 itself, so that a flexible application of the criteria becomes possible.

Procedural mechanisms such as sanctions for data processors in case of non-compliance with data protection rules, a right to redress for individuals or the establishment of supervisory authorities with monitoring and complaint investigation functions are further guarantees necessary to ensure an adequate protection.[823] Usually the procedural instruments assure the compliance with the aforementioned content principles. Outside the EU structures, such procedural instruments are not always part of the legal order. Therefore, a comparison between the European and the third country data protection standards may be difficult. In consequence, to provide a basis for the assessment of the adequacy of the protection in the third country, it is crucial to identify the essential objectives of a data protection procedural system and on this basis "to judge the variety of different judicial and non-judicial procedural mechanisms used in third countries".[824]

The Article 29 Data Protection Working Party proposes three objectives:

Firstly, a good level of compliance with the data protection rules should be ensured. This criterion is generally characterised "by a high degree of awareness among data controllers of their obligations, and among data subjects of their rights and the means of exercising them".[825] The existence of effective and dissuasive sanctions can also play an important role in ensuring compliance with the procedural rules supported by an effective supervisory system.[826] In this context, instead of considering only the legal and organisational instruments, the crucial point is the effective implementation of the rights and freedoms of the individual in practice.[827]

Secondly, support and help to individual data subjects in the exercise of their rights also plays an important role. Data subjects must be able to enforce their rights rapidly and effectively, and without excessive cost.[828] Furthermore there must be "some sort of institutional mechanism allowing independent investigation of complaints".[829] This independent control authority must be able to investigate and to guarantee redress where necessary.[830]

---

[823] Ibid.

[824] Ibid.

[825] Ibid.

[826] Ibid.

[827] Dammann and Simitis (1997), Article 25, para 28.

[828] Document adopted by the Article 29 Working Party, WP 12 of 24 July 1998 on the transfers of personal data to third countries: applying Articles 25 and 26 of the EU data protection directive, p. 7.

[829] Ibid.

[830] Brühann (1998).

Thirdly, appropriate redress to the injured party where rules are not complied with must be guaranteed. A "system of independent adjudication or arbitration which allows compensation to be paid and sanctions imposed where appropriate" should exist.[831]

(4) Brief Summary

The working papers of the Article 29 Data Protection Working Party regarding the transfer of data to third states create an adequacy profile whose content principles orientate on the provisions of Directive 95/46, although the main focus constitutes the effective enforcement of the rights in practice. This practical approach guarantees a decision closely related to the individual case, without sticking to predetermined criteria ("to be set in stone"). This means that, as long as the underlying objectives – which might be achieved trough mutual concessions – will be respected, the procedural mechanisms in third states may be different from the European ones.

In addition, the content principles set limits to the procedural objectives and prevent their ambiguous interpretation. This rather practical and less theoretical approach allows to react flexibly to changing data protection conditions of third countries. Finally the approach of the Article 29 Data Protection Working Party affirms the result discussed in the framework of the comparison with the European Council Convention No. 108 mentioned above.[832]

Summarising, the wording "adequacy" has to be interpreted in the sense of "functionally adequate", which means that the fundamental rights protection of the person concerned should be assessed in accordance with the concrete situation in the respective third country. Thereby, the purpose limitation principle is the most important, but at the same time the most problematic element. It is susceptible to abuse and should therefore be handled with care.[833] Respecting the purpose limitation principle assures a legitimate processing and therefore plays an important role in assessing whether the protection is adequate.

The content principles and the procedural mechanisms developed by the Article 29 Data Protection Working Party assure effective data protection regarding the transfer of data to third states. However, these principles and mechanisms only refer to Article 25 Directive 95/46. Exemptions to the principles are stipulated in Article 26 of the Directive 95/46. They will be illustrated in following.

[831] Document adopted by the Article 29 Working Party, WP 12 of 24 July 1998 on the transfers of personal data to third countries: applying Articles 25 and 26 of the EU data protection directive, p. 7.

[832] See Sect. III 2 e bb (2).

