Chapter 8
Information Sharing in the Area of Freedom, Security and Justice—Towards a Common Standard for Data Exchange Between Agencies and EU Information Systems

Franziska Boehm

8.1 Introduction

In the Area of Freedom, Security and Justice[1] (AFSJ), the process of European integration has considerably supported the establishment of Union bodies, agencies and information systems in recent years. Horizontal information sharing, including the exchange of personal data between these bodies, has become an essential tool in the internal security policy of the European Union (EU). Inter-agency cooperation between AFSJ actors, such as Europol, Eurojust or Frontex as well as the Commission's anti-fraud unit, OLAF, led to the conclusion of agreements providing for mutual information exchange. In addition, the access of law enforcement and judicial agencies

This contribution is based on my PhD research carried out during the last years. It provides a brief overview of some of the results of the research. The complete thesis with the title: "Information sharing and data protection in the Area of Freedom, Security and Justice" is published by Springer.

[1] The term AFSJ is a political notion describing several policies brought together under the umbrella of an overarching concept. Introduced by the Treaty of Amsterdam and further developed in the Lisbon Treaty, this policy aims at offering "its citizens an area of freedom, security and justice without internal frontiers, in which the free movement of persons is ensured in conjunction with appropriate measures with respect to external border controls, asylum, immigration and the prevention and combating of crime" (Article 3 (2) TEU). These political goals are practically enforced by the adoption of multi-annual work programmes (the Vienna (1998), the Tampere (1999), the Hague (2004) and the Stockholm programme (2009)), which establish general priorities and political objectives in this area. Although multi-annual work programmes are not as such binding instruments, these programmes set different political goals, which are subsequently legally implemented by the instruments available to the European legislator, primarily by way of Directives, Regulations and Council Decisions. As a result thereof, these programmes have a substantial effect on the future institutional policy and often directly influence legislative actions in this area.

F. Boehm (✉)
University of Luxembourg, Luxembourg
e-mail: franziska.boehm@uni.lu

S. Gutwirth et al. (eds.), *European Data Protection: In Good Health?,*
DOI 10.1007/978-94-007-2903-2_8, © Springer Science+Business Media B.V. 2012

to data stored in the European information systems, such as the Customs- (CIS), the Schengen- (SIS) or the Visa Information System (VIS) and Eurodac, occupies an increasingly important place in this area.

Post-9/11 policy concepts, such as "the Hague" and "the Stockholm programmes", promote an enhanced cooperation and coordination of law enforcement agencies and other agencies in the AFSJ.[2] Under their influence, formerly not related policy areas, such as the prevention of crime and immigration, are swiftly linked and lead to an intensive cooperation between AFSJ actors of a completely different legal nature, vested with different powers (Mitsilegas 2009). Without being limited by the former pillar constraints and, above all, in absence of a unified approach to data protection in judicial and criminal matters[3], legal and structurally different bodies, equipped with different tasks, exchange and transfer personal data within and outside the EU. The result is that data collected for one specific purpose may be transferred and used for other purposes completely unrelated to the original collection. This fast increasing cooperation at multiple levels necessarily touches upon different data protection regimes. Title V TFEU specifies the policies of the AFSJ.[4] They are a mix of former first as well as former third pillar policies.[5] While on the one hand information and personal data exchange is identified as a priority in this field, on the other hand data protection concerns risk to be undermined.

---

[2] The Hague programme adopted in 2004, for instance, promoted the enforced cooperation of the actors in the AFSJ and introduced the "availability principle", which should govern law enforcement-related data exchange from then on. Bilateral agreements between EU bodies and provisions in secondary legislation were foreseen intending to exchange data and leading, amongst others, to a reinforced inter-agency cooperation. Other measures aimed to allow mutual access to databases or their common use. National databases were supposed to become "interoperable" and direct access to central EU databases such as the SIS should have been established whereby nevertheless data protection standards should have been "strictly observed" (The Hague Programme: Council doc. 16054/04 from 13 December 2004, point 2.1, pp. 18–19). As a main consequence of this instrument, which covered the period from 2005 to the end of 2009, more and more data were shared and the actors in the AFSJ worked closer together than before. The period after 2009 is now covered by the Stockholm programme valid from 2010 to 2014 endorsing the availability principle while repeating the data protection pleas (The Stockholm Programme, Council doc. 17024/09 from 2 December 2009, point 4.2.2, pp. 37–38), Compare also note from the General Secretariat to the Standing Committee on operational cooperation on internal security (COSI), final report on the cooperation between JHA agencies, Council doc. 8387/10 from 9 April 2010.

[3] Council Framework Decision 2008/977/JHA 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 FDPJ, OJ 2008, L-350/60 represents a first step towards a comprehensive framework in this area; the FDPJ is, however, very restricted in scope as it is, for instance, not applicable to the data processing of most of the AFSJ law enforcement agencies, such as Europol and Eurojust, as well as at other AFSJ exchange systems, that is, the Schengen or the Customs Information Systems; moreover, excluded from the scope is also the internal processing of the Member States in police and criminal matters.

[4] Four main areas stand out: policies on border checks, asylum and immigration, judicial cooperation in civil as well as in criminal matters and police cooperation (Title V Chapters 2–5 TFEU).

[5] The Provision on police and judicial cooperation in criminal matters (former Title VI EU Treaty) are former third pillar policies whereas the provisions on asylum and immigration were regulated under former first pillar Community law (Title IV EC Treaty).

Questions relating to the coherency and the respect of data protection rules within this cooperation network of the AFSJ actors seem to be pushed into the background. This unbalanced situation can have a profound impact on the rights of the individuals. It is worth pointing out that, even though the context in which information is used is changing rapidly, no evaluation or overview of the existing data collection, processing and data-sharing systems, including a thorough assessment of their effectiveness, their possible overlapping effects, proportionality and their respect of data protection rights have been carried out so far.[6]

In the light of these considerations, this chapter first, in Sect. 2, briefly illustrates the legal background of data protection rules in the AFSJ. Section 3 focuses on the organisation of the existing and the planned instruments governing AFSJ data exchange as well as their compliance with the data protection rules mentioned in Sect. 1. Inconsistencies in the AFSJ data exchange network relating, among others, to gaps of protection, transparency issues and incoherent access procedures and conditions are disclosed. In the respective subsections, comments and criticism are offered and problems are highlighted. Section 4 suggests some basic data protection standards, which follow from the respect of Article 8 ECHR and would improve the respect of data protection rules in the field of internal AFSJ information sharing.

8.2 Legal Background

Before analysing the instruments governing AFSJ information exchange, the data protection rules applicable in this area need to be briefly identified.

8.2.1 Data Protection Before Lisbon

Due to the former pillar structure, data processing in third pillar security-related matters was not included in the relatively comprehensive data protection framework of the first pillar. While, since 1995, the Data Protection Directive 95/46[7] accompanied by sector-specific first pillar instruments[8] has established a wide-ranging data and privacy protection for individuals in an economic-related first pillar context,

[6] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions—Delivering and area of freedom, security and justice for European's citizens—Action Plan implementing the Stockholm Programme, COM(2010) 171 final, in particular p. 6.

[7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995, L-281/31.

[8] For instance: 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.

data processing for security purposes carried out by governmental law enforcement agencies was excluded from the scope of Directive 95/46.[9]

For a long time, data protection in the framework of former third pillar matters was therefore covered by public international law instruments instead of EU law, most notably by the instruments of the Council of Europe (Siemen 2006).[10] Article 8 of the ECHR and its interpretation by the Strasbourg Court as well as Convention No. 108[11], its respective additional protocols[12] and Recommendation (87) 15[13] built the reference instruments for security-related data processing in the EU.[14]

8.2.2 Guarantees for Security-Related Data Processing in Article 8 ECHR

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 quite comprehensive data protection framework in this specific area (Siemen 2006; De Schutter 2008).[15] The main principles are briefly summarised in the following.

---

[9] Article 3 (2) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995, L-281/31. This statement was clarified by the ECJ in the famous PNR case: joined cases C-317/04 and C-318/04, *Parliament v. Council*, [2006], ECR I-4721.

[10] Compare for a profound analysis of the instruments of the Council of Europe.

[11] Convention No. 108 of the Council of Europe for the protection of individuals with regard to automatic processing of personal data from 28 January 1981.

[12] In particular the additional protocol to Convention for the protection of individuals with regard to automatic processing of personal data regarding supervisory authorities and trans-border data flows, which entered into force in 2004.

[13] Recommendation R (87) 15 of the Committee of Ministers to the Member States regulating the use of personal data in the police sector, adopted 17 September 1987.

[14] However, since the adoption of the Framework Decision "on the protection of personal data in the framework of police and judicial cooperation in criminal matters" (DPFD) in 2008, OJ 2008, L-350/60, certain minimum requirements also apply in the field of security-related data processing at the EU level.

[15] See: Siemen (2006). 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. Compare also: De Schutter (2008). See also: joint declaration on cooperation and partnership between the Council of Europe and the European Commission from 3 April 2001, accessed July 12, 2011, http://www.jp.coe.int/Upload/91_Joint_Declaration_EF.pdf; Memorandum of Understanding between the Council of Europe and the European Union from 10 May 2007, CM(2007)74, accessed July 12, 2011, https://wcd.coe.int/ViewDoc.jsp?Ref=CM(2007)74&Language=lanEnglish.

The Strasbourg Court refers to the right to private life of article 8 ECHR when data protection infringements are at stake.[16] Even if personal 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.[17]

The jurisprudence of the ECtHR clearly illustrates that governmental data collection and retention interferes with the right to private life as protected by article 8 ECHR.[18] Every transmission of personal data from one authority to another, including the subsequent use of such data, constitutes another separate interference with individual rights under article 8 ECHR. The transmission enlarges the group of individuals with knowledge of the personal data and can therefore lead to investigations being instituted against the persons concerned.[19] The indented AFSJ data exchange therefore undoubtedly interferes with article 8 ECHR.

After the interference has been established, the ECtHR examines whether the measure in question may be justified. In this context, one has to consider three conditions: the act in question must be "in accordance with the law", pursue one of the legitimate aims listed in article 8 (2) ECHR and must additionally be necessary in a democratic society, which means principally that the interfering law must be proportionate to the aim pursued. Whereby 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 and to predict the consequences a given action might entail.[20]

---

[16] Compare for instance: ECtHR, *Leander v. Sweden*, Application no. 9248/81 from 26 March 1987; ECtHR, *Amann v. Switzerland*, Application no. 27798/95 from 16 February 2000; ECtHR, *Rotaru against Romania*, Application no. 28341/95 from 4 May 2000; ECtHR, *Panteleyenko v. Ukraine*, Application no. 11901/02 from 29 June 2006; ECtHR, *S. and Marper v the United Kingdom*, Application nos. 30562/04 and 30566/04 from 4 December 2008; ECtHR *Weber and Saravia v. Germany*, Application no. 54934/00 Admissibility Decision from 29 June 2006; ECtHR, *C.G. and others v. Bulgaria*, Application no. 1365/07 from 24 April 2008; ECtHR, *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, Application no. 62540/00 from 28 June 2007; ECtHR, *Malone v. the United Kingdom*, Application no. 8691/79 from 2 August 1984; ECtHR, *Valenzuela v. Spain*, Application no. 27671/95 from 30 July 1998.

[17] ECtHR, *Z. v Finland*, Application no. 22009/93, from 25 February 1997, para 95; ECtHR, *Peck v. United Kingdom*, Application no. 44647/98 from 28 January 2003, para 78; ECtHR, *L.L. v France* Application no. 7508/02 from 10 October 2006, para 43; ECtHR, *Biriuk v Lithuania*, Application no. 23373/03 from 25 November 2008, para 39; ECtHR, *I v Finland* Application no. 20511/03 from 17 July 2008, para 38; ECtHR, *S. and Marper v the United Kingdom*, Application nos. 30562/04 and 30566/04 from 4 December 2008, para 103; ECtHR, *C.C. v. Spain*, Application no. 1425/06 from 6 October 2009, para 31.

[18] ECtHR, *Amann v. Switzerland*, Application no. 27798/95 from 16 February 2000, paras 65–67.

[19] ECtHR, *Weber and Saravia v. Germany*, Application no. 54934/00 Admissibility Decision from 29 June 2006, para 79.

[20] ECtHR, *Sunday Times v. the United Kingdom*, Application no. 6538/74, para 49 from 26 April 1979; ECtHR, *Liberty and others v. the United Kingdom*, Application no. 58234/00 from 1 July

To be more precise, in judgments related to governmental data collection and the implementation of surveillance measures in the framework of article 8 ECHR, certain criteria must be fulfilled to guarantee proportionality and in this way the balance of powers 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 the processing.[21] 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.[22]

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).[23] Independent review and adequate and effective safeguards against abuse, including effective remedies, must exist to assure compliance with the rule of law.[24]

With regard to the subsequent notification of individuals subjected 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.[25] In the case *Weber and Saravia v. Germany*, the Strasbourg Court adds: "As soon as notification can be carried out without jeopardizing the purpose of the restriction after the termination of the surveillance measure, [. . .], information should be provided to the persons concerned".[26]

2008, para 68; ECtHR *Silver v. the United Kingdom*, Application no. 5947/72 and others from 25 March 1983, paras 85–88.

