

Ensuring effective data protection in the field of police and judicial activities: some considerations to achieve security, justice and freedom

Diana Alonso Blas



Published online: 30 April 2010
© ERA 2010

Abstract The Treaty of Lisbon creates new opportunities in the field of data protection at European level. While some advocate for one set of rules applicable for all sectors of activity of the European Union, this article aims at explaining, based on the extensive experience of the author in implementing data protection in practice in a law enforcement organisation, why the “one fits all” perspective would not offer effective protection in the former third pillar sector and why a tailor made legal framework would lead to better protection for individuals and better compliance with data protection.

Keywords Data protection · Justice · Treaty of Lisbon · Tailor made rules · Security · Freedom

1 Introduction

The entry into force of the Treaty of Lisbon¹ in December 2009 has brought with it a number of substantial changes regarding data protection in Europe. The most important improvement is the introduction of its Article 16,² which reads as follows:

¹Treaty of Lisbon amending the Treaty of the European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007 (2007/C 306/01), OJ C 306 of 17.12.2007, p. 1. See for more information: http://europa.eu/lisbon_treaty/index_en.htm.

²Article 16 of the Treaty on the Functioning of the European Union.

This paper is based on the presentation given by the author at the ERA event on “Data Protection in the Field of Justice and Home Affairs”, held on 30 January 2010 in Brussels. The opinions expressed in this article are however her personal ones and do not necessarily represent those of the organisation.

D. Alonso Blas LL.M., Data Protection Officer (✉)
Eurojust, Maanweg 174, 2516 AB, The Hague, Netherlands
e-mail: dalonsoblas@eurojust.europa.eu

“1. Everyone has the right to the protection of personal data concerning him or her.

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

The existence of this Article, combined with the abolition of the previous pillar structure, has been considered by some as a great new opportunity to put in place one general comprehensive instrument for all fields of activity of the Union.³ Legally speaking, this is of course a possible result of the Treaty; however, it is important to mention that the Treaty also contains elements which point to a different direction:

- A declaration was adopted together with the treaty⁴ with the following wording: *The Conference acknowledges that specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 B of the Treaty on the Functioning of the European Union may prove necessary because of the specific nature of these fields.* As underlined by Hijmans and Scirocco,⁵ it clarifies that in the view of the Member States the current Third Pillar will not be a normal area of law where just the general framework for data protection applies.
- Further, all existing legislation adopted before the entry into force of the Treaty of Lisbon remains valid until the acts are repealed, annulled or amended.⁶ In that respect it should not be forgotten that the EU legislator has been very active in the field of data protection in the former third pillar area during the last couple of years and the Council has adopted, with unanimity of the Member States as it was required before Lisbon, the Framework Decision on the protection of personal data processed in the framework of police and judicial coop-

³See the article of H. Hijmans and A. Scirocco [3], both working at the European Data Protection Supervisor: *The point of departure is that the Lisbon Treaty necessarily leads to a fundamental change in the system of data protection within the EU. It abolishes the pillar structure, which is the cause of a number of the deficiencies and it introduces a provision on data protection (Art. 16 TFEU) with general application, which means that all areas of EU law are covered. This new Article 16 TFEU is designed to be the central source of data protection within the EU.*

⁴Declaration number 21. Declaration on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation.

⁵See footnote 3.

⁶See Article 10 of Protocol No. 36 on transitional provisions, which regulates that the legal effects of all acts adopted before the entry into force of the Lisbon Treaty shall be preserved, until the acts are repealed, annulled or amended.

eration in criminal matters⁷ as well as the revised Eurojust⁸ and Europol⁹ decisions. The first of these decisions has yet to be implemented by the Member States by 27 November 2010; the Eurojust decision entered into force on 4 June 2009 and the Europol one from the 1st of January 2010 but both the Eurojust and Europol decision are still in the process of implementation at national level.

- It can also be observed that Article 16 does not necessarily imply one set of rules for all areas of activity of the European Union. The Article refers to “the rules”, without prescribing whether it should be one legal instrument or several. It also refers to “independent data protection authorities”, in plural.

The recent communication from the Commission to the European Parliament and the Council on *An area of freedom, security and justice serving the citizen*¹⁰ (Stockholm programme), while giving data protection a prominent role in this context, does not define any clear direction for the development of this area in the following years. It refers on one hand to the fact that the Union must secure a new comprehensive strategy to protect citizens’s data within the EU and in its relations with other countries, suggesting therefore *a contrario* a change from the existing division first-third pillar. On the other hand, the communication refers to the high level of protection offered by the current legal framework, which should be maintained.

The Lisbon Treaty creates the possibility for the EU legislator to put in place one comprehensive set of rules for all sectors but it does not prescribe that. It allows also for other options, such as various instruments which together would constitute a comprehensive framework for data protection but would at the same time respect the distinct needs linked to the specific nature of the processing of personal data in the fields of judicial cooperation in criminal matters and police cooperation, as recognised by the Member States in Declaration 21.

This article aims at explaining, based on the extensive experience of the author in implementing data protection in practice in a law enforcement organisation, why the “one fits all” perspective would not offer effective protection in the sector of the former third pillar and why a tailor made legal framework would lead to better protection for individuals and compliance with data protection.

⁷Council Framework Decision 2008/977/JHA of 27 November 2008, OJ 350, 30.12.2008, p. 60.