[833] To the possibilities of abuse, see Simitis (2000), in particular p. 476; Weichert (2006) and Dix and Gardain (2006), in particular 346.

cc) Derogations According to Article 26 Directive 95/46 and Article 9 (6) Regulation 45/2001

The derogations from the adequacy requirement listed in Article 26 Directive 95/46 and Article 9 (6) Regulation 45/2001 mainly refer to situations arising in the context of private data transfer and international economic transactions. Analysing this topic in details would go far beyond the objectives of this research. For that reason, the derogations are only briefly mentioned in the following.

In terms of Article 26 Directive 95/46 and Article 9 (6) Regulation 45/2001, the transfer to third countries not providing an adequate level of protection should be allowed under the condition that:

(a) The data subject has given his consent unambiguously to the proposed transfer; or
(b) The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or
(c) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or
(d) The transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or
(e) The transfer is necessary in order to protect the vital interests of the data subject; or
(f) The transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

The derogations usually concern cases where legally protected interests of third parties play a role or where there is a small risk to interfere with the right to privacy. Nevertheless, the derogations have to be interpreted restrictively and in view of the fundamental rights considering Article 1 (1) of Directive 95/46.[834]

Article 26 (2) Directive 95/46 and Article 9 (7) Regulation 45/2001 authorise Member States or the EDPS to transfer personal data (or a set of personal data) to a third country which does not ensure an adequate level of protection, where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights. Such safeguards may in particular result from appropriate contractual clauses.[835]

[834] Wuermeling (2000), p. 142.

[835] Article 26 (3) of Directive 95/46 provides a reporting requirement for the Member States about the authorisations they grant pursuant to paragraph 2. If a Member State or the Commission objects

dd) Data Transfer in the Framework Decision Governing Data Processing in Police and Judicial Cooperation

Quite contrary to the rather detailed provisions and the additional documents regulating and specifying personal data transfer in the framework of Directive 95/46 and Regulation 45/2001, the FDPJ includes far less guidelines. Its provisions refer to the data transfer to third states and to private parties.[836] While the former first pillar Regulation 45/2001 ensures the application of the data protection principles of Directive 95/46 in former first pillar EU institutions and bodies, the FDPJ does not regulate EU-internal personal data transfer in the framework of police and judicial cooperation.

Recital (23) of the FDPJ stipulates that where personal data are transferred from a Member State to third states or international bodies, these data should, *in principle*, benefit from an adequate level of protection.[837] Article 13 (1) FDPJ specifies that personal data may be transferred only, if (a) it is necessary for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties (b) the receiving authority in the third tate or receiving international body is responsible for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties (c) the Member State from which the data were obtained has given its consent to the transfer in compliance with its national law[838] and (d) the third state or international body concerned ensures an adequate level of protection for the intended data processing.

---

on justified grounds involving the protection of the privacy and fundamental rights and freedoms of individuals, the Commission shall take appropriate measures in accordance with the procedure laid down in Article 31 (2) Directive 95/46. Member States shall take the necessary measures to comply with the Commission's decision.

Pursuant to the last paragraph the Commission can decide that certain standard contractual clauses offer sufficient safeguards as required by Article 26 (2) Directive 95/46. So far there a three Commission decisions according to standard contractual clauses, compare 2001/497/EC: Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC, OJ 2001, L-181/19; 2002/16/EC: Commission Decision of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC, OJ L-6/52 and 2004/915/EC: Commission Decision of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, OJ 2004, L-385/74.

[836] Articles 13 and 14 FDPJ, OJ 2008, L-350/60.

[837] Recital (26) FDPJ, OJ 2008, L-350/60.

[838] Transfer without prior consent in accordance with paragraph 1(c) shall be permitted only if transfer of the data is essential for the prevention of an immediate and serious threat to public security of a Member State or a third state or to essential interests of a Member State and the prior consent cannot be obtained in good time; the authority responsible for giving consent shall be informed without delay, compare Article 13 (2) FDPJ, OJ 2008, L-350/60.