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

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

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

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

[25] ECtHR, *Weber and Saravia v. Germany*, Application no. 54934/00 Admissibility Decision from 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".

[26] ECtHR, *Weber and Saravia v. Germany*, Application no. 54934/00 Admissibility Decision, para 135 from 29 June 2006.

8.2.3 Data Protection After Lisbon

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 "European Community" actions and "European Union" activities, a development, which will largely influence data protection policy in the AFSJ.

The protection of personal data in the AFSJ is strengthened in three ways: its Article 16 (TFEU) guarantees the right to the protection of personal data to "everyone" and Article 6(3) TEU stipulates that the Charter of Fundamental Rights, which shall have the same legal value as the EU treaties, is additionally applicable when it comes to fundamental rights protection in the EU.[27] Its Article 8 includes the right to the protection of personal data. Important improvements are additionally offered by the intended accession of the EU to the ECHR provided for in Article 6(2) TEU. Particular attention is thereby paid to the ECtHR's interpretation of article 8 ECHR, mentioned above. Improved decision making by the introduction of the ordinary legislative procedure in the AFSJ, where Parliament and Council act as co-legislators[28] in data protection matters, upgrades democratic control. Although transitional provisions delay the effects of the full enforcement of Article 16 TFEU in the AFSJ (Hijmans and Scirocco 2009)[29], the exclusive competence of the Council vanishes and the Parliament has co-decision rights in every question concerning the necessary changes in the legal frameworks of the AFSJ actors.[30] With a view to this fundamental change in the upcoming legislative processes, it is important to propose

[27] Article 6 (3) TFEU.

[28] 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, additionally the Council's acting by a qualified majority in the legislative process.

[29] For an excellent overview of the situation of data protection after the Lisbon Treaty, see: Hijmans and Scirocco (2009). Article 9 of the Protocol No. 36 annexed to the Lisbon Treaty 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*. 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. 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 ECJ under Title VI of the former TEU shall remain the same. 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. Declaration 20 and 21 provide for the possibility to enact other data protection rules in the ASFJ than those being possibly applicable to former first pillar matters as regards national security as well as in police and judicial cooperation. Moreover, certain Member States (United Kingdom, Ireland, Denmark) complicatedly exclude the application of Article 16 TFEU in specific cases.

[30] 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" (Article 16 (2) TFEU).

improvement in terms of data protection in the AFSJ, which could then be used by the parliament in future negotiations.

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 principles for security-related data processing, could support this process in a valuable way. However, before proposing improvements, it is important to describe the organisation of the AFSJ data exchange and its shortcomings.

8.3 Organisation of AFSJ Data-Exchange

Information exchange in the AFSJ is on the one hand taking place between the AFSJ agencies (Europol, Eurojust, Frontex) and the Commission's anti-fraud unit OLAF[31] (para 2.1) and on the other hand the law enforcement and the judicial agency, Europol and Eurojust, have access to the information systems such as SIS, CIS, VIS and/or Eurodac[32] (para 2.2). In view of the data protection rules described in the first part, this section not only analyses the organisational structure of AFSJ data exchange, but also criticises the legal shortcomings arising in the current exchange network(s).

8.3.1 Inter-Agency AFSJ Data Exchange and OLAF

Inter-agency data exchange is carried out in two situations: data are exchanged during Joint Investigation Teams (JITs) operations or transferred between the actors based on bilateral agreements.

8.3.1.1 Information Exchange in JITs: Europol, Eurojust and OLAF

The idea of JITs was introduced in 2000 by the Convention on Mutual Assistance in Criminal Matters and later reaffirmed by a Framework Decision on JITs.[33]

---

[31] Europol and Eurojust are Europe's law enforcement agencies, which collect personal data of criminals, but also of suspects, victims and witnesses. Frontex assures the control of the external borders of the EU and collects data of third state nationals trying to pass the border. OLAF is the Commission's anti-fraud unit carrying out internal investigations within the EU institutions, bodies and agencies. The unit mainly collects personal data of individuals suspected of fraud.

[32] The SIS is a database in the framework of law enforcement and immigration control, which contains data of third state nationals, but also EU nationals. The CIS serves customs control purposes and contains personal data of individuals suspected of illicit trafficking activities. The VIS serves the purpose of the exchange of visa data and entails information of third state nationals who apply for a visa to enter the EU. Eurodac stores fingerprint data of asylum seekers and should prevent that asylum seekers make multiple asylum applications in different Member States of the EU.

[33] Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the

Legal Concept

The concept of JITs involves the "coordination, organisation and implementation of investigative and operational action carried out jointly with the Member States' competent authorities [. . .]".[34] In recent years, Europol's and Eurojust's main responsibilities relating to JITs were rather of organising and supportive nature[35], acting on basis of their establishing Council Decisions.[36]

However, the role of both agencies in JITs continually evolved in the last years.[37] Europol's, Eurojust's as well as OLAF's current function in JITs is described in a JITs Manual from 23 September 2009 (JIT manual). According to it, only Eurojust's national members acting on the basis of their national law can be a member of the JIT, officials from Europol, Eurojust and OLAF may participate but are not allowed to be a member of the JIT (Lopes da Mota 2009).[38] Article 6 Europol Decision and the JIT manual restrict their function to the involvement in the operation of the JIT, but exclude the participation in any coercive measures.[39] These general rules may be, however, subject to further specific arrangements in forming a particular agreement between the participating Member States and the bodies concerned annexed to

European Union, OJ 2000 C 197/1, Article 13; to the initiation of the JIT project, see: Horvatis and Bart De Buck (2007) and Rijken and Vermeulen (2006).

[34] Article 88 (2) (b) TFEU.

[35] Compare recital 9 and Articles 5 (1) (d), 5 (5), 6, 8 (7) c and 54 Council Decision of 6 April 2009 establishing the European Police Office, OJ 2009, L121/37 as well as Articles 6 (b) (iv), 9 (f), 12 (2) (d), 13 (2) (5) and 25 (a) (2) Eurojust Decision.

[36] Article 6 Europol Decision and Article 7 (4) Eurojust Decision.

[37] The Framework Decision on JITs (Article 1 and recital (9) of Council Framework Decision of 13 June 2002 on JITs, OJ 2002 L 162/1 and Article 13 Council Act of 29 May 2000 establishing in accordance with Article 34 Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ 2000, C 197/1) specifies that two or more Member States can set up a JIT for a specific purpose and a limited period of time to carry out investigations while Eurojust and Europol may participate in the JITs. For this purpose, participating Member States conclude mutual agreements and Europol and Eurojust organise information events and publish manuals on the concept of JITs. In their aforementioned joint JIT manual from 2009, both agencies encourage Member States to set up JITs to better coordinate cases involving several Member States. A JIT consists of law enforcement officers, prosecutors, judges or other law enforcement-related personnel and is established in the Member State in which investigations are supposed to be principally carried out. Other European Union bodies, particularly the Commission (OLAF) as well as law enforcement bodies from third states such as the FBI may additionally be involved, however, just as Europol and Eurojust, they may participate in the operation of a JIT, although they cannot lead or be a member of it. They are associated by an agreement between the agency/administration of a Member State as a party to the agreement and the relevant European Union or third state body; compare: Explanatory report on the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ 2000, C 379/7 and JITs Manual from 23 September 2009, Council Doc. 13598/09.

[38] JITs Manual from 23 September 2009, Council Doc. 13598/09, p. 10 and Eurojust Decision, Article 9 (f).

[39] JITs Manual from 23 September 2009, Council Doc. 13598/09, p. 10, see also: Article 6 (1) Council Decision of 6 April 2009 establishing the European Police Office, OJ 2009, L121/37.

the initial agreement setting up the JIT, which may confer more rights to Europol, Eurojust or OLAF.[40]

Considering the formulations in the JIT manual, in practice it seems to be hard to distinguish between the "participation in the operation of the JIT" on the one hand and the exclusion of coercive measures on the other, in particular when taking Article 6(2) Europol Decision into account, which stipulates that Europol staff should "assist in *all* activities and exchange information with all the members" of the JIT (De Buck 2007).[41]

Information Exchange in JITs

Rules on information exchange in the JITs follow a local solution and are generally attached to the national law[42] and stipulate that information could be shared within the limits of the national law of the national members seconded to the JIT.[43]

Further details regarding the exchange of information and data protection issues are entailed in the specific arrangements of the agreements setting up the JIT[44], but the specifics of these arrangements are not published and depend on the agreed compromise between the Member State and the relevant European actor in a particular case. Rules of general application regulating this nevertheless rather informal data exchange do not exist, but would definitely lead to more legal certainty and transparency in this context (Rijken and Vermeulen 2006; Mitsilegas 2009).[45]

Despite this rather non-transparent practice, Europol's role in JITs is of great importance: it may provide the JIT members with information stemming from its databases (the EIS or from an analysis work file).[46] Europol can grant access to both systems "by means of a Europol mobile office located where the JIT is operating" (De Buck 2007). JIT members are allowed to have direct access to Europol's information systems, which enables them to have access to information of Member States, which

---

[40] JITs Manual from 23 September 2009, Council Doc. 13598/09, pp. 26 and 27 suggesting a model agreement for the participation of Europol, Eurojust or OLAF.

[41] Emphasis added, Article 6 (1) Council Decision of 6 April 2009 establishing the European Police Office, OJ 2009, L121/37, with regard to this problem, see: De Buck (2007).

[42] They are vaguely mentioned in Article 6 (4) and (5) Europol Decision and Article 13 (9) and (10) Convention on Mutual Assistance in Criminal Matters as well as Article 1 (9) and (10) Framework Decision on JITs (which literally repeats the aforementioned Articles of the Convention).

[43] Usually, the use of this information is restricted to the purpose for which the JIT has been set up and subject to the prior consent of the Member State where the information became available. Information can further be used for preventing an immediate and serious threat to public security and if subsequently a criminal investigation is opened as well as for other purposes to the extent that this is agreed between Member States setting up the team, Article 1 (10) (a)—(d) of Council Framework Decision of 13 June 2002 on JITs, OJ 2002 L 162/1.

[44] See example of a model agreement in: JITs Manual from 23 September 2009, Council Doc. 13598/09, p. 24.

[45] To this problem, see: Rijken and Vermeulen (2006); Mitsilegas (2009).

[46] Council Decision of 6 April 2009 establishing the European Police Office, OJ 2009, L121/37, Article 6 (4).

do not participate in the JIT or to information of third States cooperating with Europol (De Buck 2007).[47] When a Europol staff member during its participation in a JIT obtains information, he can include the information in Europol's data processing systems, after having obtained the prior consent of the relevant Member State.[48]

The active participation of Europol at the information exchange in the JIT nevertheless risks conflicting with the aforementioned local approach chosen in the JIT cooperation when considering that the information could only be shared within the boundaries of the national law of the national members seconded to the JIT. As a result, different domestic rules on data exchange and data protection may conflict with each other and additionally with the Europol rules, which could finally lead to a considerable lack of legal certainty.

Whereas the Europol Decision entails rules allowing for the exchange between its data processing systems and the JITs, Eurojust's or OLAF's data exchange with the JITs is not regulated. Although, for instance, Article 7(a) (iv) Eurojust Decision reinforces Eurojust's participation in JITs and clearly speaks of a participation of Eurojust's officials in JIT operations (Lopes da Mota 2009; Vervaele 2008)[49], information exchange or data protection rules in this regard are missing. The redraft of the Eurojust Decision in 2009 could have closed this regulatory gap, but either it was not detected or intentionally not regulated (Gusy 2008).[50] Rules comparable to the Europol Decision, which clarify the transfer of data between Eurojust and the JITs as well as the specifics of the information entered in the Case Management System are necessary to regulate this specific problem.

Moreover, OLAF's various legal bases do not even give an indication of its inclusion in JITs.[51] While OLAF officials proceed on the assumption that the second

[47] Information from third States can be obtained by using the so-called Virtual Private Network (VPN) connecting Europol's national units and offering encrypted lines with third States, see: De Buck (2007). Compare Council Decision of 6 April 2009 establishing the European Police Office, OJ 2009, L121/37, Article 6 (4) and (5).

[48] Compare Council Decision of 6 April 2009 establishing the European Police Office, OJ 2009, L121/37, Article 6 (4) and (5).

[49] JITs Manual from 23 September 2009, Council Doc. 13598/09, p. 10. It is worth mentioning that Eurojust's function is not any longer restricted to a mere "interface" between national authorities, limited to horizontal cooperation given that the Eurojust Decision 2009 visibly extended its operational tasks and Eurojust's role in JITs. For instance, Eurojust's national members are allowed to participate in JITs and the Secretariat of the JIT Experts Network shall form part of the Eurojust's staff, compare: Lopes da Mota (2009) and Vervaele (2008).