⁸Council Decision on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime, adopted by the Council on the 16th of December 2008, Council Decision 2009/426/JHA of 16 December 2008, published on the OJ L 138, 4.6.2009, p. 14. For more information on this Decision see *Alonso Blas* [2].

⁹Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (EUROPOL), published in the OJ L121, 15.5.2009, pp. 37–66.

¹⁰COM (2009) 262 final, Brussels, 10.6.2009.

2 Need for specific, tailor made rules in the sector of police and judicial cooperation

2.1 Historical perspective: many acknowledgments of the specific nature of processing of personal data in the police and judicial cooperation

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,¹¹ ratified as of 1 April 1910 by 41 countries and signed by another three,¹² is the only existing international data protection instrument generally applicable at present. The application of Convention 108 is not limited to the former first pillar; in fact the pillars are an “EU invention”, not a Council of Europe one. Actually, the Convention plays a fundamental role in the former third pillar sector.

Already in 1987 the Council of Europe saw the need to deal with the specific elements linked to the processing of personal data in the police sector, issuing the Recommendation on the use of personal data in the police sector,¹³ which was adopted by the Council of Europe’s Committee of Ministers and contained more detailed provisions. As the Position paper on Law Enforcement & Information Exchange in the EU, adopted at the Spring Conference of European Data Protection Authorities, in Krakow on 25–26 April 2005 (hereinafter referred to as the Krakow declaration) explained, *the different Recommendations from the Committee of Ministers of the Council of Europe including the Recommendation on the use of personal data in the police sector demonstrate the need to adapt the general principles in order to meet the specific requirements of particular sectors.*

In the context of the European Union, many instruments have been introduced in the area which formerly constituted the third pillar, including very specific rules for the various sectors of activity within this field. For instance, Article 129 of the Convention implementing the Schengen Agreement¹⁴ provides for specific rules regarding police co-operation and the exchange of personal data. The Europol convention¹⁵ and the 2002 Eurojust Decision¹⁶ were put in place and created a very detailed framework for data protection taking into account the mandate and operations of such organisations.

¹¹Convention opened to signature on the 28th January 1981 in Strasbourg, often referred to as “Convention 108”.

¹²See for a full overview of the ratifications and signatures: <http://Conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=1&DF=&CL=ENG>.

¹³Recommendation No. R (87) 15, of 17 September 1987.

¹⁴Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, O.J. 2000, L 239/19.

¹⁵The Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention), *Official Journal C 316, 27/11/1995 P. 0002–0032*.

¹⁶Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against organised crime, OJ L 63, 6.3.2001, p. 1, as last amended by Decision 2003/659/JHA (OJ L 245, 29.9.2003, p. 44), often referred to as “the Eurojust Decision”.

The value of these detailed and complete sets of rules was acknowledged in recital 39 of the preamble of the framework decision on data protection in the field of police and justice.¹⁷

Several acts, adopted on the basis of Title VI of the Treaty on European Union, contain specific provisions on the protection of personal data exchanged or otherwise processed pursuant to those acts. In some cases these provisions constitute a complete and coherent set of rules covering all relevant aspects of data protection (principles of data quality, rules on data security, regulation of the rights and safeguards of data subjects, organisation of supervision and liability) and they regulate these matters in more detail than this Framework Decision. The relevant set of data protection provisions of those acts, in particular those governing the functioning of Europol, Eurojust, the Schengen Information System (SIS) and the Customs Information System (CIS), as well as those introducing direct access for the authorities of Member States to certain data systems of other Member States, should not be affected by this Framework Decision.

The Krakow declaration 2005 underlined the specific nature of the processing operations in the field of police and justice and advocated for tailor made rules in this area:

Personal data processed for law enforcement purposes are particularly sensitive given the consequences that might result from any improper use of these data. Furthermore, the legal environment in which law enforcement authorities operate is changing. For example, the ‘availability principle’ put forward in the Hague Programme would require law enforcement authorities to disclose personal data to other Member States, rather than just allowing them to do so. For these reasons, a new legal framework applicable to law enforcement activities—as advocated by the Commission—would have to provide a tailor-made set of rules; simply reaffirming general principles would not be sufficient.

It is particularly interesting to mention that the European Data Protection Supervisor, in its first opinion on the envisaged framework decision on data protection in the third pillar,¹⁸ underscored the need to have rules taking into account the *specific and sensitive nature of the processing of personal data in this area* (police and justice sector):

The EDPS points to the fact that the present general framework for data protection in this area is insufficient. In the first place, directive 95/46/EC does not apply to the processing of personal data in the course of activities which fall outside the scope of Community law, such as those provided for by Title VI of the Treaty on the European Union (Article 3 (2) of the directive). Although in most Member States the scope of the implementing legislation is wider than the

¹⁷Council Framework Decision 2008/977/JHA of 27 November 2008, OJ 350, 30.12.2008, p. 60.

¹⁸Opinion of 19 December 2005 on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters (COM (2005)475 final). OJ C 47, 25.02.2006, p. 27.

directive itself requires and does not exclude data processing for the purpose of law enforcement, significant differences in national law exist. In the second place, the Council of Europe Convention No 108 by which all the Member States are bound does not provide for the necessary preciseness in the protection as has been recognised already at the time of the adoption of Directive 95/46/EC. In the third place, neither of these two legal instruments takes into account the specific characteristics of the exchange of data by police and judicial authorities.

This new framework should not only respect the principles of data protection as laid down in Directive 95/46/EC—it is important to guarantee the consistency of the data protection within the European Union—but also provide for an additional set of rules taking into account the specific nature of the area of law enforcement. [...] They reflect the specific and sensitive nature of the processing of personal data in this area.