Article 13 (4) FDPJ uses the same formulation as Directive 95/46 when is comes to the specification of the adequacy of the level of protection.[839] However, whether or not the term *adequate* refers to the same strict criteria stipulated in the framework of Directive 95/46 is not further specified. Moreover, broad exceptions to these conditions apply. Personal data may be transferred if (a) the national law of the Member State transferring the data so provides because of: (i) legitimate specific interests of the data subject or (ii) legitimate prevailing interests, especially important public interests or (b) the third state or receiving international body provides safeguards which are deemed adequate by the Member State concerned according to its national law.[840] Consequently, personal data relating to police and judicial purposes can be transferred to third states or international organisations for various reasons. Member States may assess the level of adequacy on their own. Very vague and far reaching derogations to the criteria stipulated in Article 13 (1) FDPJ, such as public interests, apply. Additionally, Article 26 FDPJ permits further derogations in case that Member States or the EU have already concluded (at the time of the adoption of the FDPJ) bilateral or multilateral agreements with third states which provide for other rules.[841]

Another provision which aroused criticism[842] is Article 14 FDPJ referring to the transmission of personal data to private parties. Personal data collected for police and judicial purposes can be transferred to private parties if (a) the competent authority of the Member State from which the data were obtained has consented to transmission in compliance with its national law, (b) no legitimate specific interests of the data subject prevent transmission, and (c) in particular cases transfer is essential for the competent authority transmitting the data to a private party for: (i) the performance of a task lawfully assigned to it, (ii) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, (iii) the prevention of an immediate and serious threat to public security or (iv) the prevention of serious harm to the rights of individuals.[843] The party transmitting the data shall inform the private party of the purposes for which the data may exclusively be used.[844]

---

[839] The level of protection shall be assessed in the light of all the circumstances surrounding a data transfer operation or a set of data transfer operations. Particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the state of origin and the state or international body of final destination of the data, the rules of law, both general and sectoral, in force in the third state or international body in question and the professional rules and security measures which apply (compare Article 13 (4) FDPJ, OJ 2008, L-350/60).

[840] Article 13 (4) FDPJ, OJ 2008, L-350/60.

[841] Ibid.

[842] Compare EDPS opinion on the FDPJ, OJ 2007, C-139/1, paras 34–36.

[843] Article 14 (1) FDPJ, OJ 2008, L-350/60.

[844] Ibid.

When reading these provisions, it becomes clear that personal data can be transferred to private parties for various reasons. It is not required that the purpose of collection is maintained. In fact, the transmitting party may establish a new purpose for which the data may then be processed by the private party. Additional supervision in this sensitive area is not provided for in this context. Although the FDPJ regulates the transfer of law enforcement data to private parties, it regrettably remains silent on the topic of rules regulating the access of law enforcement bodies to data stored in private databases. Recent developments such as the Data Retention Directive or the PNR agreements with the USA[845] clearly show the need for regulation in this currently unregulated field.

f) Transparency and Data Protection

The balance between transparency and the right of individuals for the protection of their personal data is not only important in the ECHR context,[846] it was also recently subject to the famous EU case *Bavarian Lager Co. Ltd v. Commission*.[847] In a nutshell, *Bavarian Lager*, a German trade association for beer, requested the annulment of a Commission decision rejecting its request for full access to the minutes of a meeting organised by the Commission. Based on Article 4 (1) (b) Regulation 1049/200 on access to documents,[848] the Commission had refused access to the names of 5 members of trade associations attending the meeting on grounds of the protection of their personal data following from the application of Regulation 45/2001.[849] While the Court of First Instance (now General Court) in

[845] For an overview of the transfer of data to the United States, compare, Bellanova and De Hert (2009).

[846] The case *Társaság a Szabadságjogokért v. Hungary*, Application no. 37374/05, judgment of 14 April 2009 of the ECtHR is worth remembering here, compare above Sect. II 2 c.

[847] Cases: T-194/04, *Bavarian Lager Co. Ltd v. Commission*, judgment of 8 November 2007, reversed in appeal in case C-28/08, *Bavarian Lager Co. Ltd v. Commission*, judgment of 29 June 2010; compare Sanner (2010); Wägenbaur (2001).