[50] It seems also possible that information obtained in course of JITs is entered by the Eurojust's national Members acting on the basis of national law and not by Eurojust officials in Eurojust's Case Management System. This possibility would also lead to a non-regulated transfer of data from the Case Management System to the other JIT members considering that national law does not apply in this rather European context. In addition, if only Eurojust's national members supply Case Management Information to the JIT or information stemming from Eurojust's own analysis, the questions of information transfer from Eurojust's Case Management System to the JIT through a member acting on behalf of Eurojust involved in the JIT is left unanswered, compare to the general data protection problems arising out of JITs: Gusy (2008).

[51] Compare Commission Decision 1999/352/EC of 28 April 1999 establishing the European Anti-Fraud Office (OLAF) OJ 1999 L136/20 and Regulation (EC) No. 1073/1999 of the European

protocol from 1999 to the Convention on the protection of the EC's financial interests[52]—broadly dealing with the cooperation between the Member states and the Commission in fraud-related matters, active and passive corruption and money laundering—taken together with the Convention on Mutual assistance in Criminal Matters enables OLAF to participate in JITs (De Moor 2009; Ralf 2009), none of these instruments explicitly refers to this sensitive subject matter. On the contrary, OLAF is not even mentioned.[53]

Keeping in mind Europol's extensive data exchange possibilities in the JITs, particularly the inclusion of information obtained in the JIT framework in its databases and vice versa, OLAF participation in JITs in absence of a clear legal basis, is legally doubtful.

Therefore, OLAF's role within the JIT structure certainly has to be clarified. In this context, special attention has to be paid to the fact that the cooperation of these two bodies is so far based on an agreement not allowing for personal data exchange (see Sect. 8.3.1.2). The participation of OLAF and Europol in common JITs unavoidably leads to personal data exchange and would therefore contradict OLAF's existing legal bases as well as the cooperation agreement between Europol and OLAF, discussed hereafter.

The question of joint participation in JITs of Eurojust and OLAF is, however, integrated in their cooperation agreement (analysed in Sect. 8.3.1.2).[54] However, details regarding the JITs cooperation, including the applicable data protection rules, are subject to the JIT agreement concluded between the participating parties.

8.3.1.2 Agreements Providing for Mutual Information Exchange

In addition to the cooperation in JITs, information exchange between the AFSJ actors is provided for in the agreement concluded between the relevant parties.

Parliament and the Council of 25 May 1999 concerning investigation conducted by the European Anti-Fraud Office (OLAF), OJ 1999 L136/31; Article 2 (6) Commission Decision 199/352 broadly regulates that "the office shall be in direct contact with the police and judicial authorities" and Article 1 (2) Regulation 1073/1999 only refers to "assistance" from the Commission to the Member States in organising close cooperation between the competent authorities of the Member States.

[52] Second Protocol, drawn up on the basis of Article K.3 of the treaty on European Union, to the Convention on the protection of the European Communities' financial interests—Joint Declaration on Article 13 (2)—Commission Declaration on Article 7, OJ 1997, C-221/12.

[53] Indeed, the Convention provides for "operational assistance" including exchange of personal data in fraud-related offences between the Commission and the Member States, but it does not specify at all the instruments to be used in this context.

[54] If one party is associated to a JIT related to fraud, corruption or criminal offences affecting the EU's financial interest, it shall inform the other party about its participation and propose the Member States setting up the JIT to consider inviting the other party, Practical Agreement on arrangements of cooperation between Eurojust and OLAF from 24 September 2008, point 9 (1).

Europol-Eurojust

The new Europol-Eurojust Agreement from January 2010[55] mainly regulates Eurojust participation at Europol's analysis work files, which is a new development linking the legal framework of the two bodies, hence affecting data protection questions related to the opening of the files to another agency. Problems regarding the accountability of processing as well as the supervision of it might arise.[56]

The agreement stipulates that both, Europol as well as Eurojust, shall "of its own motion" or upon request, provide each other with analysis results including interim analysis results.[57] When the information communicated matches the information stored in the respective processing systems, Europol or Eurojust shall additionally provide each other with data linked to the information provided.[58] This evidently leads to merging of the data yet stored separately either in the Europol or in the Eurojust databases. Article 8(3) Europol-Eurojust Agreement further provides for a regularly transmission of relevant data stored at Eurojust for the purpose of using them in Europol's analysis work files. The same applies to other information, in particular to information on cases provided that they fall within Europol's competence.[59] It is worth mentioning here that both actors are principally competent to deal with the same criminal offences.[60]

In addition to the exchange of information as regards the analysis work files, there is a further profound and important change as regards Eurojust's possibilities to play a part in Europol's analysis work files.

Whereby direct access by Eurojust to Europol's analysis work files was excluded under the former cooperation agreement from 2004, according to the new Europol-Eurojust Agreement, Eurojust has the right to take the initiative to open an analysis work file or even to establish a target group, if Eurojust is associated with the analysis work file concerned.[61]

---

[55] Agreement between Europol and Eurojust, which entered into force the 1 January 2010, Articles 7 (2) and 8 (2), in the following Europol-Eurojust Agreement; this Agreement replaced the Agreement between Europol and Eurojust from 9 June 2004.

[56] The EDPS in its opinion to the amendment of the Eurojust Decision rightly points to the questions of "who will be the processor?" and "who will be the controller?" within this new collaboration structure. Details to these questions are unfortunately not regulated in the Agreement as it indeed provides for the mutual association, but it does neither clarify questions of supervision in case of Eurojust's participation in Europol's analysis work files, nor regarding the transmission of personal data, compare: EDPS opinion on the Council Decision concerning the strengthening of Eurojust and amending Decision 2002/187/JHA from 5 December 2008, OJ 2008, C 310/1, p. 6, para 34.

[57] Articles 7 and 8 Europol-Eurojust Agreement.

[58] Articles 7 (2) and 8 (2) Europol-Eurojust Agreement.

[59] Article 8 (3) Europol-Eurojust Agreement.

[60] Eurojust's mandate refers to list of crimes for which Europol is responsible and which is laid down in Article 3 Europol Decision, compare Article 4 (1) Eurojust Decision.

[61] Article 9 (2) Europol-Eurojust Agreement. Article 11 (1) and (2) of the Europol-Eurojust Agreement 2010 clarifies that: Europol shall associate experts of Eurojust to participate within the activities of Europol's analysis work files, in particular when Eurojust initiated the opening of the respective file. Eurojust may also request to be associated with the activities of a particular analysis group.

The participation of Eurojust in the activities of an analysis work file and an analysis group at Europol is, however, astonishing, in particular with regard to Article 14(2) Europol Decision whereupon the access to analysis work files is strictly restricted to analyst, designated Europol staff, liaison officers or experts from the Member States. This Article moreover provides that only analysts are authorised to enter data into the file and modify such data. Taking into account that Article 13 Europol-Eurojust Agreement stipulates that the transmission shall be in accordance with the establishing act of the parties and additionally considering the enormous variety (information about criminals, victims, witnesses, contacts, etc.) as well as amount of personal data (up to 69 data elements), which can be stored in Europol's analysis work files, each widening of the circle of persons having access to the relevant information should be accompanied with additional safeguards against abuse as well as effective tools of supervision (compare ECtHR case *Weber and Saravia v. Germany*[62]).

It is worth noting that the Europol-Eurojust Agreement, however, lays down access as well as correction and deletion rights.[63] Disappointingly, although the participation of Eurojust at Europol's work files was newly introduced in the 2010 agreement, the data protection provisions introduced in the former 2004 agreement, were not adapted to the new circumstances. Rules requiring information of witnesses, victims or persons requesting access about the transfer of their data as well as rules relating to the information of Europol's or Eurojust's Joint Supervisory Body (JSB) about the transfer, are missing. Provisions regulating the competence for access request once Eurojust's data are included in Europol's analysis work files are additionally not provided for in the agreement, not to mention provisions relating to the supervision of the data generated in this way.

All in all, Eurojust's participation at Europol's analysis work files demands further protections for individuals, in particular regarding the rights of victims or witnesses to know whether and to whom their data are transferred. The JSB and the data protection officers of both agencies should be informed in any case to guarantee at least a minimum supervision. In addition, when taking the enormous amount of

[62] The transmission of personal data to other authorities was only allowed when it was particularly supervised and restricted to the transmission of data arousing the suspicion that specific facts, as opposed to mere factual indications, pointing to the fact that this person has committed a crime, compare: *Weber and Saravia v. Germany*, Application no. 54934/00 Admissibility Decision, paras 42–43 and 123–129 from 29 June 2006; Article 14 (4) Europol-Eurojust Agreement, however, lays down that the transmission of data revealing racial origin, political opinions or religious or other beliefs, or concerning health and sexual life shall be restricted to absolutely necessary cases and that such data shall only be transmitted in addition to other data.

[63] According to Article 18 (3) Europol-Eurojust Agreement, transmitted data shall be deleted when they are no longer necessary for the purpose for which they were transferred or when they are not necessary for the tasks of the receiving party or when no decision has been taken within 3 months after receipt (Article 16 (4)); a retention review must take place within the first 3 years of storage and when the storage exceeds 3 years, an annual review has to be implemented, see Article 18 (5) Europol-Eurojust Agreement.

data into account with which both agencies are dealing[64], it is worth considering the establishment of an independent authority only for the purpose of monitoring the data transfer between them.

Europol-OLAF Cooperation

Europol's and OLAF's cooperation is based on an administrative agreement restricted to the exchange of strategic information signed in 2004.[65] Currently, negotiations are taking place discussing an administrative arrangement similar to that concluded with Eurojust, which allows for personal data exchange.[66]

However, it is worth noting that, after the entry into force of the new Europol Decision on 1 January 2010, Article 22(3) Europol Decision permits Europol to directly receive, use and transmit information, including personal data from OLAF even prior to the conclusion of a formal exchange agreement "in so far as it is necessary for the legitimate performance of Europol's or OLAF's tasks". In case the transmitted data were originally introduced by a Member State, Europol has to ask the Member State for prior consent.[67]

Taking into account the different existing provisions, on the one hand, a valid agreement not allowing for personal data exchange and on the other, the rules stipulated in the Europol Decision, the legal basis for personal data exchange between OLAF and Europol is far from being clear. Theoretically, according to its legal basis, Europol could transmit and receive personal data stored in OLAF's databases, although it has to be taken into account that OLAF's legal framework lags considerably behind. Apart from the fact that data processing must be generally in accordance with the provisions of Regulation 45/2001[68], none of OLAFs legal bases include transfer provisions regulating the personal data exchange with EU agencies such as Europol.[69]

---

[64] Eurojust registered 1,372 new cases in 2009, compare Eurojust annual report 2009, p. 50 and Europol had 88,419 objects stored in the EIS and initiated 8,377 cases in 2008, compare Europol annual report 2008, pp. 33–35.

[65] Administrative Arrangement between the European Police Office (Europol) and the European Anti-Fraud Office (OLAF) from 8 April 2004, accessed July 12, 2011, https://www.europol.europa.eu/sites/default/files/flags/european_anti-fraud_office_olaf_.pdf.

[66] OLAF annual report 2009, ninth activity report for the period 1 January 2008–31 December 2008, section 4.6.2, p. 59.

[67] Article 24 (1) Europol Decision.

[68] Regulation 45/2001 is restricted in scope and refers only to personal data transfer between Community bodies, which represent bodies established under the former first pillar and does not include Europol or Eurojust.

[69] Regrettably, neither Commission Decision 1999/352/EC establishing OLAF nor Regulation 1073/1999 includes transfer provisions regulating the personal data exchange with third states or agencies such as Europol. Article 10 Regulation 1073/1999 refers to the forwarding obtained in course of internal investigations to the bodies, offices and agencies concerned by the investigation, however, this provision does not take the data exchange in the framework of criminal or judicial cooperation into account. Rules on the transfer to agencies are nowhere to be found in OLAF's instruments.

Europol-Frontex

Frontex and Europol cooperate based on a "strategic agreement" concluded in 2008.[70] The agreement is limited to the exchange of strategic and technical information[71] prohibiting the exchange of personal data, more precisely the transfer of "data related to an identified individual".[72]

Astonishing, however, are the provisions regulating the exchange of information. They are remarkably detailed and seem rather to make sense when personal data shall be exchanged.[73]

Such specified provisions are exceptional and not included in similar strategic agreements Europol has concluded with other EU bodies.[74] The existence of such provisions casts doubts on the complete exclusion of personal data exchange from the cooperation between the two actors.

In addition, the agreement's exclusion of personal data exchange seems to be rather obsolete, yet disconnected to a great extent from Europol's and Frontex's cooperation in reality, also in the light of Europol's new Council decision, which provides for personal data exchange even in absence of an agreement allowing for the latter.[75]

The mysterious wording of the agreement seems, however, to make sense when taking the practical cooperation between the Europol and Frontex into account: a

---

[70] Strategic cooperation agreement between the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union and the European Police Office from 28 March 2008; in the following: Europol-Frontex Agreement from 28 March 2008.