The long awaited Framework Decision in the police and judicial sector, whose implementation period has still not finished, has generally been considered by the data protection community as a “missed opportunity”¹⁹ but luckily, the specific regimes of Eurojust, Europol and the Schengen and Customs Information Systems remained untouched. According to one of the responsible negotiators from the Council Secretariat, one of the main reasons for the disappointing outcome of the negotiations of this instrument was the fact that the areas which it aimed to cover were too diverse; in other words, regulating the processing operations of police and justice in one instrument was extremely difficult. The preamble of this framework decision acknowledges in its recital 11 the need for specific rules:

It is necessary to specify the objectives of data protection within the framework of police and judicial activities and to lay down rules concerning the lawfulness of processing of personal data in order to ensure that any information that might be exchanged has been processed lawfully and in accordance with fundamental principles relating to data quality. At the same time the legitimate activities of the police, customs, judicial and other competent authorities should not be jeopardised in any way.

The recent joint contribution of the Article 29 Working Party²⁰ and the Working Party on Police and Justice²¹ to the Consultation of the European Commission on the legal

¹⁹See for further information on the discussions regarding the Framework Decision the opinions of 19 December 2005, 29 November 2006 and 27 April 2007 of the European Data Protection Supervisor on this instrument (the third opinion is published in the OJ C 139, 23.06.2007, p. 1; the first Opinion can be found in the OJ C 47, 25.2.2006, p. 27; the second Opinion is available on EDPS website: www.edps.europa.eu) as well as the article by Alonso Blas [1].

²⁰This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. The secretariat is provided by Directorate D (Fundamental Rights and Citizenship) of the European Commission, Directorate General Justice, Freedom and Security, B-1049 Brussels, Belgium, Office No LX-46 01/190. Website: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm.

²¹The Working Party on Police and Justice was set up as a working group of the Conference of the European Data Protection Authorities. It is mandated to monitor and examine the developments in the area of

framework for the fundamental right to protection of personal data on the Future of Privacy, adopted on 01 December 2009,²² also emphasises the specificity of this area:

Data protection in the field of police and justice is a specific subject which requires specific attention, taking into account the complex relation between the activities of the State to ensure security and the protection of the personal data of the individual. The specificity of this area is not only the result of the former pillar structure of the previous EU-Treaties, but is more widely recognised (see for instance the exceptions of Article 13 of Directive 95/46/EC and Declaration 21 attached to the Lisbon Treaty). With the entry into force of the Lisbon Treaty, new perspectives will be created for law making in the field of data protection. The pillar structure will be abolished and with Article 16 TFEU a single legal basis is created for data protection in almost all areas of EU law. This does not necessarily mean that the implementation of data protection principles for police and justice should be the same as the rules in other parts of society. Declaration 21, attached to the Lisbon Treaty claims that specific rules for law enforcement area 'may prove to be necessary'.

This joint document of the Working Parties mentions in its introduction that the new legal framework under Lisbon could be used to, among other things, *include the fundamental principles of data protection into one comprehensive legal framework, which also applies to police and judicial cooperation in criminal matters*. The formulation chosen is interesting as it refers only to the fundamental principles of data protection, not to detailed regulation, and it refers to one comprehensive legal framework, not to one instrument, and a legal framework may comprise various instruments. Obviously other interpretations of this wording are possible but, in the light of the above-mentioned comments in the document as to the specific nature of the sector, as well as the mention later on in the text to the fact that *special attention—including where necessary tailor made safeguards for data protection—is needed for large scale information systems within the EU*, leads to the conclusion that the Data Protection Authorities did not necessarily want one single instrument for everything. In any case such wish is not clearly stated anywhere in the extensive document.

A further important element to consider is the speech of Commissioner Viviane Reding at the occasion of the Data Protection Day, 28 January 2010, at the European Parliament.²³ In her speech, titled *The challenges ahead for the European Union*, Commissioner Reding highlighted the *need to incorporate the fundamental principles of data protection to cover all areas of EU competence, including police and judicial cooperation in criminal matters and the EU's external relations*. In the same line of the document of the Working Parties, the Commissioner refers to the need to apply the fundamental principles of data protection to all fields.

police and law enforcement to face the growing challenges for the protection of individuals with regard to the processing of their personal data.

²²WP 168, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/WP1682009/wp168_en.pdf.

²³This speech can be found at: <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/16&format=HTML&aged=0&language=EN&guiLanguage=en>.

It is the opinion of the author of this article that the general application of the principles is not only desirable but it is already a reality as those principles are already generally applicable to all Member States in all sectors due to the ratification of Convention 108. The problem is not to apply the common principles, which are already there and have been taken over in all existing EU rules regarding data protection in the former third pillar sector, but, on the contrary, to establish one EU instrument containing detailed data protection applicable to all sectors would be neither feasible nor advisable, as it will be further explained in the following sections.

2.2 Some practical examples of the specific nature of processing of personal data in the police and judicial cooperation

As the first opinion of the EDPS on the Framework Decision on data protection in the field of police and justice²⁴ had stressed, it is fundamental to have rules in place *taking into account the specific nature of the area of law enforcement and reflecting the specific and sensitive nature of the processing of personal data in this area.*

While indeed the principles, as established in Convention 108 and further developed in Directive 95/46/EC,²⁵ are the same as in the former first pillar are, there are a number of substantial differences in the data processing activities of police and justice which make the rules of Directive 95/46/EC not directly suitable in this field.