[848] Regulation No. 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, OJ 2001, L-145/43, Article 4 (1) (b) stipulates that: "the institutions shall refuse access to a document where disclosure would undermine the protection of privacy and the integrity of the individual, in particular in accordance with Community legislation regarding the protection of personal data."

[849] The fundamental difference between the right of access to documents and the right of individuals for the protection of their personal data is excellently summarised by the Court of First Instance (General Court) in para 98 of the judgment *Bavarian Lager Co. Ltd v. Commission*: Regulation 1049/2001 is "designed to ensure the greatest possible transparency of the decision-making process of the public authorities and the information on which they base their decisions. It is thus designed to facilitate as far as possible the exercise of the right of access to documents, and to promote good administrative practices". Regulation 45/2001 "is designed to ensure the protection of the freedoms and fundamental rights of individuals, particularly their private life, in the handling of personal data", T-194/04, *Bavarian Lager Co. Ltd v. Commission*, judgment of 8 November 2007, para 98.

2007 obliged the Commission to disclose the names of the attendants arguing that the disclosure would not undermine the privacy of the relevant persons (mainly because they attended the meeting in their role as an official representative of a collective body and not as a private person),[850] the Court of Justice in 2010 repealed this decision.

It ruled that the General Court correctly held that surnames and forenames may be regarded as personal data and that the communication of personal data in response to a request for access of documents falls within the definition of processing for the purpose of Regulation 45/2001.[851] However, it held that the General Court disregards the wording of the exception provided for in Article 4 (1) (b) of Regulation 1049/2001,[852] which requires that any undermining of privacy and the integrity of an individual must be examined and assessed in conformity with the legislation of the EU, in particular with Regulation 45/2001.[853] The General Court mainly focused on Article 8 and the case law of the ECtHR to assess the conformity. The Court of Justice made clear that the reference to Article 8 ECHR and the case-law of the ECtHR indeed applies to processing carried out by Community institutions and bodies falling outside the scope of Regulation 45/2001 (activities relating to police and judicial cooperation and common foreign and security policy),[854] but not to the activities covered by Regulation 45/2001.[855]

It follows that "where a request based on Regulation No. 1049/2001 seeks to obtain access to documents including personal data, the provisions of Regulation No 45/2001 become applicable in their entirety, including Articles 8 and 18 thereof".[856] Consequently, the Commission was right to verify whether the attendants had given their consent to disclosure of personal data concerning them. The Commission correctly based its reasoning on Article 4 (1) (b) of Regulation 1049/2001 and Regulation 45/2001 and succeeded in establishing an equilibrium

[850] T-194/04, *Bavarian Lager Co. Ltd v. Commission*, judgment of 8 November 2007, paras 145–158.

[851] Ibid.

[852] "The institutions shall refuse access to a document where disclosure would undermine the protection of privacy and the integrity of the individual, in particular in accordance with Community legislation regarding the protection of personal data" (Regulation No. 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, OJ 2001, L-145/43, Article 4 (1) (b)).

[853] C-28/08, *Bavarian Lager Co. Ltd v. Commission*, judgment of 29 June 2010, para 59.

[854] Compare recital (15) of Regulation No. 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, OJ 2001, L-145/43.

[855] C-28/08, *Bavarian Lager Co. Ltd v. Commission*, judgment of 29 June 2010, para 62.

[856] Ibid, para 63. Article 8 (b) of Regulation 45/2001 refers to the transfer of personal data to recipients, other than Community institutions and bodies, subject to Directive 95/46 "if the recipient establishes the necessity of having the data transferred and if there is no reason to assume that the data subject's legitimate interests might be prejudiced". Article 18 of Regulation 45/2001 refers to the data subject's right to object.

between the two regulations in question.[857] As provided for in Article 8 (b) of Regulation 45/2001,[858] it rightly required that *Bavarian Lager* must establish the necessity for transfer of the relevant personal data. As the necessity was not convincingly demonstrated, the Commission was right to reject the application for access to the full minutes.[859]