[71] According to Article 2 Europol-Frontex Agreement: 1. "Strategic information" includes, but is not limited to: (a) enforcement actions that might be useful to suppress offences and improve the integrated border management of the Member States of the European Union; (b) new methods used in committing offences, in particular, those threatening the security of external borders or facilitating illegal immigration; (c) trends and developments in the methods used to commit offences; (d) observations and findings resulting from the successful application of new enforcement aids and techniques; (e) routes and changes in routes used by smugglers, illegal immigrants or those involved in illicit trafficking offences covered by this agreement; (f) prevention strategies and methods for management to select law enforcement priorities and (g) threat assessments, risk analysis and crime situation reports. 2. "Technical information" includes, but is not limited to: (a) means of strengthening administrative and enforcement structures in the fields covered by this agreement; (b) police working methods as well as investigative procedures and results; (c) methods of training the officials concerned; (d) criminal intelligence analytical methods and (e) identification of law enforcement expertise.

[72] Article 1 Europol-Frontex Agreement from 28 March 2008.

[73] For instance: conditions on the further use and transfer of the transmitted information may be imposed on the receiving party, just as Europol shall only supply information to Frontex ", which was collected, stored and transmitted in accordance with the relevant provisions of the Europol Convention and its implementing regulations" though the latter apparently deals with personal data. Compare: Article 5 para 3 et 8 Europol-Frontex agreement.

[74] For instance with: the Central Bank, Commission, Monitoring Centre for Drugs and Drug Addiction, OLAF.

[75] Pursuant to its Article 22 (3).

House of Lords report reveals that Europol has worked "informally" with Frontex since 2006.[76] An external report evaluating Frontex's work and published on Frontex's webpage sheds light on this issue and discloses further problems. According to the report, Frontex collects data in the framework of joint operations in order to send them to other agencies, such as Europol for threat analysis (Holzenberger 2006).[77] Pursuant to the report, 10% of the detained persons during a joint operation are interviewed by Frontex staff[78], which finally means that Frontex itself also collects personal data notwithstanding its restrictive legal framework at present, which does not allow for personal data processing. Consequently, Frontex acts in absence of a legal basis allowing for the collection and processing as well as the transfer of personal data.[79]

Above, we have seen two important facts relating to data processing at Frontex: while neither the Frontex Regulation 2007/2004 nor the Europol-Frontex agreement permit personal data processing or transfer, the reality seems to tell another story. The exchange and in particular Frontex's collection of personal data is neither covered by the Europol-Frontex agreement, nor by Frontex's current legal basis.

For this reason, clarifications in Frontex's legal framework were long overdue and have resulted in 2010 in the Commission's and the Council's Frontex proposal to amend the Frontex regulation 2007/2004[80] by, amongst others, now including two important changes concerning the question of data processing at Frontex: on

---

[76] House of Lords Europol report, European Union Committee, 29th report of session 2007–2008, "Europol: coordinating the fight against serious and organised crime", published 12 November 2008, p. 80.

[77] Final report of COWI (European consulting group) from January 2009 preparing an external evaluation of Frontex provided for in Article 33 of the Council Regulation (EC) No. 2007/2004 of 26 October 2004 establishing Frontex, p. 48, accessed July 12, 2011, http://www.frontex.europa.eu/specific_documents/other/, joint operations are described as a "good example of integrated analyses by Europol and Frontex" and are regarded as a working practice in which intelligence and operations are brought together as closely as possible". To the details of the cooperation between Europol and Frontex.

[78] Final report of COWI (European consulting group) from January 2009 preparing an external evaluation of Frontex provided for in Article 33 of the Council Regulation (EC) No. 2007/2004 of 26 October 2004 establishing Frontex, p. 48, accessed July 12, 2011, http://www.frontex.europa.eu/specific_documents/other/.

[79] The proposal to amend the Frontex regulation should eventually put this exchange on a legal basis. Nevertheless, even if the proposal enters into force, personal data exchange with Europol or other Union agencies or bodies would generally require the conclusion of a new cooperation agreement. Compare: Proposal for a Regulation of the European Parliament and the Council amending Council Regulation (EC) No. 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX) from 24 February 2010, COM (2010) 61 final.

[80] Proposal for a Regulation of the European Parliament and the Council amending Council Regulation (EC) No. 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX) from 24 February 2010, COM (2010) 61 final and Council document 2010/0039 (COD), 8121/10, proposal for a regulation of the European Parliament and the Council amending Council Regulation (EC) No. 2007/2004 establishing a European Agency for the Management

the one hand, the Frontex proposal allows to collect, process and exchange personal data concerning the detection of criminal networks organising illegal immigration[81] and on the other hand, it supports the use and the possibility of carrying out risks analysis.[82]

While on the one hand the widening of Frontex's mandate in this regard would connect two not directly linked remits (border control and serious crime prevention), on the other hand, the possibility to carry out risks analysis would considerably overlap with Europol's mandate. Regrettably, the proposal does neither specify the details of data processing at Frontex nor the cooperation with EU agencies. Individual rights, such as data protection rights, are not (yet) included in the proposal.[83] According to recent developments, provisions on the cooperation with Europol as well as on data protection issues should be added to the Frontex proposal.[84] However the details of these provisions are not yet published.[85]

Moreover, it is very important that, in contrast to Europol, Frontex's mandate does not (and will not) cover the collection of data related to serious crime or organised immigration crime, which means that the data of Europol and Frontex are definitely not collected for the same purpose. The possible exchange of the data could eventually lead to the connection of data of potential immigrants with data included in Europol's databases, the latter dealing for the most part with data related to persons associated to crimes. Linking these two subjects while disregarding any distinction between data of criminals and data of (possible) immigrants, contravenes the purpose limitation principle and blurs the border between criminals and immigrants. Clear rules respecting the protection of personal data of the individuals concerned in

---

of operational cooperation at the external borders of the Member States of the European Union (Frontex) 29 March 2010.

[81] Proposal for a Regulation of the European Parliament and the Council amending Council Regulation (EC) No. 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX) from 24 February 2010, COM (2010) 61 final, Article 2; Eurosur is the planned European Border Surveillance System, for more details, see: Commission staff working paper, report on progress made in developing the European Border Surveillance System (EUROSUR) from 24 September 2009, Sec (2009), 1265 final and analysis of the Commission communications on future development of Frontex and the creation of a EUROSUR, briefing paper from policy department C, citizens' rights and constitutional affairs, civil liberties, justice and home affairs, Directorate General internal policies of the Union from June 2008.

[82] Impact assessment accompanying the proposal for a Regulation of the European Parliament and the Council amending Council Regulation (EC) No. 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX) from 24 February 2010, p. 34.

[83] Compare for more details: opinion of the European Data Protection Supervisor (EDPS) on the proposal for a Regulation of the European Parliament and the Council amending Council Regulation (EC) No. 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX) from 17 May 2010.

[84] Compare press release 11916/11, Presse 192 from 23 June 2011, accessed July 12, 2011, http://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/en/jha/122983.pdf.

[85] Last verified on 30 June 2011.

the Frontex proposal would help to prevent the criminalisation of this specific group and should accompany the Council's and the Commission's ambitions to extend Frontex's possibilities to exchange data.

Eurojust-OLAF Cooperation

The practical agreement on arrangements of cooperation between Eurojust and OLAF from 2008 provides for the collaboration in operational and strategic meetings as well as the exchange of information including personal data in specific cases.[86] Restrictions, the conditions on the use of the data or the time of storage of the transmitted data are regrettably not given.

Individual rights are not directly mentioned, although OLAF's data processing must usually comply with Regulation 45/2001. The misleading title "rights of data subjects" of point 14 of the agreement only reveals a consultation duty for the requested party towards the other party before deciding about a request by an individual to have access to, to demand correction, blocking or deletion of its personal data transmitted under the agreement.[87] Apart from that provision, the agreement makes reference to the relevant data protection rights of the parties.

However, the mere reference to the applicable rules of the parties does not automatically assure compliance with them. Considering that the motivation to exchange personal data represents one of the main reasons for the amendment of first cooperation agreement from 2003, additional safeguards taking into account the specific risks of data transfer would have illustrated the "good will" of the parties to acknowledge the importance of data protection rights in this context. The indication of an authority exercising, for example, independent supervision of the agreement would have, for instance, emphasised the submission under an efficient data protection regime.[88]

A further important point concerns the different time limit of storage—20 years at OLAF and as long as it is necessary at Eurojust—which is not taken into account by the text of the agreement. Questions relating to restrictions and the conditions on the use of OLAF's data in Eurojust's Case Management System arise.[89]

---

[86] Practical Agreement on arrangements of cooperation between Eurojust and OLAF from 24 September 2008, point 6.

[87] Practical Agreement on arrangements of cooperation between Eurojust and OLAF from 24 September 2008, point 14.

[88] Theoretically, the EDPS and possibly Eurojust's JSB are responsible for this task, it would not do any harm to the parties to mention them in the agreement. A particular problem in this context relates to the fact that the responsibility for personal data transfer from Eurojust to OLAF lies only with the national member and not with Eurojust, having for consequence that supervision is becoming increasingly difficult and can usually not be exercised by Eurojust's JSB.

[89] Mutual information duties apply and include the notification duty of the other party about corrections or deletions made, including the reasons therefore. In addition, regarding cases in which one of the parties assumes that information received is not accurate, not up to date or should not have been transmitted, the other party has to be warned. A further provision consists of the requirement to inform a third party, to which transmitted data have been transferred, about any deletions or

8.3.2 Europol's and Eurojust's Access to Information Systems

Personal data exchange is not only limited to AFSJ agencies, it is also taking place between European information systems and the AFSJ agencies. The information systems include the databases SIS (II), CIS, VIS and Eurodac. The increasing data exchange between the mentioned actors considerably enlarges the authorities and bodies having access to personal data originally entered in only one of the databases. Therefore, attention should be paid to the rather limited purpose for which the databases were established[90] and which is continually broadened when allowing various actors, not necessarily connected to this original purpose, to access. In the light of the foregoing considerations, it is therefore interesting to briefly analyse the relation and the data exchange possibilities in the framework of ASFJ agencies and European information systems in order to understand the data protection impact of the access from the AFSJ agencies to the mentioned databases.

8.3.2.1 Europol's and Eurojust's Access to the SIS II

Europol as well as Eurojust have access to the SIS (II).

Europol gained access to information relating to important categories of data contained in the SIS already in February 2005.[91] In the meanwhile, Europol's and Eurojust's tasks as well as the scope of the new SIS II have been evolved continually and the data entered in the respective databases are getting more and more extensive. Europol's tasks and functions remain nevertheless more comprehensive and the data processed in its databases entail much more elements than those stored in the SIS II.[92]

Despite the access, the Europol Decision does not directly mention the SIS II. Article 21 Europol Decision, however, permits wide-ranging access to data of Union databases to the extent "that is necessary for the performance of its tasks". The SIS II Decision 2007/533 mirrors this provision by stipulating that Europol and Eurojust have the right "within its mandate" to access and search data directly in the SIS II.[93]

---

corrections made concerning this data. Finally, the time limits of the storage bases on the respective rules of the parties, compare practical Agreement on arrangements of cooperation between Eurojust and OLAF from 24 September 2008, point 15.

[90] The SIS for security purposes with regard to EU as well as to third state nationals, CIS for customs control, VIS for the exchange of visa data and Eurodac for the exchange of fingerprint data of asylum seekers.

[91] Council Decision 2005/211/JHA of 24 February 2005 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism, OJ 2005 L-68/44, Article 1 referring to Articles 95, 99 and 100 Schengen Convention, OJ 2000, L-239/19 (persons wanted for extradition, persons or vehicles placed under surveillance or subjected to specific checks as well as to objects sought for the purpose of seizure or use in criminal proceedings).

[92] Up to 69 data elements can be, for instance, stored in an analysis work file at Europol.

[93] Articles, 41, 42 and 43 SIS II Decision 2007/533; the scope of the access relates to persons wanted for arrest or surrender purposes, persons and objects for discreet checks or specific checks

Whereas Europol's legal basis mentions the mandate of the access, *Eurojust's access* to other databases, is neither referred to in the new Eurojust Decision, nor in any of its predecessors. Only Article 42 SIS II Decision 2007/533 refers to the possibility of Eurojust's national Members, not including Eurojust staff, to access and search data in the SIS II.[94]

The absence of Eurojust's mandate is particularly striking when looking at the remarks of the House of Lords, already made in 2003, which clearly point to the lacking provisions allowing Eurojust's access.[95] The amendment of the Eurojust Decision in 2009 could have been an opportunity to define the conditions of Eurojust's access to the SIS II as well as the details regarding the use of the data. The non-inclusion of this topic in the instrument leaves strong doubts on the political will to concretely identify Eurojust's mandate regarding the SIS II data and opens the way for a non-regulated data use at Eurojust.

