EUROPEAN PARLIAMENT

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C
CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

Constitutional Affairs

Justice, Freedom and Security

Gender Equality

Legal and Parliamentary Affairs

Petitions

The data protection regime applying to the inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area

Study for the LIBE Committee

EN

2014

DIRECTORATE GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C: CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS

The data protection regime applying to the inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area

STUDY

Abstract

Upon request by the LIBE Committee, this study aims at identifying data protection shortcomings in the inter-agency cooperation in the EU criminal justice and law enforcement area. Its objective is also to outline, under six possible scenarios, the interplay among the data protection legal instruments currently being discussed, as well as the response each scenario could provide to such shortcomings.

PE 510.001 EN

DOCUMENT REQUESTED BY THE
COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS

AUTHORS

Prof. Paul de Hert, Vrije Universiteit Brussel, VUB

Dr. Vagelis Papakonstantinou, Vrije Universiteit Brussel, VUB

RESPONSIBLE ADMINISTRATOR

Mr Alessandro DAVOLI
Policy Department C - Citizens' Rights and Constitutional Affairs
European Parliament
B-1047 Brussels
E-mail: poldep-citizens@ep.europa.eu

Editorial assistant
Ms. Lucia-Cristina ACHIHAEI

LINGUISTIC VERSIONS

Original: EN

ABOUT THE EDITOR

Policy Departments provide in-house and external expertise to support EP committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny.

To contact the Policy Department or to subscribe to its monthly newsletter please write to:
poldep-citizens@ep.europa.eu

European Parliament, manuscript completed in November 2014.

This document is available on the Internet at:
http://www.europarl.europa.eu/studies

DISCLAIMER

CONTENTS

EXECUTIVE SUMMARY

From a data protection perspective, fragmentation is the main characteristic of the legal framework in place in the agencies in the EU criminal justice and law enforcement area. A multitude of EU agencies operates under their own individual legal framework with little regard for harmonization, consistency or even compatibility among their personal data processing, while the basic text that would supposedly set the common standard in the field, the Data Protection Framework Decision, expressly excuses itself from assuming this role. Each one of the EU bodies and agencies operating within the EU criminal justice and law enforcement area is until today governed by its own legal constituting text(s) that customarily address data protection issues but however does so in a piecemeal and introverted way: supervision of data protection practices is vested upon each agency's internal mechanisms and management. This architecture, that reflects the pre-Lisbon third pillar environment, has been preserved until today, despite of the fact that in the meantime inter-agency cooperation has proliferated: not only have formal bilateral cooperation agreements been entered among all EU agencies but also cooperation takes place outside EU borders as well, through chartered, or unchartered, personal data exchanges with third countries and international organisations. Adequate data protection supervision, in the sense of a single, coordinated monitoring authority, is emphatically missing from all such exchanges.

The ratification of the Treaty of Lisbon is a milestone that affected the EU criminal justice and law enforcement area in more than one way. Among others, the culmination of a standalone individual right to data protection and the involvement of the European Parliament in any decision-making in the field are crucial factors that enabled an, admittedly much needed, change. Such change came in the form of a series of Commission proposals that were released over the past couple of years and which, if implemented, will completely restructure the current EU data protection architecture in the criminal justice and law enforcement area. The Commission proposals originate from Article 16 TFEU, which introduces a new right to data protection and requires new rules on the personal data processing by EU agencies, as well as independent monitoring, but also from Declaration 21, which allows for "specific rules" in the field. To this end, the Commission introduced both general and agency-specific texts. At a general level, a Police and Criminal Justice Data Protection Directive is intended to replace the Data Protection Framework Decision. At agency-specific level, the Europol and Eurojust draft Regulations are intended to replace the respective Decisions in force today; at the same time a new Regulation is aimed at introducing the European Public Prosecutor's Office (EPPO) while work has been promised by the Commission also on amending Regulation 45/2001.