2.2.1 Legal grounds for processing

Starting from the basis for the processing operations, the legal grounds making processing legitimate, it is obviously practically impossible to use consent as a legal ground for processing for police and justice processing operations.

2.2.2 Data subjects

Many documents in the past, such the Krakow declaration, have mentioned the need to have specific rules for various categories of individuals taking into account their position in the law enforcement processes.²⁶ In the same line of thinking it should be considered that there are substantial differences of approach when processing data of clients of a company, as it is commonly the case within the scope of application

²⁴Opinion of 19 December 2005 on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters (COM (2005)475 final), OJ C 47, 25.02.2006, p. 27.

²⁵Directive 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, *Official Journal of the European Communities* L 281, p. 31, Volume 38, 23 November 1995, often referred to as “the Directive”.

²⁶The processing of data on persons who are not suspected of having committed any crime (other than victims and witnesses) should only be allowed under certain specific conditions and when absolutely necessary for a legitimate, well-defined and specific purpose. The processing of data on non-suspects such as when making speculative enquiries or for the purpose of establishing whether or not a suspicion relating to a serious criminal activity might be justified, should be restricted to a limited period, and the further use of these data for other purposes should be prohibited.

of the Directive, or collecting and further processing personal data of people who are suspects of a crime, victims or witnesses. Such differences should also lead to particular rules and provisions. This is for instance the case in the Eurojust Decision, which contains rules²⁷ offering particular protection when personal data on persons who are suspect of a criminal investigation or prosecution, victims and witnesses are processed. The data which might be processed regarding victims and witnesses are limited and additional guarantees are put in place for its protection.

2.2.3 Specialised data processing/information systems

Many processing operations taking place in the area of police and justice are linked to specialised data processing/information systems which, as underlined in the recent document of the Working Party 29 and the Working Party on Police, deserve special care: *special attention—including where necessary tailor made safeguards for data protection—is needed for large scale information systems within the EU*. The complexity of such information systems, which are presently regulated to a great level of detail in the context of Eurojust²⁸ and Europol²⁹ in any case, requires very meticulous regulation and raises other issues than the normal processing activities taking place in the private or even public sector.

2.2.4 Transfers to third countries/parties

Regarding transfers of data to third countries, the situation is also completely different for a company, which can normally decide with which parties it wishes to get into business and can in that context therefore take into account the adequacy requirement for third countries, and for law enforcement agencies, which might need to cooperate with authorities in a third country due to imminent reasons of protection of individuals, prevention of crimes and so forth.

This surely does not imply that in the field of the former third pillar the criteria of adequate protection should not be taken into account, and the very extensive data protection provisions in the international agreements concluded by Europol³⁰ and

²⁷ See article 15 of the Eurojust Decision, in particular paragraphs 2, 3 and 4.

²⁸ The Rules of procedure on the processing and protection of personal data at Eurojust, adopted by the College of Eurojust unanimously in October 2004 and by the Council in Brussels in February 2005 (OJ C 68, 19.3.2005, p. 1), introduced in their Article 23 the concept of the automated Case Management System (CMS), including the temporary work files and the index. Chapter III of the data protection rules regulates in detail various aspects of the processing of personal data in the CMS, which has become the crucial tool for the processing of personal data at Eurojust. The CMS was designed taking full account of the data protection provisions in the Eurojust decision and in the rules on the processing and the protection of personal data. The design facilitates compliance with the legal base and prevents possible breaches of the data protection rules to a great extent. Only pre-defined data classes may be entered in the system preventing the insertion of non-allowed data. Compliance is also ensured in what regards notifications to the DPO, which are automatically generated by the system.

²⁹ See for Europol the Council Act of 3 November 1998 adopting rules applicable to Europol analysis files (*Official Journal C 026, 30.1.1999, p. 1*), and Council Decision of 15 October 2007 amending the Council Act adopting rules applicable to Europol analysis files (*Official Journal L 027, 20.10.2007, p. 23*).

³⁰ See for the list of agreements concluded by Europol: <http://www.europol.europa.eu/index.asp?page=agreements>.

Eurojust³¹ with third countries underscore the seriousness with which the level of protection applicable to the law enforcement authorities of a third country is considered, but it implies that it will need to be applied in a different way, more linked to the specific position of the recipients in that third country instead of a whole country.

It should further also be considered that in some circumstances transfers might have to take place, even if the level of protection of the third country is not adequate, due to the need to prevent terrorism attacks or other serious crimes. This is for instance regulated in Article 26a, paragraph 9, of the Eurojust Decision as follows:

However, even if the conditions referred to in paragraph 7 are not fulfilled, a national member may, acting in his capacity as a competent national authority and in conformity with the provisions of his own national law, by way of exception and with the sole aim of taking urgent measures to counter imminent serious danger threatening a person or public security, carry out an exchange of information involving personal data. The national member shall be responsible for the legality of authorising the communication. The national member shall keep a record of communications of data and of the grounds for such communications. The communication of data shall be authorised only if the recipient gives an undertaking that the data will be used only for the purpose for which they were communicated.

Article 28.4 of the Eurojust Data Protection Rules further defines the obligation to register such exceptional transfer in the Case management system to ensure that a control *a posteriori* by the Data protection officer can take place: The National Member shall document such an exceptional transfer in the temporary work file related to the case, stating the grounds for such a communication, and shall inform the Data Protection Officer of such a communication. The Data Protection Officer shall verify if such transfers only take place in exceptional and urgent cases.