As regards the processing of the data, both agencies may use the SIS II data. The handling of the data is left to the respective legal bases of the accessing actors.[96] Questions relating to the inclusion of data from other information systems in Europol's or Eurojust's databases are left, however, unanswered. Neither the Europol or the Eurojust Decision nor the SIS II Decision 2007/533 provide for clarifications.[97]

Provisions relating to the protection of the information at Europol and Eurojust are limited.[98] Although both agencies must introduce a recording duty of every access and search made by them as well as a provision interdicting the connection, the transfer, the download and the copying of the SIS II data to another computer system for data collection and processing operated by or at Europol or Eurojust, they may introduce SIS II information in their own database (either, by asking the relevant Member State after a hit in the SIS II to introduce the same information in

---

as well as to objects for seizure or use as evidence in criminal proceedings Eurojust has additionally access to data of missing persons.

[94] Articles 42 (1) and (6) SIS II Decision 2007/533. This might be partially due to the fact that only national members of Eurojust can access the SIS II database, then integrating the data in the Eurojust system, but it does not explain why a reference is entirely lacking.

[95] "The only provision that enables Eurojust access to SIS data appears to be an unpublished non-legally binding declaration annexed to the Eurojust Decision (which we have asked to see but have never received)", compare: House of Lords, Select Committee on European Union Written Evidence Sub-Committee F (Social Affairs, Education and Home Affairs), letter from the Chairman to Bob Ainsworth, MP, Under-Secretary of State, Home Office, Schengen Information System: new functions, (9407/02 and 9408/02) from 9 April 2003.

[96] Article 41 (3) SIS II Decision 2007/533.

[97] Europol's legal basis, for instance, limits further clarifications to the simple provision that the legal instruments of the relevant partner databases shall govern Europol's use of the data as well as its access conditions, "in so far as they provide for stricter rules on access and use" than those of the Europol Decision. Compare Article 21 Council Decision of 6 April 2009 establishing the European Police Office, OJ 2009, L121/37.

[98] Articles 41 (5) and 42 (4), (5) and (7) SIS II Decision 2007/533.

the Europol or Eurojust database or by asking the Member State for consent to use the information in their own databases).[99]

This possibility also influences the following restrictions of Article 41(5) (c) and (d) SIS II Decision 2007/533 pursuant to which Europol must adopt security and confidentiality rules as well as limit access to data entered in the SIS II to specifically authorised staff. Even if the access is initially restricted to certain persons, which is generally a welcomed provision, if the data are later introduced by a Member State in Europol's databases EIS, the initially restricted access only exists on paper.

Article 41(3) SIS II Decision 2007/533 additionally provides for the possibility to transfer the obtained SIS II information to third states (Member State's consent provided), circumventing the initial restriction of Article 54 SIS II Decision 2007/533 whereupon SIS II data should not be made available to third countries.

8.3.2.2 Europol's Access to the VIS

Access to the VIS is limited to Europol. It is briefly mentioned in the VIS Regulation 767/2008 and further detailed in Council Decision 2008/633 concerning access for consultation of the VIS by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (VIS access Decision 2008/633).[100]

As in the case of the SIS II, Europol's access depends on its mandate restricted to "the performance of its tasks".[101]

Due to the influence exerted by the European Parliament during the negotiations[102] and compared to the SIS II instruments, the VIS access Decision 2008/633 requires a more sophisticated, if not necessarily always sufficient, data protection framework briefly analysed hereinafter.

As the VIS Regulation 767/2008 does not specify Europol's access conditions, VIS access Decision 2008/633 does not succeed in reaching comprehensive clarification in this regard either.

The purpose of Europol's access remains vague and generally refers to the purpose of prevention, detection and investigation of terrorist offences and of other serious

---

[99] Compare Article 41 (3) SIS II Decision 2007/533.

[100] Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the VIS by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, OJ 2008, L-218/129 (in the following: VIS access Decision 2008/633).

[101] Article 3 (1) VIS Regulation 767/2008, OJ 2008, L-218/60.

[102] The VIS access Decision 2008/633 entered into force in September 2008 and was not, contrary to VIS Regulation 767/2008, which is a former first pillar instrument, adopted by using the co-decision procedure, but formed part of the "VIS legislative package" agreed between the European Parliament and the Council in 2007 after two and a half years of negotiations. The reason therefore can be found in the legal basis of the instrument, which is governed by Title VI of the EU Treaty dealing with police and judicial cooperation in criminal matters, more specifically the Decision bases on Article 30 (1) (b) and 34 (2) (c) EU. Treaty; thus the Council alone could decide about the adoption of the instrument.

crime.[103] Article 7 VIS access Decision 2008/633 refers to the access for the purpose of the performance of Europol's tasks[104] as well as for analysis purposes according to Article 10 Europol Convention.[105]

Similar criticism as mentioned in the SIS II discussion applies also in the framework of the VIS. In both cases, access depends on a variable factor, namely the performance of Europol's tasks, which are subjected to modifications at any time. A good example is the last amendment of the Europol Convention, the Europol Decision entering into force in January 2010, which completely reversed Europol's legal framework and considerably enlarged its tasks.

A further important, although regrettable, aspect in context of the access of Europol to the VIS, is the fact that important requirements restricting the access conditions of national "designated authorities" do apply to Europol.[106] As a result, Europol's access is significantly wider than the access of the national authorities and does not require that the data are necessary for a specific case or that the consultation substantially contributes to the purpose of the access.[107]

In the light of the foregoing, it is interesting to note that both the Commission as well as the European Parliament stressed during the decisions' negotiations that a "routine access" of Europol should be prevented.[108]

---

[103] The offences are further detailed in two Framework Decisions, which list a range of different crimes, not always corresponding to those of the Europol Decision. Terrorist offences means the offences under national law corresponding or being equivalent to the offences listed in Article 1–4 Framework Decision 2002/475 on combating terrorism (OJ 2002, L-164/3) and serious criminal offences embraces the forms of crimes corresponding or being equivalent to those referred to in Article 2 (2) Framework Decision 2002/584 on the European Arrest Warrant (OJ 2002, L-190/1).

[104] Europol's tasks are described in Article 5 (1) (a) Europol Decision and mentions that Europol has the task to "obtain, collate and analyse information and intelligence".

[105] Mainly corresponding to Article 14 Europol Decision, which stipulates the conditions for collection, processing and utilisation of personal data in analysis work files.

[106] Article 5 (1) VIS access Decision 2008/633 dictates three cumulative access conditions for the national law enforcement and intelligence authorities: first, the access must be necessary for the purpose of prevention, detection and investigation of terrorist offences or other serious crime, second, necessary in a specific case and third, consultation must substantially contribute to the mentioned purposes. Once the national authorities comply with these requirements, a two-step access to the VIS data is stipulated in Article 5 (2) and (3) VIS access Decision 2008/633, which, at this stage of the procedure, also applies to Europol. The two-step access limits the initial search in the VIS to 11 data elements, including fingerprints. Only in the event of a hit, the other data from the visa application form, as well as photographs and the data entered in respect of any visa issued, annulled, revoked, refused or extended are open to access. Whereas the Member States have to fulfill all of the conditions of Article 5 VIS access Decision 2008/633, Europol's access seems to be regarded as less intrusive.

[107] However, Member States as well as Europol have to establish a list with the operating units, which are allowed to access the VIS. These units play an important role in the access procedure as they must submit a reasoned written and electronic request to the central access point established in each Member State or, respectively, at Europol to coordinate the VIS access, compare Articles 3 (3), 4 (1) and 7 (3) VIS access Decision 2008/633, OJ 2008, L-218/129.

[108] Report from 21 May 2007 of the European Parliament on the on the proposal for a Council Decision concerning access for consultation of the VIS by the authorities of the Member States

In the current state of play, Europol's rather wide access to the VIS is worrying. The exceptional aspect of allowing a law enforcement authority access to a database dealing with individuals not suspected of any crime should be at least compensated through very rigid access conditions to avoid the transformation of the VIS into a general crime fighting database, disregarding the fundamental rights of individuals. The introduction of stricter access conditions would have been an important step in this direction.[109]

In context of the enlargement of authorities having access to the VIS data, it is worth noting that not only Europol and the participating Member States may access the VIS data, but also Member States to which the VIS Regulation 767/2008 does not apply.[110] It is exercised via a participating Member State in the way that Member States not yet participating at the VIS shall make its visa data available to the participating Member States, on basis of a "duly reasoned written or electronic request".[111] The question arises whether it makes sense to limit the participation in the VIS Regulation 767/2008 to the Schengen Member States when the non-participating Member States eventually could get access to the VIS data pursuant to Article 6 VIS Regulation 767/2008.

Data protection provisions in the framework of the VIS access orientate on the level of protection of Convention No. 108 and its subsequent amendments[112], the case law pursuant to Article 8 ECHR[113], Recommendation R (87) 15 and on the third pillar data protection Framework Decision 2008/977.[114] If the data are transferred to Europol, the general rules of the Europol Decision apply.

The VIS access Decision 2008/633 nevertheless entails an important provision prohibiting the onward transfer of the VIS data at Europol.[115] In "exceptional cases of

---

responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (COM(2005)600final—2005/0323(CNS)), Committee on Civil Liberties, Justice and Home affairs, rapporteur: Sarah Ludford, pp. 7–8, para (7) and proposal for a Council Decision from 24 November 2005 concerning access for consultation of the VIS by the authorities of the Member States responsible for internal security and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences (COM(2005)600final—2005/0323(CNS)), p. 5.

[109] A welcomed provision, however, relates to the requirement to designate a specialised unit for the VIS access within Europol, allowing for better supervision while concentrating the request accesses at one specific entity. Such as in the SIS II, Europol's use of the data is subject to the consent of the Member States entering the data in the VIS, Article 7 (4) VIS access Decision 2008/633, OJ 2008, L-218/129.

[110] Due to their limited participation in the Schengen cooperation, certain Member States, such as the United Kingdom, are usually not allowed to access the VIS.

[111] Article 6 VIS access Decision 2008/633, OJ 2008, L-218/129.

[112] For those Member States, which have ratified it, the Additional Protocol of 8 November 2001 to Convention No. 108 should also be taken into account.

[113] Recital (9) VIS access Decision 2008/633/JHA, OJ 2008, L-218/129.

[114] Article 8 (1) and recital (9) VIS access Decision 2008/633, OJ 2008, L-218/129.

[115] Article 8 (4) VIS access Decision 2008/633, OJ 2008, L-218/129.

urgency", third states may nonetheless receive the VIS data.[116] A provision similar to Article 13(1) (d) third pillar data protection Framework Decision 2008/977 according to which the level of data protection of the third party must be adequate for the intended data processing does regrettably not exist.[117] While the rules on third party data transfer apply to the Member States as well as to Europol, the provisions on data security, liability and claims for compensation are governed by national law and are only addressed to the Member States. Europol relies on its own data security rules whose implementation is subjected to a very unconvincing necessity criterion.[118] The right of access, correction and deletion depends on the law of the Member State in which an applicant invokes that right.[119]

8.3.2.3 Europol's and Eurojust's Access to the CIS

In contrast to the VIS access, an agreement regulating the details of the access from Europol or Eurojust to the CIS data does not exist. Therefore, only Article 11 CIS Council Decision 2009/917 on the use of information technology for customs

---

[116] Article 8 (4) VIS access Decision 2008/633, OJ 2008, L-218/129. There is no definition of such an exceptional case, but there are three additional criteria to be fulfilled to transfer the VIS data to third parties: the data must be necessary in a specific case, the consultation must substantially contribute to the mentioned purposes and the Member States having entered the data into the VIS must have given its consent.

[117] Although, as the third pillar data protection Framework Decision 2008/977 is applicable to the VIS access Decision 2008/633, the latter rules must comply with those of the former one.

[118] Article 35 Europol Decision stipulates specific rules relating to data security involving the "necessary technical and organisational measures to ensure the implementation of this Decision". As the wording of this first paragraph of Article 35 Europol Decision suggests, the implementation of data security measures depends on the necessity of these measures. The latter are considered as "necessary where the effort they involve is proportionate to the objective they are designed to achieve in terms of protection". Thus, data security rules are subjected to a necessity criterion whose content leaves open certain questions. Which body within Europol decides about the effort to be made and about the proportionality of this effort? Europol's JSB is not mentioned in this context, but Article 10 (3) Europol Decision refers to the Management Board, which shall ensure that the measures and principles referred to in Article 35 Europol Decision are properly implemented. Consequently, the Management Board decides about the implementation of data security rules and in this way about the question to what extent the effort appears to be proportionate and as a result about the effort to be made to adopt a specific security measure. The internal Data Protection Officer or the JSB are not involved.