The importance of the case lies in the balance between the issues of transparency/access to documents and the protection of personal data. Critical voices feared that data protection arguments risks to be invoked in order to minimise transparency of the institutions.[860] The EDPS, supporting the applicant, argues that the reasoning of the Commission that information can only be disclosed after the attendants have given their consent or if *Bavarian Lager* proves the necessity of having the data transferred (Article 8 (b) Regulation 45/2001) risks to become counterproductive to data protection objectives.[861] An interpretation of the Article 8 (b) of Regulation 45/2001[862] which would deprive the access Regulation 1049/2001 of its main content should be avoided.[863] Article 6 of Regulation 1049/2001 underlines that the applicant for access to a document is not obliged to state reasons for the application.[864]

The interpretation of Article 8 (b) of Regulation 45/2001 according to which the applicant must justify its request would therefore be contrary to the objective of Regulation 1049/2001.[865] The EDPS refers to the *Borax v. Commission* case in which the Court of First Instance (General Court) confirmed that names can be disclosed to the applicant without the consent of the person concerned if the privacy

[857] C-28/08, *Bavarian Lager Co. Ltd v. Commission*, judgment of 29 June 2010, paras 65 and 67.

[858] Article 8 (b) of Regulation 45/2001 refers to the transfer of personal data to recipients, other than Community institutions and bodies, subject to Directive 95/46 "if the recipient establishes the necessity of having the data transferred and if there is no reason to assume that the data subject's legitimate interests might be prejudiced".

[859] C-28/08, *Bavarian Lager Co. Ltd v. Commission*, judgment of 29 June 2010, para 79.

[860] Compare the Pleadings of the EDPS of 16 June 2009 at the hearing of the Court in case C-28/08, *Bavarian Lager Co. Ltd v. Commission*, accessible at: http://www.edps.europa.eu/EDPSWEB/edps/lang/en/Consultation/Court (accessed February 2011).

[861] Ibid.

[862] Article 8 (b) of Regulation 45/2001 refers to the transfer of personal data to recipients, other than Community institutions and bodies, subject to Directive 95/46 "if the recipient establishes the necessity of having the data transferred and if there is no reason to assume that the data subject's legitimate interests might be prejudiced".

[863] Pleadings of the EDPS of 16 June 2009 at the hearing of the Court in case C-28/08, *Bavarian Lager Co. Ltd v. Commission*, p. 2, accessible at: http://www.edps.europa.eu/EDPSWEB/edps/lang/en/Consultation/Court (accessed February 2011).

[864] Article 6 (1) Regulation No. 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, OJ 2001, L-145/43.

[865] Pleadings of the EDPS of 16 June 2009 at the hearing of the Court in case C-28/08, *Bavarian Lager Co. Ltd v. Commission*, p. 4, accessible at: http://www.edps.europa.eu/EDPSWEB/edps/lang/en/Consultation/Court (accessed February 2011).

is not effectively undermined by such disclosure.[866] The EDPS refers to the risk of censoring the public debate if persons acting in public decision-making could themselves decide in the name of their personality rights whether or not to publish information. It refers to the ECtHR case *Társaság a Szabadságjogokért v. Hungary*, briefly discussed above,[867] in which the ECtHR insisted that "it would be fatal for the freedom of expression if public figures could censor the press and public debate in the name of their personality rights".[868] A similar reasoning could be applied in the *Bavarian Lager* case.

The dispute in this case clearly demonstrates that the balance between transparency and data protection is not always easy to find. The dangers of a possible misuse of data protection arguments to restrict public access to documents are real and require a sophisticated solution. Taking this risk into account, the solution can not be the supremacy of data protection provisions in any potential case, as postulated by the Court of Justice in the *Bavarian Lager* case. As we have seen above, according to the Court's reasoning, whenever personal data is involved, the rules on data protection apply, even to the detriment of transparency.[869] This, however, does not constitute a real balance. One of the solutions therefore could be the strict application of proportionality requirements following from Article 5 (4) TEU.[870] In case that two rights conflict, the usual balance relates to the application of the principle of proportionality.[871] For that reason, data protection concerns could not generally override the interest in public access to documents. On the contrary the interest of the individual in keeping its data secret and the interest of the applicant of public access must be critically weighted. Excluding this assessment from the outset, by arguing that if based on Regulation No. 1049/2001 an applicant seeks access to documents containing personal data, the provisions of Regulation 45/2001

[866] Compare case T-121/05, *Borax Europe Ltd. v. Commission*, judgment of 11 March 2009, paras 40–42, and Pleadings of the EDPS of 16 June 2009 at the hearing of the Court in case C-28/08, *Bavarian Lager Co. Ltd v. Commission*, p. 5, http://www.edps.europa.eu/EDPSWEB/edps/lang/en/Consultation/Court (accessed February 2011).