Europol has by the way a similar regime in its legal framework, in paragraphs 8 and 9 of Article 23 of the Europol Decision.³²

³¹ So far Eurojust has agreements in place with Norway (2005), Iceland (2005), the United States of America (2006), the Republic of Croatia (2007), Switzerland and the former Yugoslav Republic of Macedonia (both concluded in 2008). Eurojust has Memoranda of Understanding in place, not implying any exchange of personal data, with the European Judicial Training Network (2008), IberRed (2009) and the UNODC(2010).

³² 8. By way of derogation from paragraphs 6 and 7 and without prejudice to Article 24(1), Europol may transmit personal data and classified information which it holds to the entities referred to in paragraph 1 of this Article where the Director considers the transmission of the data to be absolutely necessary to safeguard the essential interests of the Member States concerned within the scope of Europol's objectives or in the interests of preventing imminent danger associated with crime or terrorist offences. The Director shall in all circumstances consider the data-protection level applicable to the body in question with a view to balancing that data-protection level and those interests. The Director shall inform the Management Board and the Joint Supervisory Body as soon as possible of his or her decision and of the basis of the assessment of the adequacy of the level of data protection afforded by the entities concerned.

9. Before the transmission of personal data in accordance with paragraph 8, the Director shall assess the adequacy of the level of data protection afforded by the entities concerned, taking into account all the circumstances relevant to the transmission of personal data, in particular: (a) the nature of the data; (b) the purpose for which the data is intended; (c) the duration of the intended processing; (d) the general or specific data-protection provisions applying to the entity; (e) whether or not the entity has agreed to specific conditions required by Europol concerning the data.

The author wishes to stress that such exceptional transfers have never taken place at Eurojust so far but it is not unthinkable that such a situation, especially in the context of prevention of imminent terrorism attacks, could take place. In that context one should not lose perspective of the fact that freedom, security and justice should go hand in hand and there are some situations in which other considerations might make necessary to exceptionally transfer data to a country where no general data protection regime exists while taking all possible precautions to avoid further dissemination or use of such information transferred.

2.2.5 *Rights of the individuals*

The exercise of the rights of the individuals in the context of the activities of police and justice require as well considering the specific circumstances of every single request and taking into account the state of play of the ongoing investigation or prosecution. It is crucial to consider together the need to ensure guarantee those rights while at the same time not jeopardising the investigations or prosecutions in progress. The following examples aim at calling attention to the complexity of such situations.

2.2.5.1 *Right of information* Articles 10 and 11 of the Directive deal with the information to be given to the data subject at the moment of collection of personal data or, at least, at the time of recording such data.

- One of the typical examples of cases which Eurojust deals with is the so-called “controlled delivery” in which law-enforcement authorities are aware of the fact that a certain vehicle is transporting drugs from one country to another and decide to let that vehicle cross the border without being arrested, to be able to find out where the delivery leads to and possibly get hold of the whole organisation behind the drug trafficking activities. To be able to carry out such an operation, often several surveillance mechanisms are put in place such as telephone tapping, devices to follow the vehicle and so forth, on the basis of the required authorisation of the judicial authorities of the countries involved. Needless to say, it is by all means impossible to inform the data subject in advance or at the time of recording of such processing operation/s without jeopardising the investigation.
- A similar example is the case of telephone tapping, a not uncommon practice in preliminary phases of an investigation, in which obviously information can not be given to the data subject/s at the moment in which the telephone interception has been authorised by the judicial authorities. One could even wonder if it is reasonable, as it seems to be the case under German legislation, to inform all people who have called or who have been called by a certain person of the fact that their conversations were tapped in the course of an investigation at a later stage, even if this investigation led to no action by the judicial authorities. The fact that persons would receive notice that the telephone of somebody they knew was at a certain moment tapped in the course of an investigation could have substantially negative impact on the reputation of that person, even if the investigation did not have any judicial consequence for the person as such.

2.2.5.2 Right of access to personal data Articles 12 and 13 of the Directive deal with the issue of access to personal data. In the practice of international investigations, the sole fact of confirming that a certain authority has data on one person can have a negative impact on ongoing investigations.

For instance, if a person receives confirmation of the fact that Eurojust processed information on him/her, he/she receives *de facto* confirmation of the existence of an ongoing international investigation regarding him/her and possibly, where relevant, regarding the organisation in which he/she operates and this might lead to a change of pattern of actions of the organisation, jeopardising the ongoing investigation. In practice, exceptions are used relatively often and practices such as indirect access are fairly common in the former third pillar sector and are still allowed in the context of the third pillar framework decision.³³

The Eurojust Decision contains in its article 19.7 a provision dealing with the cases in which access is denied or when no personal data concerning the applicant are processed by Eurojust: in such a case Eurojust shall just notify the applicant that it has carried out checks, without giving any information which could reveal whether or not the applicant is known. Needless to say, the applicant has the right to appeal to the Joint Supervisory Body, which shall verify if Eurojust has correctly applied the rules regarding rights of the individuals.

2.2.5.3 Right to object It seems quite obvious why article 14 of the Directive, dealing with the right of the data subject to object to the processing of personal data, could not possibly be implemented in the third pillar sector.