[119] Article 14 VIS access Decision 2008/633/JHA, OJ 2008, L-218/129. Individuals interested in knowing whether their VIS data have been transferred to Europol are merely informed in the framework of the information right provided for in Article 37 VIS Regulation 767/2008. According to this Article, the notification of the applicant is broadly restricted to the fact that Europol may receive the data. There is no information duty provided for in VIS Regulation 767/2008 in the very likely case that the data are transferred to Europol after the visa applicant or the person issuing an invitation or liable to pay the applicant's subsistence cost, has been initially informed about Europol's possibility to access the VIS data. Consequently, information about the actual transfer of the information is not given.

purposes, provides for, at first glance, almost unfettered access to the data entered into the third pillar CIS.[120]

The CIS Council Decision 2009/917 uses the general wording within its respective "mandate and the fulfilment of Europol's or Eurojust's tasks"[121], when describing the limits of the right of access of the two agencies to the CIS.[122]

Recital (5) of Council Decision 2009/917 specifies the reason for Europol's access in this way as it "should allow Europol to cross-check information obtained through other means with the information available in those databases, to identify new links that were so far not detectable and thus to produce a more comprehensive analysis".[123] Finally, access should enable Europol to "uncover connections between cases of criminal investigations, so far unknown to Europol that have a dimension in and outside the European Union".[124]

Eurojust's access refers to the need "to obtain immediate information required for an accurate initial overview enabling to identify and overcome legal obstacles and to achieve better prosecution results" as well as "to receive information of ongoing and closed investigations in different Members States and thus to enhance the support of judicial authorities in the Member States".[125]

Regrettably, no further specifications as regards the subsequent processing of the CIS data at Europol or Eurojust can be found in the CIS Council Decision 2009/917, apart from the obligation to ask the Member State originally entering the data for consent when using and transferring the data to third countries.[126]

After having obtained the consent, in case of Europol, the rules of the Europol Decision apply, which do not regulate the use or the processing of data from the other European databases within the databases of Europol.[127]

Comparable to the situation regarding the SIS II, the Eurojust Decision remains silent on the topic of Eurojust's access to the CIS.

More details on Eurojust's access to the CIS are not codified, which reveals a significant lack of legal rules resulting in the complete absence of Eurojust's mandate to access the CIS data in its own legal basis, the lack of provisions regulating both, the individual rights when the data are transferred as well as the technical details concerning the practical implementation of the access.

Moreover, a legally very doubtful provision is Article 8(1) CIS Council Decision 2009/917, which allows Europol and Eurojust to use the CIS data for any other purposes as long as they are vaguely connected to policing purposes.

---

[120] Article 11 CIS Council Decision 2009/917/JHA of 30 November 2009 on the use of information technology for customs purposes, OJ 2009, L-32320 (in the following referred to as Council Decision 2009917, OJ 2009, 323/20).

[121] Articles 11 (1) and 12 (1) Council Decision 2009/917, OJ 2009, L-323/20.

[122] Article 11 (1) Council Decision 2009/917, OJ 2009, L-323/20.

[123] Recital (5) Council Decision 2009/917, OJ 2009, L-323/20.

[124] Recital (5) Council Decision 2009/917, OJ 2009, L-323/20.

[125] Recital (6) Council Decision 2009/917, OJ 2009, L-323/20.

[126] Articles 11 (3) and 12 (2) Council Decision 2009/917, OJ 2009, L-323/20.

[127] Article 11 (3) Council Decision 2009/917, OJ 2009, L-323/20.

The only provision slightly referring to an access restriction relates to the usual interdiction to directly connect parts of the CIS to Europol's or Eurojust's own data processing systems and to transfer, download or copy the CIS data to its systems, although Europol may also request further information from the Member State.[128]

The persons having access to the CIS shall be limited to "duly authorised" Europol staff and the national members of Eurojust. In case of Europol, reminiscent of the SIS II and the VIS access rules, Europol's JSB shall additionally monitor Europol's activities in this regard. As only national members of Eurojust access the CIS, the monitoring of Eurojust's JSB is curtailed.[129]

All in all, the conditions dealing with Europol's and Eurojust's access to the CIS, compared to the SIS II and the VIS, are even more far reaching. Provisions restricting the access cannot be found which leads to almost unrestrained access of Eurojust and Europol to the CIS data.

8.3.2.4 Common Problems with Regard to the Access of Europol and Eurojust to the European Information Systems

Taking the aforementioned examples into account, it is remarkable that the purpose of the use of the transmitted data to Europol or Eurojust, which should usually be defined explicitly and restrictively when transferring personal data[130], is not further explained. The fact that the use of the data for Europol's or Eurojust's purposes considerably varies from a rather restricted use in the SIS II, the VIS or the CIS is not particularly mentioned. Taking Europol's and Eurojust's different tasks into consideration, the possible processing of SIS II, VIS or CIS data, for instance, at Europol, could have serious consequences for the social and legal situation of an individual.

Allowing Europol and Eurojust access to the extent that is necessary "for the performance of its tasks" without restricting the use afterwards is much too far reaching and should be clarified by specifying the purpose of the access and linking it to the purpose of the subsequent use. This has also to be seen in the light of the continually evolving tasks of Europol and Eurojust. A concrete factor not susceptible to change over time should be used to define Europol's and Eurojust's access conditions and the subsequent use of the data. It is, for instance, regrettable that the relatively strict access conditions applying to the law enforcement authorities of the Member States in case of the VIS do not affect Europol's access.

---

[128] Articles 11 (4) and (5) and 12 (4) Council Decision 2009/917, OJ 2009, L-323/20.

[129] However, a responsibility to inform the supplying Member State if Europol or Eurojust have evidence to suggest that an item of data is factually inaccurate or was entered contrary to the CIS Council Decision 2009/917, applies to the body as well as the obligation to introduce security measures, compare Articles 13 (3) and 28 Council Decision 2009/917, OJ 2009, L-323/20.

[130] Compare *Weber and Saravia v. Germany*, Application no. 54934/00 Admissibility Decision, from 29 June 2006.

With regard to the CIS it is important to mention that although the CIS processes various personal data elements[131], Europol's and Eurojust's access and whose subsequent processing, including a specification of the purpose of the processing of the received data, are not regulated. Individual rights, applicable to the transferred data, are limited to the standard Europol or Eurojust rules and not specifically tailored to the received data. It seems that the transfer of CIS data to Europol and Eurojust was found not important enough to be accompanied by the necessary safeguards, which are to be introduced when transferring personal data from a (customs) database to a law enforcement or judicial agency, such as Europol and Eurojust, which tasks significantly vary from the CIS and whose actions might have a serious impact on the situation of an individual.

The entire or, in Europol's case, partial lack of provisions regulating the subsequent use of the SIS II or CIS data at Eurojust and Europol, for instance, produces the situation that the responsibility of the use of the data is to a great part not clarified. Even though this might be the "heritage" of the former third pillar structures, provisions assuring that the decision of the Member States regarding the transfer of the data is supervised should have been included.[132] Otherwise, supervision at

[131] According to the CIS Convention, the CIS comprises data necessary to achieve the CIS's aim previously mentioned, such as commodities, means of transport, businesses, persons, fraud trends, availability of expertise. The new CIS Decision 2009/917 added two new categories: items detained, seized or confiscated and cash detained, seized or confiscated. The Member States determine the items to be included relating to the each of the mentioned categories whereby the data elements, which can be entered, relate to a closed list of personal data and are divided into two groups depending on the aforementioned categories. With regard to the four first categories (commodities, means of transport, businesses and persons), 11 data elements can be stored including: names, date and place of birth, nationality, sex, number and place and data of issue of the identity papers, address, any particular objective and permanent physical characteristics, reasons for entering the data, suggested action, a warning code indicating any history of being armed, violent or of escaping, registration number of the means of transport. Data elements relating to the newly introduced last two categories (items detained, seized or confiscated and cash detained, seized or confiscated) refer to names, date and place of birth, nationality, sex and address. Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership or data concerning health or sex life are excluded in any case from processing (compare Articles 3 and 4 Council Decision 2009/917, OJ 2009, L-323/20).

[132] Such provisions could, for instance, provide for a notification of the relevant national DPA about the access and transfer of the data by Europol or Eurojust. So far, in the case of Europol, in addition to its already exhaustive tasks (it issues opinions and is responsible for various other tasks: additionally to the review of compliance with individual data protection rights at Europol; it should monitor the permissibility of the transmission of data to third bodies as well as it should review the activities of Europol in its exercise of its rights to access and search data in other databases, such as the SIS II or the VIS; the JSB must also produce a report after having carried out an annual inspection at Europol; Whereby, the JSB describes inspection as a key part of its work, it also functions as an appeal committee; additionally, the JSB also interprets and examines the implementation of the Europol Decision; compare: Article 34 Council Decision of 6 April 2009 establishing the European Police Office, OJ 2009, L121/37) Europol's JSB shall also review the activities of Europol in the exercise of its access to SIS II data.

this kind of stage seems to be difficult to exercise and raises concern.[133] A further possibility could be a duty to inform the individual concerned as soon as possible about the access of other authorities to the SIS II or the CIS data or the transfer of them. This is currently left to the Member States and depends on the national data protection systems.[134]

Inconsistencies further concern in particular the general supervision of Europol's or Eurojust's access to the SIS II, CIS or VIS data. There is no coordinated approach such as it is exercised, for instance, by the European Data Protection Supervisor (EDPS) and the national DPAs in context with the central VIS.[135] Meetings between the EDPS and Europol's or Eurojust's JSB should regularly take place to guarantee a minimum of supervision. Although, in case of the VIS, one may even go further and suggest that the EDPS, which supervises the VIS, should become responsible for the supervision of the data transfer from the VIS to Europol, including regular checks on the compliance with the provisions of VIS access Decision 2008/633 during the processing of the VIS data in Europols' databases. This argument should be kept in mind, especially when considering that the VIS data contain data of innocent individuals, which are at no point suspected of a crime. When already allowing wide-ranging access conditions for Europol, the supervision of this access should at least be effective, independent and equipped with the necessary personal resources.

Also regrettably is the fact that no words are made about Europol's and Eurojust's need to access the SIS II or the CIS data, neither about the possibility to obtain the data by other less intrusive means.[136] It is particularly striking that Eurojust does not even have a legal basis to access the CIS data (apart from the CIS Council Decision 2009/917). The deficiencies in context with the CIS are fundamental and clearly need to be corrected as soon as possible to be in accordance with basic legal requirements.

A further important question arises out of the fact that neither the SIS II Decision 2007/533 nor the CIS Council Decision 2009/917 clarifies by whom and in which of Europol's databases the SIS II or the CIS data are to be included. Are they introduced by Europol or by a Member States in the EIS or used in context of an analysis work file? What happens to the data after they were included in one of Europol's databases? Are they marked and remain connected to the purposes, which had justified their collection just as the ECtHR has considered it as appropriate in *Weber and Saravia v. Germany*?[137]

---

[133] Once the consent is given, formerly SIS II data can be entered in Eurojust's and Europol's databases or transferred to third states.

[134] Compare Article 16 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-350/6.

[135] Compare VIS Regulation 767/2008.

[136] Opinion of the EDPS on the SIS II proposals [2006] OJ C91/38, point 4.2.3.

[137] *Weber and Saravia v. Germany*, Application no. 54934/00 Admissibility Decision, para 121 from 29 June 2006.

Moreover, when requesting further information from the Member States[138] or when introducing the SIS II, CIS or VIS data in, for instance, Europol's databases EIS, it is very likely that the time limit for storing originally provided for in the SIS II, CIS or the VIS starts to run again, then subject to Europol's rules. This would bypass any possible effects of the provisions providing for a time limit, such as in the SIS II (3 years), in particular in cases in which the data are transferred shortly before the original time limit expires.

Another important issue relates to the circle of accessing actors: the SIS II, for instance, prohibits access from states not participating in the Schengen Cooperation, but, Europol allows for access of a much wider range of actors, such as liaison officers from third states or international organisations, invited "experts" from the third states or other European actors such as OLAF.[139] In consequence, the circle of persons and authorities having access to the data is significantly enlarged when transferring (even if indirectly) the data in Europol's databases and could lead to investigations being instituted against the persons concerned.[140] The proposal of the EDPS and the Joint Supervisory Authority (JSA) Schengen to limit searches to the individuals whose name are already contained in Europol's files, was regrettably not considered.[141]

To conclude, in addition to the aforementioned shortcomings in context of Europol's and/or Eurojust's access to the SIS II, CIS and the VIS, it is worth noting that Europol should additionally be allowed to access the Eurodac database in the near future. If the proposal on law enforcement access to Eurodac[142] enters into force, Europol would be granted access to a database concerning exclusively the data of individuals very likely never to be convicted or suspected of a crime. As a result, law enforcement agencies of 30 countries[143] as well as Europol would have access to the data of persons who were never involved in any criminal procedure.

Serious concerns going far beyond data protection concerns arise out of the planned measures. They are among others outlined by the Meijers Committee[144],

---

[138] According to Article 41 (4) SIS II Decision 2007/533.

[139] Compare Articles 9, 22 and 23 Europol Decision.

[140] Compare *Weber and Saravia v. Germany*, Application no. 54934/00 Admissibility Decision, para 79 from 29 June 2006.

[141] Opinion of the EDPS on the SIS II proposals [2006] OJ C91/38, point 4.2.2.

[142] Proposal for a Council Decision on requesting comparisons with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, COM (2009) 344 final from 10 September 2009, in the following: Proposal on law enforcement access to Eurodac, COM (2009) 344 final from 10 September 2009.

[143] 27 Member States plus Norway, Iceland and Switzerland.