[867] Compare above Sect. II 2 c.

[868] *Társaság a Szabadságjogokért v. Hungary*, Application no. 37374/05, judgment of 14 April 2009, para 37.

[869] Compare the reasoning in para 63 of the *Bavarian Lager* judgment in which the Court of Justice stipulated: "It follows that where a request based on Regulation No. 1049/2001 seeks to obtain access to documents including personal data, the provisions of Regulation No 45/2001 become applicable in their entirety, including Articles 8 and 18 thereof", C-28/08, *Bavarian Lager Co. Ltd v. Commission*, judgment of 29 June 2010, para 63.

[870] Compare for an excellent analysis: EDPS background paper series, July 2005, n°1, "public access to documents and data protection", in particular pp. 32–40, accessible at: http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/Papers (accessed February 2011).

[871] *Koch* (2003), pp. 158–172, and EDPS background paper series, July 2005, n°1, "public access to documents and data protection", in particular pp. 32–40, accessible at: http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/Papers (accessed February 2011).

become applicable in their entirety,[872] the full respect of the proportionality principle is denied. The aforementioned *Schecke* case[873] in which the Court obliged the EU legislator to balance the different interests involved (namely transparency and the infringements of the rights to data protection and private life) by carrying out a detailed proportionality test can serve as an example for the method to be applied in similar cases.

g) Common Foreign and Security Policy

With regard to the common foreign and security policy, there is no harmonised standard or general framework governing data processing in this area.[874] However, it should be briefly mentioned that the European Union Courts established case law on the legitimacy of some activities of the common foreign and security policy regarding the management of so called terrorists' blacklists.

In the cases *Sison v. Council*, *Organisation des Modjahedines de people d'Iran (OMPI) v. Council* and *PKK and KNK v. Council*,[875] the Tribunal of First Instance annulled two Council Decisions implementing Article 2 (3) of Regulation No. 2580/2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism and repealed the Council Decision placing the applicants on the list of terrorist organisations. Some of the applicants achieved their erasure from the blacklist and, consequently, the Council agreed in April 2007 to a new policy regarding the way in which individuals and groups are added to the list, taking into consideration the *Modjahedines* judgement.[876] This policy includes "that the parties concerned will be informed that the Council intends to maintain them on the list and will be informed via a "statement of reasons" of the specific information that forms the basis for the Council's decision".[877] "The persons, groups and entities concerned will also be informed about the opportunity to make their views known and present observations".[878] The Council will also "consider any reaction by the parties concerned before taking

[872] C-28/08, *Bavarian Lager Co. Ltd v. Commission*, judgment of 29 June 2010, para 63.

[873] Compare Sect. III 1 e.

[874] Hijmanns and Scirocco (2009), in particular p. 1447.

[875] Cases T-228/02, *Organisation des Modjahedines de people d'Iran v. Council*, judgment of 12 December 2006; T-284/08, *Organisation des Modjahedines de people d'Iran v. Council*, judgment of 4 December 2008; Case T-47/03, *Sison v. Council*, judgment of 11 July 2007; C-266/05 P, *Sison v. Council*, judgment of 1 February 2007 and C-229/05 P, *PKK and KNK v. Council*, judgment of 18 January 2007.

[876] See Council press release 8425/07 (Presse 80), p. 34, 35; for further information see Guild (2008), in particular p. 189; with regard to the protection against the placing on the lists, see Feinäugle (2010), pp. 188–190; Gless and Schaffner (2009).

[877] Council press release 8425/07 (Presse 80), p. 35.