2.2.6 Conclusion

These are just some examples related to areas in which the general existing rules for processing of personal data in the former first pillar require adjustment to the reality of the work of the law enforcement sector but this section does by no mean intends to be exhaustive. One could surely think of other issues requiring additional attention such as the processing of sensitive data, data quality, data security and so forth. The Krakow declaration mentioned a total of 13 issues in which the standard of data protection of the Directive needed to be further detailed and particular attention was needed.

The rules of procedure on the processing and protection of personal data at Eurojust³⁴ are a good example of third pillar rules which were drafted taking full account

³³See in that respect recital 29 of the preamble to this instrument: *Some Member States have provided for the right of access of the data subject in criminal matters through a system where the national supervisory authority, in place of the data subject, has access to all the personal data related to the data subject without any restriction and may also rectify, erase or update inaccurate data. In such a case of indirect access, the national law of those Member States may provide that the national supervisory authority will inform the data subject only that all the necessary verifications have taken place. However, those Member States also provide for possibilities of direct access for the data subject in specific cases, such as access to judicial records, in order to obtain copies of own criminal records or of documents relating to own hearings by the police services.*

³⁴See footnote number 13.

of the provisions of the Directive but also of the mandate and the activities which Eurojust has to perform to achieve its tasks in the field of judicial cooperation and coordination.

3 Need for specialised effective supervision

3.1 The present discussion

At present a joint supervisory body is supervising and monitoring compliance with the existing data protection rules at Europol, Eurojust and the Schengen Information System. While some seems to imply that the entry into force of the Treaty of Lisbon should automatically imply the disappearance of such supervisory bodies and their replacement by the European Data Protection Supervisor, the author of this article, with due respect for the EDPS, fails to see reasons justifying such change.

On several occasions, the European data protection authorities assessing developments in the area of law enforcement stressed the need for effective supervision in the law enforcement field.³⁵ It is therefore necessary to evaluate which system offers the best and most efficient supervision in this field and not to run into hasty conclusions based in no other argument than the legal possibility to change the existing system under the Lisbon regime. It might also be relevant to mention in that context that the Lisbon Treaty does not give the European Data Protection Supervisor the status of EU institution, as it is for instance the case for the Ombudsman, so assuming that the EDPS must in all cases be the solution for supervision for all EU information systems might be premature, as it has been put in evidence by the recent discussion in the context of the Customs Information System.

A couple of years ago, a related discussion took place based on the proposal of the German presidency, in the framework of the negotiations on the draft framework decision on data protection in the field of police and justice, to replace the various existing joint supervisory bodies by one single JSB. Such proposal ended fully disappearing from the text of the legal instrument although a declaration was adopted which merely indicated the possibility of studying such possibility in the future. In that context however the EDPS commented on the German proposal in his third opinion on the framework decision,³⁶ indicating that although such proposal might see logical, *at this moment there is no immediate need for such a new supervisory body. The supervision itself functions satisfactorily.* Replacement of the existing JSBs by another supervisor would therefore not be done based on the need for effective protection and compliance.

³⁵See for example the position paper of the Spring Conference on law enforcement and information exchange (Krakow 25th–26th April 2005), the opinion of this conference on the DPFD (Brussels, 24th January 2006) and the Opinion 3/2006 of the WP 29 on the Directive 2006/24/EC.

³⁶Third opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters (2007/C 139/01), published in the *Official Journal of the European Union* C 139/1, 23.6.2007.

Some of the declarations and documents issued by the Data Commissioners Conference during the last years have underlined the wish of the Data Protection Authorities to have systems of supervision in which the national involvement is respected. For instance, the Krakow declaration mentions the following: *It will be essential to develop a system of effective supervision in which all Member States participate*. The Edinburgh declaration³⁷ provided a very substantial document dealing with inspections and supervision in the police and justice sector carried out commonly by the Data Protection Authorities, providing the following interesting remarks:

The need and importance for the cooperation and joint activities of national data protection authorities in the EU IIIrd pillar was emphasized by establishment of the joint supervisory authorities such as Schengen Joint Supervisory Authority, Europol Joint Supervisory Body, Eurojust Joint Supervisory Body, Customs Joint Supervisory Authority, in order to ensure joint independent control and monitoring of the data processing in the IIIrd pillar and protection of the rights of the individuals. Even when the Lisbon Treaty creating amendments of the existing EU Treaties will enter into force, this will not change the need for such cooperation. The experiences with the joint inspections of the use of the Schengen information system, the coordinated inspection of Eurodac, the joint inspections at Eurojust and Europol and the initiatives taken by the Europol Joint Supervisory Body demonstrate the added value of a common approach.

Indeed, the experience during the last ten years of common inspections carried out at Europol, Eurojust and the SIS, with involvement of various experts from the Data Protection Authorities and with the indispensable support of the Data Protection Secretariat of the Council of the European Union, has been extremely appreciated and positively evaluated by all involved parties. It is further not strange that the Member States wish to have their independent DPAs participating to the inspections and supervision of systems which process personal data originated from their own national authorities. In that context it is relevant to mention that the data processed by Eurojust is provided by the national judicial authorities and that a very similar situation occurs at Europol where there is in any case a part of the data which remains under the national regime.

The recent document of the Working Party 29 and the Working Party on Police does not make any specific proposals regarding supervision. It only mentions that *independent supervision, as well as judicial oversight and remedies should be properly addressed. This includes in any event adequate resources and competences for independent supervision*.