[144] Meijers Committee, standing committee of experts on international immigration, refugee and criminal law, Utrecht/The Netherlands, letter from 30 December 2009 to the European Parliament, Civil Liberties, Justice and Home Affairs Committee on the Proposal on law enforcement access to Eurodac, COM (2009) 344 final.

the EDPS[145] and the Working Party on Police and Justice[146] and can be summarised as follows: the proposals seriously challenge proportionality as well as purpose limitation, compliance with the ECtHR case law is extremely doubtful, the principle of non-discrimination risks to be undermined and the right to asylum and protection against torture and inhuman treatment seems to be disregarded. Data protection questions relating to the storage and the treatment of fingerprint data of not convicted individuals entitled to the presumption of innocence, the reasons for access, the extension of the purpose of processing, the evaluation of existing system (e.g. the Prüm Decision) and the different time limits of storage of Europol and Eurodac data arise and need to be further discussed before the adoption of the proposal.

8.4 Perspectives and Suggestions for Improvement

As follows from the foregoing considerations, information sharing in the AFSJ has become an essential tool in recent years to contribute to EU internal security policy. The Hague as well as the Stockholm programme call for an increasing inter-operability of the AFSJ databases, which in some cases leads to a questionable connection of systems established for different purposes. In view of the authors of the Stockholm programme, inter-operability constitutes a precondition for the efficiency of police and judicial cooperation in the AFSJ, whereby the interpretation of inter-operability is limited to a technical understanding. The legal dimension of inter-operability is not touched upon. Data protection rules are currently (re)negotiated for each new instrument (cf. De Hert and Vandamme 2004). Moreover, the language used in the programmes tends to understate the crucial influence the increasing cooperation has on the fundamental rights of the individuals concerned. Implicitly linked to the technical considerations is therefore the harmonisation of the individual rights standard. Otherwise, inter-operability may be reached at the cost of a week fundamental rights framework.

As a result, in addition to questions relating to the lawfulness of the ever extending functionalities of Europol and Eurojust and the limits of law enforcement access to data originally collected for a different purpose, which have to be answered elsewhere, the growing tendency to exchange data between the different AFSJ actors

[145] Opinion of the EDPS on the amended proposal for a Regulation of the European Parliament and of the Council concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EC) No (. . . /. . .) (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third country national or a stateless person), and on the proposal for a Council Decision on requesting comparisons with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, OJ 2010, C-92/1, in the following EDPS opinion on the proposal of law enforcement access to Eurodac, OJ 2010, C-92/1.

[146] The Working Party on Police and Justice (WPPJ) is a working party composed of experts from national DPA's and works together with the Article 29 Working Party, compare: Draft Annual Report for the Year 2009, p. 4.

makes it relevant to embed safeguards governing this transfer to compensate for the increased risks caused by the exchange of personal data.

Certainly, as the AFSJ still is a mix of former public international law and intergovernmental structures as well as of supranational EU structures, the data processing and protection framework is necessarily not entirely harmonised. However, the cooperation and the personal data transfer between the analysed systems already goes far beyond the former limited (legal) possibilities. So far, due to the "tendency to agree new functions before deciding the legal or technical limitations required" (Garside 2011), data protection rights could not keep up with the steady extension of the possibilities to exchange data among the AFSJ actors. In some cases, the legal instruments allowing for data exchange have a low level of individual rights protection. In others, data exchange is entirely carried out without a legal basis (e.g. Eurojust-CIS). The need for a coherent and general legal instrument on the exchange of personal data between AFSJ actors respecting the data protection rights of the persons concerned is obvious and should be urgently developed to better comply with fundamental rights in the AFSJ.

The first essential criterion, following from the respect for the rule of law, is, however, first and foremost, a clear legal basis to allow for security-related data transfer.[147] This legal basis should take into account the case whether or not the purpose of collection of the data differs from the purpose of access. Several provisions of Council Decision 2008/633 allowing national law enforcement authorities and Europol to access the VIS data[148] have an exemplary function and might serve as an example on how such an instrument would look like. A harmonised AFSJ instrument could replace the different solutions chosen so far. Its provisions might include rules on the access of domestic law enforcement authorities to European databases serving a different purpose than law enforcement, but can also be limited to EU internal AFSJ information exchange. When developing a single instrument harmonising the AFSJ data exchange, the following reflections not yet recognised in the security-related personal data exchange between AFSJ actors could be considered.

8.4.1 Specifying Unclear Legal Terms and Restricting the Purpose of Access and Transfer

Avoiding ambiguous terms is an essential requirement of an instrument regulating information exchange in the AFSJ.[149] For this purpose, the databases of the respective actors in which the transferred data could be possibly introduced as well as the databases allowed to be accessed, should be precisely defined. This definition should

[147] Examples of data exchange in absence of a legal basis was Eurojust's data transfer in JITs or Eurojust's access to the CIS.

[148] Article 5 Council Decision 2008/633, OJ 2008, L-218/129.

[149] To the requirement to define terms such as "serious crime" in a legal act, compare ECtHR case law *Kennedy v. the United Kingdom*, Application no. 26839/05, para 159 from 18 May 2010.

not only relate, for instance, to the general description of AFSJ actors' databases, but should include specifications referring to the exact databases (EIS, analysis work files) in which the data could be entered or from which the data could be retrieved (e.g. exact description of the SIS II databases).

Moreover, essential terms repeatedly used in AFSJs' legal bases and information exchange instruments, such as "terrorist offences", "serious criminal offences" and above all "prevention of crime", are to be explained and defined in a harmonised way in order to avoid legal uncertainty.[150]

Inextricably linked with clear definitions is the respect of the rule of law. Therefore, the legal basis should always lay down the conditions under which the respective European actor or Member States may obtain access for consultation of the relevant database. To prevent unclear processing purposes, the purpose of access to another database should be limited to the prevention, detection and investigation of terrorist offences and serious criminal offences subject to the mandate of the accessing actors. To avoid unilateral and possible far-reaching changes, eventual amendments to the mandate of the accessing actor after the adoption of the access decision should not be covered by the instrument.

8.4.2 Designating the Accessing Actors and Authorities

To guarantee transparency in the AFSJ data exchange and to comply with ECtHR requirements demanding "explicit and detailed provisions" relating to the information, which may be handed out and to "the authorities to which information may be communicated"[151], the authorities, which are authorised to access the data of the respective database must be precisely defined. Member States as well as the European AFSJ actors should keep a list of the designated authorities or units and should notify in a declaration to the European Parliament, the Commission and the General Secretariat of the Council their designated authorities or units.[152] To improve transparency, the list and the declarations, including possible amendments to it, could be published by the Commission in the Official Journal of the European Union. At the national level, each Member State should be obliged to keep a list of the (operating) units within the designated authorities that are authorised to access the respective

[150] The definition of the terms "terrorist and serious criminal offences" could correspond to the offences under national law, which correspond or are equivalent to the offences in Articles 1–4 of Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism, OJ 2002, L-164/3 and to the forms of crime, which correspond or are equivalent to those referred to in Article 2 (2) of Framework Decision 2002/584/JHA on the European Arrest Warrant, OJ 2001, L-190/1. The not yet defined term "prevention of crime" needs specification and could, for instance, describe a situation in which criteria based on a verifiable prognosis, open to scrutiny by an external supervisor, suggest that somebody plans to commit a crime. Factual indications, which exclude individual assumptions or pure hypothetical reflections, should underpin this estimation.

[151] *Leander v. Sweden*, Application no. 9248/81, para 55 from 26 March 1987.

[152] Similar to Article 3 (2) Council Decision 2008/633, OJ 2008, L-218/129.

database. To further strengthen the internal handling and security of the data and to guarantee that only persons authorised to consult the files[153] access the personal data, only duly empowered staff of a special unit, which received special training in the handling of personal data of the accessing actor as well as the respective database should be authorised to access the respective database.

8.4.3 Harmonising the Access Procedure

Harmonising the access procedure with regard to data entailed in another database could be a further important development towards a coordinated approach to AFSJ data exchange.

Prior to accessing a database, a reasoned written or electronic request to the respective database should be submitted by the aforementioned special units of the AFSJ actor. Upon receipt of a request for access, duly empowered staff of the special unit within the respective database should verify whether the conditions for access are fulfilled. If all conditions for access are fulfilled, transmission of the requested data to the accessing actor should be carried out by the special unit of the database in such a way as not to compromise the security of the data.[154]

8.4.4 Coordinating the Access Conditions

Access for consultation of the respective database by the designated authorities and the respective EU actors should only take place within the scope and the limits of their powers and only if certain conditions applying in every AFSJ data exchange and respecting the rights of individuals are met.

In view of the increasing data exchange, the access for mutual consultation between the AFSJ actors should be always restricted to the necessity of the access in a specific case for the purpose of the prevention, detection or investigation of terrorist offences or serious criminal offences clearly defined in the access decision. Reasonable grounds to consider that the consultation of the data will substantially contribute to the prevention, detection or investigation of any of the criminal offences in question should be an additional access condition. Furthermore, to assure that interferences with the purpose limitation principles remain exceptional, if the

---

[153] *Rotaru v. Romania*, Application no. 28341/954, para 57 from 4 May 2000.

[154] Similar to Article 4 Council Decision 2008/633, OJ 2008, L-218/129. Alternatively, in exceptional cases of urgency, the special unit within the respective database may receive written, electronic or oral requests. In such cases, it shall process the request immediately and only verify ex post whether all access conditions are fulfilled, including whether an exceptional case of urgency existed. Such an exceptional case should be immediately reported to the supervisory authority of the respective database. The ex post verification shall take place without undue delay after the processing of the request.

grounds for access differ from the purpose of the collection of the requested data, a reasoned written or electronic request to the respective database justifying the reasons for access, should be required. In that case, upon receipt of a request for such processing, duly empowered staff of the special unit within the respective database should verify whether the conditions for processing for purposes different from the purpose of collection are fulfilled.[155]

Similar to the conditions of VIS access Decision 2008/633 allowing national law enforcement authorities and Europol to access the VIS data[156], consultation of the respective database should undergo a two-step process: in a first step, access could be limited to searching with a limited amount of data in the particular file depending on the respective database and including only a selection of the data actually stored in the relevant database, such as, for instance: surname, surname at birth (former surname(s)), sex, date, place and country of birth, residence, fingerprints, etc. Only in the event of a hit, consultation of the relevant database should give full access to all of the data entailed in the database (such as any other data taken from the respective file, photographs, etc.).

8.4.5 Data Protection and Data Security Rules

With regard to the level of data protection and in the absence of an overall approach to law enforcement and judicial data protection rules, the processing of personal data consulted should be at least equivalent to the level of protection resulting from the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data as well as to the level of protection offered by the Recommendation R (87) 15 of 17 September 1987 of the Committee of Ministers of the Council of Europe Regulating the Use of Personal Data in the Police Sector, and for those Member States, which have ratified it, to the Additional Protocol of 8 November 2001 to that Convention. The provisions of 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 should additionally be applicable.

---

[155] To assure transparency and to specify the conditions for Europol, some specifications could additionally apply; Europol's access could be, for instance, necessary for the purpose of a specific analysis in a specific case referred to in Article 14 Europol Decision or for an analysis of a general nature and of a strategic type, as referred to in Article 14 (4) of the Europol Decision, provided that the data is rendered anonymous by Europol prior to such processing and retained in a form in which identification of the data subjects is no longer possible; data obtained by Europol could be further prevented from being introduced in Europol's Information System, exemptions to this rule should require the consent of Europol's supervisory body; possible additional conditions for Eurojust could also relate to the restriction not to introduce data obtained in Eurojust's Case Management System whereby exemptions to this rule should require the consent of Eurojust's supervisory body.

[156] Council Decision 2008/633, OJ 2008, L-218/129.

The processing of personal data by the accessing actor should be in any case in accordance with the legal basis of the accessing actor and the rules adopted in implementation thereof and supervised by the supervisory body of the accessing actor. In the absence of one single AFSJ supervisory system and to guarantee effective supervision, personal data originally underlying the supervision of another authority must at any stage of the processing be accessible to this authority.

Special attention needs to be paid to the current violation of the purpose limitation principle in cases in which data collected for purposes outside of crime prevention are later used for law enforcement purposes. Enforcing and strictly applying the purpose limitation principle by introducing a general rule applicable to each AFSJ data exchange whereupon personal data obtained from the respective database shall only be processed for the specific purpose of the collection would counteract this worrying development. If, in exceptional cases, the purpose of collection differs from the purpose of the transfer, this purpose has to be evaluated by the duly empowered staff of the special unit within the respective database mentioned above. Particular attention thereby has to be paid to the question whether the change in the purpose is justified by evidence that indicates that the data in question substantially contribute to the prevention, detection or investigation of the criminal offences in question and that the change in the purpose is proportional in its means.

To limit data storing in time[157], any extension to the time limit originally applicable to the obtained data by the accessing actor should be subject to the approval of the supervisory bodies of both, the accessing actor as well as of the accessed database.[158]

Finally, the list laying down the data security measures of Council Decision 2008/633 allowing national law enforcement authorities and Europol to access the VIS data[159] regulates in detail the necessary security requirements, which the Member States have to apply. This list could serve as an example for similar provisions in every AFSJ data exchange. To guarantee a harmonised standard and to prevent provisions, such as in the Europol Decision, which make the establishment of data security rules dependent the necessity of such rules[160], its provisions should in any case be extended to all AFSJ actors.