[878] Ibid.

a final decision".[879] Member States are therefore required to provide information concerning the reasons of the placement of certain persons on the list.

In the aforementioned cases,[880] the Court of Justice used elements of data protection to guarantee the protection of other fundamental rights, such as the right to defence and judicial protection.[881] Although the Court of Justice in *Sison v. Council* made clear that Regulation 1049/2001[882] does not include a right to access personal data, the Court however refers to the possibility that the applicant may have a right to be informed about the nature and cause of the accusations against him and that this right may involve the access to documents held by the Council.[883] In *Organisation des Modjahedines de people d'Iran v. Council,*[884] the rights of defense were violated because the Council did not comply with the requirement to duly inform the applicants about the processing of their personal data.[885] In *PKK and KNK v. Council,*[886] the Court of Justice underlines the importance of periodical reviews of the situation which lead to the inclusion of the persons in the blacklists.[887] In other words, the principle to keep personal data accurate and up to date was duly considered.[888]

Although none of the aforementioned cases directly mention data protection guarantees, the case-law shows that even in common foreign and security policy[889] certain minimum legal requirements, which include data protection elements, apply in the context of personal data processing in this area. With the entry into force of the Lisbon Treaty, the situation for individuals in the area of common foreign and security policy has additionally improved. Although, in general, the Court of Justice shall not have jurisdiction with respect to the provisions relating to the common foreign and security policy or with respect to acts adopted on the basis of those

[879] Ibid.

[880] Cases C-266/05 P, *Sison v. Council*, judgment of 1 February 2007, T-284/08, *Organisation des Modjahedines de people d'Iran v. Council*, judgment of 4 December 2008 and C-229/05 P, *PKK and KNK v. Council*, judgment of 18 January 2007.

[881] For an excellent analysis of this case law and its data protection elements, see Hijmanns and Scirocco (2009), in particular p. 1509.

[882] Regulation 1049/2001 (of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, OJ 2001, L-145/43) gives the general public a right of access to documents of the institutions and should not be confused with the right to access to personal data subject to Regulation 45/2001.

[883] Case C-266/05 P, *Sison v. Council*, judgment of 1 February 2007, para 48, and Hijmanns and Scirocco (2009), in particular p. 1510.

[884] Case T-284/08, *Organisation des Modjahedines de people d'Iran v. Council*, judgment of 4 December 2008.

[885] Ibid.

[886] Case C-229/05 P, *PKK and KNK v. Council*, judgment of 18 January 2007.

[887] Ibid.

[888] Hijmanns and Scirocco (2009), in particular p. 1511.

[889] A good overview of the recent developments in the Common Foreign and Security Policy is made by Oppermann et al. (2009), pp. 684–701.

provisions, Article 275 TFEU stipulates that the Court of Justice has jurisdiction in proceedings "reviewing the legality of decisions providing for restrictive measures against natural or legal persons adopted by the Council on the basis of Chapter 2 of Title V [specific provisions on the common foreign and security policy] of the Treaty on European Union".[890]

3. *Conclusion: Data Protection Rules in the AFSJ are Still a Patchwork*

The patchwork of data protection rules in the AFSJ leads to a complex situation in EU data protection law in which the former pillar structures still have a great impact on the current post-Lisbon area.[891] Nonetheless, the impact of the Lisbon Treaty is important and can lead to the adoption of a comprehensive data protection framework for future data processing in this area. The *status quo* however is not yet sufficient in terms of data protection rules. The restricted scopes of the main instruments in force (Directive 95/46, Regulation 45/2001 and FDPJ) and the lack of principles for security related data processing developed through EU case-law constitute a major problem. The FDPJ with its vague provisions and broad exceptions can unfortunately not fill this gap.

The case law in the framework of the former first pillar, in particular in the case *Huber v. Germany*, nonetheless shows the willingness of the EU Courts to establish a data protection regime which goes beyond the former third pillar structure. By recognizing the discriminatory effect of a database used for crime fighting purposes which contained only the data of a particular group of persons, the Court of Justice raised hopes for the indiscriminate application of data protection principles also in the former third pillar. This tendency needs to be confirmed in future judgments in this area.