3.2 The example of Eurojust

The compliance with Eurojust data protection regime is supervised internally by the Data Protection Officer, as regulated in Article 17 of the Eurojust Decision, but there is also an independent external supervisor, the Joint Supervisory Body. This body,

³⁷Data Protection Catalogue on Cooperation and Supervision in the area of Law Enforcement in Europe, adopted by the Spring Conference 2009, in Edinburgh.

composed of judges or members with an equal level of independence³⁸ nominated by the Member States, has a very important task *ensuring that the processing of personal data is carried out in accordance with this Decision* [the Eurojust Decision].³⁹

The JSB of Eurojust operates with a troika system, allowing the body to work in a very efficient and non bureaucratic way. Following a written proposal of the JSB addressed to the Council by letter of its chair including its opinion of 3 March 2008,⁴⁰ the revised Eurojust Decision⁴¹ modified the system of representation in the troika by replacing the link to the EU presidencies by a system of annual election at the plenary meeting of the JSB in which a new member is chosen between the appointees of the Member States for a period of three years.⁴² This new system should allow for more continuity and expertise in the JSB as members will have more time to be acquainted with the work of Eurojust and to build expertise in that regard. On 23 June 2009, at its first plenary meeting after the entry into force of the new Eurojust Decision, the JSB approved in its usual line of efficiency its new rules of procedure⁴³ and held its first election replacing the whole troika at once by three new members. The new Decision also adds a new sentence in paragraph 10 of Article 23 allowing the possibility for the JSB secretariat to rely on the expertise of the data protection secretariat at the Council.⁴⁴ This paragraph, supported by the JSB in its letter to the Council of March 2004 as well as by the EDPS in its opinion,⁴⁵ constitutes a legal basis for the so-far only informal cooperation with this secretariat, which had proved to be very useful in the past for the inspections carried out by the JSB in cooperation with this Secretariat and with involvement of experts of the national Data Protection Authorities.

³⁸In practice a good part of the Member States have appointed Data Protection Commissioners, as people with a clear independent status. The combination of judges, with expertise in the judicial field, with data protection experts has shown to be fruitful and efficient in this body.

³⁹See Article 23.1 of the Eurojust Decision.

⁴⁰Opinion of the Joint Supervisory Body of Eurojust on the opportunity to amend article 23 of the Eurojust Decision regarding the composition of this body, of 3 March 2008: *The Joint Supervisory Body appreciates the fact that the composition of this body by three members is a very workable construction facilitating its operation and quick decision making process and it is also a non bureaucratic and cost effective structure. It regrets however that the very frequent changes of members every six months and the short length of the participation in the troika of Eurojust for only eighteen months, makes it difficult to keep a high level of knowledge of the Eurojust complex legal and technical framework, its organisation and the state of play regarding the many developments at Eurojust having impact on the protection of personal data. It therefore considers that a more permanent structure would be beneficial, while keeping the reduced size and efficient operation of the body.*

⁴¹For more information on the modifications included in this Decision see Alonso Blas [2].

⁴²The length of the appointment to the JSB has been modified accordingly in paragraph 1 of the article from the initial 18 months of participation to the troika to three years.

⁴³See http://www.eurojust.europa.eu/official_documents/Joint_Supervisory_Body_ACT/Act-JSB-Eurojust-23June2009-en.pdf.

⁴⁴The Secretariat established by Council Decision 2000/641/JHA of 17 October 2000 establishing a secretariat for the joint supervisory data protection bodies set up by the Convention on the establishment of the European Police Office (Europol Convention), the Convention on the Use of Information Technology for Customs Purposes and the Convention implementing the Schengen Agreement on the gradual abolition of checks at the common borders (Schengen Convention), OJ L 271, 24.10.2000, p. 1.

⁴⁵Opinion of the European Data Protection Supervisor of 25 April 2008 on the review of the Eurojust Decision.

The good working of the system of supervision at Eurojust and the quality of the protection offered had in the past been remarked by the European Data Protection Supervision. In its already mentioned opinion on the revised Eurojust Decision, the EDPS stated the following:

Decision 2002/187/JHA includes extensive provisions in order to ensure compliance with the data protection requirements applicable to Eurojust. Article 17 deals with the Data Protection Officer within Eurojust, whereas Article 23 establishes a Joint Supervisory Body that shall monitor the activities of Eurojust collectively. The initiative does not propose fundamental changes to these provisions which seem to function well. Only one small addition is proposed as regards Article 23(10) which states that the secretariat of the Supervisory Body may rely upon the expertise of the secretariat established by the Council Decision 2000/641/JHA (22). The EDPS welcomes this addition which could foster the consistency of the supervision of data protection within the area of police and judicial co-operation in criminal matters (present third pillar). Using the experiences with other EU bodies and large scale information systems could not have any other effect than further improving the quality of the protection.