8.4.6 Follow-up of the Transferred Data

Harmonising the criteria for the transfer of data obtained from another database to third states would contribute to an increased legal certainty in a currently rather

---

[157] *S. and Marper v. the United Kingdom*, Application nos. 30562/04 and 30566/04 from 4 December 2008, para 119.

[158] In addition, before being authorised to process data stored in the database, the staff of the authorities having a right to access the database should receive appropriate training about data security and data protection rules including being informed of any relevant criminal offences and penalties.

[159] Article 9 (2) Council Decision 2008/633, OJ 2008, L-218/129.

[160] Compare Article 35 Europol Decision (footnote 118).

under-regulated area.[161] The transfer of such data could be subjected to the following conditions:

- If the purpose of collection of the data differed from the purpose of access, such personal data obtained from the database should not be transferred or made available to a third country or to an international organisation. Exceptions must be justified by evidence proving the importance of the exceptional situation.
- If the purpose of collection of the data corresponded to the purpose of access, such personal data obtained from the database could be transferred or made available to a third country or to an international organisation under the conditions of an agreement concluded with the third state assuring an adequate level of protection in the sense of Article 25 of Directive 95/46 for the intended data processing, exclusively for the purposes of the prevention and detection of terrorist offences and of serious criminal offences and under the access conditions set out above, subject to the consent of the Member State having entered the data into the database and in accordance with the national law of the Member State transferring the data or making them available. Ad hoc transmission to third states in absence of an exchange agreement should be limited to very exceptional cases and only with the sole aim of taking urgent measures to counter imminent serious danger threatening a person or public security. An undertaking obliging the recipient to use the data only for the agreed purpose of transmission should be concluded before the transfer. In any case, if ad hoc data transfer is carried out, the supervisory authority of the transferring actor needs to be informed about the transfer and has the right to prevent further transfers when it comes to the conclusion that the data protection requirements are repeatedly not complied with.
- In both cases the respective EU actor and, in accordance with national law, Member States should ensure that records are kept of such transfers and make them available to national data protection authorities upon request. In addition, rules restricting the onward transfer of the already transmitted data are equally important to limit the risks arising out of the extension of the circle of recipients. The conditions relating to onward transfer entailed in the implementing rules governing Europol's relations with partners[162], could thereby have exemplary function. Above all, the provisions, which oblige the recipient to give an undertaking (relating to an obligation to delete incorrect or outdated data, to delete data in case they are not anymore necessary for the purpose of the transfer, to asks the transferring actor for consent before further transferring received data, etc.) to guarantee certain basic data protection rights, should serve as an example in the whole area of AFSJ-related data exchange.

---

[161] Europol is the only body providing for certain basic rules in cases of third-party transfer, compare: Council Decision 2009/934/JHA of 30 November 2009 adopting the implementing rules governing Europol's relations with partners, including the exchange of personal and classified information, OJ 2009, L-325/6.

[162] Council Decision 2009/934/JHA of 30 November 2009 adopting the implementing rules governing Europol's relations with partners, including the exchange of personal and classified information, OJ 2009, L-325/6.

8.4.7 Cooperation Between Data Protection Authorities and Penalties in Case of Misuse

To ensure the practical enforcement of data protection rights, the national supervisory authorities, the supervisory authority of the database and the supervisory authority of the accessing actor, should closely cooperate in contributing to a coordinated supervision of the transfer from the database to the respective European actor.[163]

A provision for penalties in form of administrative and/or criminal fines that are effective, proportionate and dissuasive if the data are used contrary to the rules of the decision regulating the transfer, would considerably contribute to an effective enforcement of the data protection rules entailed in the decision.

8.4.8 Access Right, Correction, Deletion and Notification

To improve transparency, the reasons to deny access could be unified (e.g. access can be denied when the access may jeopardise the fulfilment of the AFSJ actors' tasks, a national investigation or the rights and freedoms of third parties[164]) and their application should in any case be open to external supervision. The internal Data Protection Officer should be informed about each access request and involved in the decision whether access is to be granted or not. If access is denied, appeal should be possible to the respective supervisory authority, which then should have the possibility to get access to the respective documents justifying the refusal. A time limit (of three months) to reply to an access request would support the practical enforcement of the access right.

Transparency and a clear definition of the circumstances and limits of the storing require that information about the transfer of the data to another database is to be provided to the person concerned by the accessing actor or the Member States entering the data at the time of the transfer or as soon as notification can be carried out without jeopardising the purpose of the transfer. The protection of data of persons, which were entered in the database due to the person's incidental link to the actual

[163] The cooperation between national and European DPAs should include the exchange of relevant information, the assistance of each other in carrying out audits and inspections or the examination of difficulties of interpretation or application of the decision regulating the data exchange. Studying problems with the exercise of independent supervision or with the exercise of the rights of data subjects and supporting each other in cases where individuals exercise their right of access, correction, deletion and notification or drawing up harmonised proposals for joint solutions to any problems including the promotion of awareness of data protection rights would complement the cooperation. For this purpose, regular meetings resulting in an annual joint report should take place. This joint activity report should be sent to the European Parliament, the Council, the Commission and the supervisory authority managing the database and include a chapter of each Member State prepared by the national supervisory authority of that Member State containing an assessment of the cases where individuals exercised their right of access, correction, deletion and notification.

[164] Article 19 (4) Eurojust Decision.

targeted person (e.g. victims, witnesses, person issuing an invitation and/or liable to pay the applicant's subsistence costs during the stay, etc.), could be improved when introducing a general notification duty in case their data are transferred. This duty could embrace additional information on the identity of the actor receiving the data together with its contact details, the purposes for which the data will be processed at the actor receiving the data, the categories of recipients of the data, including the possible third parties, information on changes concerning the data retention period as well as information on the necessity and the purpose of the transfer.[165]

To prevent that the incorrect data obtained from a database are again transferred to possible third parties, the AFSJ actor should, upon receiving such a request or if it has any other evidence to suggest that data processed in the database are inaccurate, immediately inform the authority of the Member State, which has entered the data in the database, which shall check the data concerned and, if necessary, correct or delete them immediately.[166]

A duty to explain in writing to the person concerned without delay why the AFSJ actor or the Member State responsible is not prepared to correct or delete data relating to him if it does not agree that data recorded in the database are inaccurate or have been recorded unlawfully, would additionally improve the practical implementation of the correction or deletion right. This information should contain an explanation of the steps, which the requesting person can take if he does not accept the explanation provided including information on how to bring an action or a complaint before the competent authorities or courts and on any assistance that is available. Moreover, a follow-up given to the exercise of the rights of correction and deletion should be carried out as soon as possible by the responsible supervisory body.

8.4.9 Keeping of Records

To facilitate the monitoring and evaluation tasks of the supervisory authorities, an ex post control of the admissibility of all data processing operations resulting from access to the database for consultation should be introduced. All access requests should be recorded for the purposes of checking whether the search was admissible or not, for the purpose of monitoring the lawfulness of data processing, for self-monitoring, ensuring the proper functioning of the system as well as for checking the data integrity and security.[167]

---

[165] In case a person concerned exercises its right to challenge the accuracy of its data, the AFSJ actor or the Member State responsible should be obliged to check the accuracy of the data and the lawfulness of their processing in the database within a limited period.

[166] Similar to Article 14 (5) VIS access Decision 2008/633 the Member State or the AFSJ actor responsible shall confirm in writing to the person concerned without delay that it has taken action to correct or delete data relating to it.

[167] Compare Article 16 VIS access Decision 2008/633, OJ 2008, L-218/129. Such records must be subject to the necessary security requirements and should be deleted after the retention period of

8.4.10 Implementing Effective Monitoring and Evaluation

Effective monitoring and evaluation mechanisms contribute to an improved control of the effectiveness and the necessity in terms of output, security and quality of service of the access to other databases.[168] Consequently, the respective supervisory authorities in cooperation with the respective AFSJ actor should carry out checks and submit a report to the European Parliament, the Council and the Commission on the technical functioning, the need and the use of the access possibilities of the respective database.[169] Exceptional cases of urgency should be documented and an overall "evaluation of the application and the results achieved against the objectives and an assessment of the continuing validity of the underlying rationale" behind the access as well as the impact on fundamental rights should be made.[170] This report should be made public to allow for discussion of its results.

8.5 Conclusion

Summarising, the currently under-regulated data exchange between the different AFSJ actors (inter-agency exchange and access of Europol and Eurojust to EU databases) can only be effectively countered by the introduction of common principles regulating the data exchange and the protection rights of individuals in this area. After the adoption of the Lisbon Treaty, the chances to introduce such principles are better than ever. The pillars are abolished, decision making has improved and the participation of the European Parliament in the legislative process in the AFSJ assures an increased respect of fundamental rights. Article 16 TFEU introduced a comprehensive legal basis for the protection of personal data applicable to almost all Union policies, including police and judicial cooperation (Commission communication 2010, p. 13, para 2.3). The Commission repeatedly emphasises the need to have a "comprehensive protection scheme and to strengthen the EU's stance in protecting the personal data of the individual in the context of all EU policies, including law enforcement and crime prevention". (Commission communication 2010) The Data Protection Directive 95/46 is in the review process and common data protection principles, covering the former first as well as the third pillar, are likely to be

---

the data has expired. Comparable to Article 16 (1) VIS access Decision 2008/633 allowing national law enforcement authorities and Europol to access the VIS data, those records could show: the exact purpose of the access for consultation referred to in Article 5 (1), including the form of terrorist offence or other serious criminal offence concerned, the respective file reference; the date and exact time of access; where applicable that use has been made of the urgent access procedure; the data used for consultation; the type of data consulted and according to the rules of the respective AFSJ actor or to national rules, the identifying mark of the official who carried out the search and of the official who ordered the search or supply.

[168] Compare Article 17 (1) VIS access Decision 2008/633, OJ 2008, L-218/129.

[169] Analogous to Article 17 VIS access Decision 2008/633, OJ 2008, L-218/129.

[170] Article 17 (4) VIS access Decision 2008/633, OJ 2008, L-218/129.

introduced in the new version (Commission communication 2010, p. 4, para 1). This essay aimed at contributing to the current discussion by presenting one of several solutions to develop a practical and comprehensive approach, including common data protection principles, in the area of EU internal AFSJ information exchange.

References

Commission communication. 2010. On A comprehensive strategy on data protection in the European Union, COM(2010) 609 final of 4 November 2010, p. 13, para 2.3.

De Buck, Bart. 2007. Joint investigation teams: The participation of Europol officials. *ERA Forum* 8:263.

De Hert, Paul, and Luc Vandamme. 2004. European police and judicial information-sharing, cooperation: Incorporation into the community, bypassing and extension of schengen. *ERA Forum* 5:425–434.

De Moor, Stefan. 2009. The difficulties of joint investigation teams and the possible role of OLAF. *Eucrim* 3:94–99, 97.

De Schutter, Olivier. 2008. The two Europes of human rights: The emerging division of tasks between the Council of Europe and the European Union in promoting human rights in Europe. *Columbia Journal of European Law* 14:509–560.

Garside, Alice. 2011. The political genesis and legal impact of proposals for the SIS II: What cost for data protection and security in the EU?, 16, Sussex Migration Working Paper no. 30, March 2006. http://www.sussex.ac.uk/migration/documents/mwp30.pdf. Accessed 12 July 2011.

Gusy, Christoph. 2008. Europäischer Datenschutz. In *Alternativentwirf Europol und europäischer Datenschutz*, ed. Jürgen Wolter et al., 265–280. Heidelberg: C.F. Müller Verlag.

Hijmans, Hielke, and Alfonso Scirocco. 2009. Shortcomings in EU data protection in the third and the second pillars. Can the Lisbon Treaty be expected to help? *Common Market Law Review* 46:1485–1525.

Holzenberger, Mark. 2006. Europols kleine Schwester—Die Europäische Grenzschutzagentur Frontex. *Bürgerrechte und Polizei/CILIP* 2:56–63.

Horvatis, Lisa, and Bart deBuck. 2007. The Europol and Eurojust project on joint investigation teams. *ERA Forum* 8:239–243.

Lopes da Mota, José Luis. 2009. Eurojust and its role in joint investigation teams. *Eucrim* 3:88–90.

Mitsilegas, Valsamis. 2009. *EU criminal law*. 223. Oxford: Hart.

Ralf, Riegel. 2009. Gemeinsame Ermittlungsgruppen, Herausforderungen und Lösungen. *Eucrim* 3:99–106.

Rijken, Conny, and Gert Vermeulen. 2006. *Joint investigation teams in the European Union, from theory to practice*. The Hague: T.M.C Asser Press.

Siemen, Birte. 2006. *Datenschutz als europäisches Grundrecht*. Berlin: Duncker & Humblot.

Vervaele, John A. E. 2008. The shaping and reshaping of Eurojust and OLAF. *Eucrim* 184:3–4.