The described patchwork situation is additionally reflected in rather weak data protection quality standards and individual rights guarantees included in the FDPJ. The purpose limitation principle is extended to a point where the authorities processing the data can decide about the change of the purpose. The initial aim of the purpose limitation principle, which is the protection of individual rights against the indiscriminate use of personal data, is therefore reversed. In addition to the purpose limitation principle, important guarantees, such as the accuracy and adequacy of data, the respect of time limits, the protection of sensitive data and the up to date nature of data are included in all three instruments. But again, the guarantees in the FDPJ are formulated in a mitigated way.

---

[890] Compare Article 275 TFEU.

[891] For a brief and general overview of the data protection provisions in Europe, refer to Holznagel and Werthmann (2010), pp. 2001–2019.

The rights of the individuals, including notification, access, erasure, blocking, deletion, objection and independent supervision, are additionally granted in the analysed instruments. The obligation to notify the individuals about the data processing in the framework of the FDPJ is however not compulsory and is left to the discretion of the Member States. Additionally, the right to get access to personal data is regulated more exhaustively in Directive 95/45 and Regulation 45/2001 when comparing it to the access right in the FDPJ. In the framework of Directive 95/46 it even includes in certain cases that states must be able to inform the applicant not only about data processing currently taking place, but also about the extent to which personal data have been disclosed to third parties in the past.[892]

The right to object to the processing of personal data is only stipulated in Directive 95/46 and Regulation 45/2001. The FDPJ does not include a similar provision, although, as previously mentioned, there may be situations in which persons concerned by data processing in a police and judicial context (e.g. victims or witnesses) have legitimate grounds to object. These situations should therefore also be considered in a police and judicial context. The requirement of independent supervision applies to all of the analysed instruments. In this context, the term "supervision" is interpreted in a broad way which includes that the mere risk that authorities may be subject to political influence violates the independence requirement of Directive 95/45.[893]

Provisions restricting the transfer of personal data to third parties are regulated in detail in Directive 95/46 and Regulation 45/2001. In particular the adequacy requirement of Directive 95/46, including its interpretations by the Article 29 Data Protection Working Party, establish a quite comprehensive data protection regime with regard to the transfer of personal data to third states. The opposite however is true in respect of the FDPJ which includes far reaching derogations for Member States when it comes to data transfer to third states. Crucial subjects such as the access by law enforcement authorities to data stored in private databases are not regulated in the FDPJ.

There is no data protection framework governing the common foreign and security policy. According to Article 39 TEU, the Council shall however adopt in future a decision laying down data protection rules in this area.[894] So far, the Court of Justice in its case law on the so called terrorist blacklists[895] however used

[892] Case C-553/07, *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer*, judgment of 7 May 2009.

[893] Case C-518/07, *Commission v. Germany*, judgment of 9 March 2010, para 36.

[894] Article 39 TEU.

[895] For instance Cases C-266/05 P, *Sison v. Council*, judgment of 1 February 2007, T-284/08 *Organisation des Modjahedines de people d'Iran v. Council*, judgment of 4 December 2008 and C-229/05 P, *PKK and KNK v. Council*, judgment of 18 January 2007.

elements of data protection to guarantee the protection of other fundamental rights, such as the right to defence and judicial protection.[896]

To sum up, the formulations used and the guarantees stipulated in the FDPJ are to a great extent less strict in terms of data protection rights than the rules contained in Directive 95/46 and Regulation 45/2001. In addition, the restricted scope of the FDPJ considerably limits its application the AFSJ. Due to these shortcomings, the legal instruments establishing the AFSJ actors play an important role in the analysis of the data protection guarantees applicable in the AFSJ. Their data processing framework is analysed in the next section.

[896] For an excellent analysis of this case law and its data protection elements, see Hijmanns and Scirocco (2009), in particular p. 1509.

http://www.springer.com/978-3-642-22391-4

Information Sharing and Data Protection in the Area of Freedom, Security and Justice
Towards Harmonised Data Protection Principles for Information Exchange at EU-level
Boehm, F.
2012, XII, 468 p., Hardcover
ISBN: 978-3-642-22391-4