A number of reasons make the JSB of Eurojust function so well:⁴⁶

- In the first place, the combination of data protection knowledge and understanding of the “business” of Eurojust is essential. The members of the JSB are either judges or Data Commissioners (and in some cases both things at the same time) which provides them an excellent understanding of the data protection issues in the context of the judicial activities, being fully aware of all relevant considerations involved when dealing with Mutual Legal Assistance, European Arrest Warrants and so forth.
- The JSB meets regularly, in any case four times a year and often a study visit and/or inspection take place, and its meetings take place at Eurojust, allowing them to dedicate a part of their meetings to exchange views with the Eurojust College or administration regarding developments in the organisation and to hold a closed part for their own discussion. In such a way the JSB is always fully informed of all ongoing matters with any data protection relevance and can advise timely and with full information the organisation.
- Its limited size is surely an important element to facilitate the functioning of the body, allowing it also to operate with a very limited budget. In the last year (2009) the JSB spent about 40.000 euros from its budget line to carry out its activities.
- The Secretariat of the JSB is held within Eurojust, permitting it to ensure full communication and cooperation with all Eurojust postholders.
- Last but not least, the JSB holds frequent and regular inspections, covering both the case-related and the non case-related (administrative) processing operations of Eurojust and delivers very extensive and detailed reports of such inspection, including findings and recommendations, whose follow-up by the organisation is monitored

⁴⁶The annual reports of activities of the JSB are available at http://www.eurojust.europa.eu/press_annual_jsb.htm.

in the following meetings. Where necessary, additional inspections dedicated to single matters or issues, are planned.

Finally, it is relevant to mention that the JSB of Eurojust liaises frequently with the other existing JSBs, attends the joint meetings organised with those and consults them when matters of common interest are being dealt with. In that context the author wishes to refer to the meeting of the chairs of all the JSBs which took place in Brussels on 16 December 2009 and where the need to maintain such specialised, experienced and knowledge-based supervision was stressed by all participants.

3.3 Conclusion

The existing systems of supervision through JSBs at Eurojust, Europol and SIS are working well, efficiently and have built through the years a very extensive and valuable expertise carrying out joint inspections using common standards and with the assistance of experts from the national Data Protection Authorities.

The author of this article would therefore plead for the maintenance of the existing good working systems. Any consideration of a possible change in those systems should only take place on the basis of a thorough analysis showing the added-value of any envisaged amendment.

Experience shows that frequent and extensive inspections are of crucial importance in such a sensitive area of data protection; the record of inspections and on the spot checks of any envisaged supervisor, the EDPS or any other possible alternative, should be thoroughly considered in order to ensure that the existing high level of protection and compliance can be maintained and ideally even further improved.

4 Some brief political considerations

The Treaty of Lisbon offers some positive perspectives for the future by introducing co-decision procedures and replacing the requirement of unanimity by qualified majority, allowing hopefully for a higher level of protection to be achieved regarding data protection in the police and justice sector in future EU general instruments.

The latest developments in the European Parliament⁴⁷ as well as the very strong and well put statements of Commissioner Reding⁴⁸ regarding data protection allow us some optimism regarding the future of this fundamental right. However, the experience from the last years, and in particular that of the negotiations regarding the framework decision, should not be forgotten and over optimism should be avoided.

The Member States have adopted, with unanimity, a whole range of instruments during the last couple of years which showed their willingness to maintain the existing former third pillar regimes as they are (revised Eurojust and Europol decision, both just entered into force and under national implementation) and their limited wish

⁴⁷On 11 February 2010, the European Parliament rejected the interim EU-US agreement on the processing and transfer of financial messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Programme on data protection grounds.

⁴⁸See footnote 23.

to create a common high level protection framework for the field of police and justice (the framework decision, which is still under implementation). Those instruments remain valid until they are amended or repealed and give a clear and reliable idea of how Member States think in this context. This can not be disregarded or underestimated and it would be in the opinion of the author not serious in the direction of the Member States to start working on the replacement of an instrument/s which the Member States have not even had the time to implement.

5 The future will tell

As stated in the introduction to this article, Article 16 TFEU offers a legal basis which could be used to introduce an EU general instrument regulating data protection in all sectors of activities and imposing general rules for all those.

Other options are however also possible, such as the coexistence of various instruments, being those which already exist or updating and improving in the future the main instruments in the former first and third pillars: the Directive and the Framework Decision.

Several possibilities could possibly work. However, on the basis of specific nature and sensitivity of the processing operations in the fields of police and justice, the author of this article strongly pleads for allowing tailor made rules for the operations in this field and, where available, for maintaining in place the existing systems of specialised supervision building further on a very extensive and valuable expertise developed by those and allowing therefore the national Data Protection Authorities to continue playing a role in this context, given the fact that the personal data processed are of national origin and will be used at national level for investigations or prosecutions.

In any case, any decisions at EU level should be taken on the basis of evaluation of the working of the existing legal rules and of the efficiency of the supervision mechanisms in place. It would be good to invest efforts in addressing the areas where gaps exist instead of reinventing the wheel in areas where data protection is being respected and complied with. People whose personal data are being processed in the context of an ongoing investigation or prosecution are in a most vulnerable position and the effective protection of their rights should be the driving force for any change proposed, not just institutional considerations which do not necessarily imply improvements for the data subjects. Harmonisation should not take place just for the sake of it, it should bring positive results for our citizens in terms of freedom, security and justice.

References

1. Alonso Blas, D.: First pillar and third pillar: need for a common approach on data protection? In: Gutwirth, S., Reinventing Data Protection? pp. 225–237. Springer, Berlin (2009). doi:[10.1007/978-1-4020-9498-9_13](https://doi.org/10.1007/978-1-4020-9498-9_13)
2. Alonso Blas, D.: The new Council Decision strengthening the role of Eurojust: does it also strengthen data protection at Eurojust? In: Gutwirth, S., et al. (eds.) *Data Protection in a Profiled World?* (2010)
3. Hijmans, H., Scirocco, A.: Shortcomings in EU data protection in the Third and the Second Pillars, Can the Lisbon Treaty be expected to help? *Common Mark. Law Rev.* **46**(5), 1485–1525 (2009)