Such law-making process entails herculean efforts by all the bodies involved in it (the Commission, the Parliament and the Council) in order to keep the overhaul of data protection rules in force today (in the EU criminal justice and law enforcement field) synchronized and coordinated. Although none of the above legislative proposals is yet finalized (in fact, only one has reached "trilogue" stage), the Commission's preferred data protection architecture has become by now evident: the draft Directive is to replace the Framework Decision but not to affect any agency-specific personal data processing. This task will be undertaken by Regulation 45/2001 (or its successor) and the European Data Protection Supervisor (EDPS). This architecture is basically taken for granted for the purposes of this analysis: regardless of its merits or drawbacks, other than the Commission also the Parliament has shown no substantial objection to it. Therefore, the interplay of the instruments involved (the Police and Criminal Justice Data Protection Directive, Regulation 45/2001 or its successor, the Europol, Eurojust and EPPO Regulations) has been attempted to be sketched

in the six different scenarios that follow, each in turn assessed in terms of legal and pragmatic plausibility under the current environment:

- A "*unified model*" scenario, under which the Police and Criminal Justice Data Protection Directive would regulate all the EU criminal justice and law enforcement area (including therefore the EU agencies operating therein);
- A "*segregated model*" scenario, whereby the Police and Criminal Justice Data Protection Directive would leave EU agencies' personal data processing outside of its scope (as is currently the situation under the Data Protection Framework Decision);
- An "*interim segregated model*" scenario, under which the above segregated approach would only last for a few years, after which EU agencies would have to bring their personal data processing under the Police and Criminal Justice Data Protection Directive;
- An "*alternative unified model*" scenario, that, as originally suggested by the Commission, would use Regulation 45/2001 as a common standard-setting text for all EU agencies, whose individual constituting legal instruments would subsequently supplement and further specify its provisions;
- A scenario whereby the current architecture is preserved and consequently neither the Police and Criminal Justice Data Protection Directive nor Regulation 45/2001 (or its successor) affect in any way the agency-specific (revised) texts, and
- An, unfortunately likely for the immediate future, scenario, whereby Regulation 45/2001 is not amended in time and all of Europol, Eurojust and EPPO Regulations, when adopted, will supplement and further specify its provisions, which are outdated and unsuitable for the criminal justice and law enforcement area.

1. THE DATA PROTECTION SCENE IN THE EU CRIMINAL JUSTICE AND LAW ENFORCEMENT AREA: LEGAL FRAMEWORK, EU AGENCIES AND BODIES, INTER-AGENCY COOPERATION AND OTHER IMPORTANT FACTORS OF INFLUENCE

KEY FINDINGS

- Fragmentation is the main characteristic of the data protection legal framework in force in the EU agencies in the criminal justice and law enforcement area: a multitude of agencies operates under their own, individual legal framework with little regard for harmonization or even compatibility among their personal data processing while the basic text that would supposedly set the common standard in the field, the Data Protection Framework Decision, expressly excuses itself from assuming this role.
- Today practically the whole EU criminal justice and law enforcement data protection architecture is under regulatory restructure. Not only are the basic data protection texts (the EU Data Protection Directive and the Data Protection Framework Decision) in the process of being replaced but also agency-specific basic regulatory texts are being reviewed (the Europol and Eurojust Decision respectively) while new agencies (the EPPO) or mechanisms (the European e-Justice Portal) are in the process of being established.
- Inter-agency cooperation in the form of personal data flows, while well-established both through relevant inter-agency agreements and in practice, largely takes place unmonitored by any (single or coordinated) data protection mechanism; Cooperation with third countries remains to-date largely unchartered and is therefore even less susceptible of data protection monitoring.

1.1. Setting the scene: the data protection legal framework and institutions in the EU criminal justice and law enforcement area

KEY FINDINGS

- While Article 16 TFEU established an independent individual right to data protection and asked for new rules on personal data processing by EU agencies as well as for compliance to be controlled by "*independent authorities*", Declaration 21 justifies "*specific rules*" in the field of judicial cooperation in criminal matters and police cooperation.
- The Data Protection Framework Decision failed to create a harmonised EU personal data processing environment in the criminal justice and law enforcement area, is inadequate within the Article 16 TFEU meaning, and is in the process of being replaced by a Police and Criminal Justice Data Protection Directive.
- Regulation 45/2001, establishing the EDPS and introducing rules on EU bodies' personal data processing, is an old first-pillar instrument that does not apply to the

(operational) processing of EU agencies in the criminal justice and law enforcement area. While the Commission has announced its amendment, nothing has become to date known on this matter.

- The Europol legal framework in force is not compatible with Article 16 TFEU because, among others, it does not allow for "*independent*" data protection monitoring either by Europol's Data Protection Officer or its Joint Supervisory Body (JSB). Under the draft Commission proposal for a Europol Regulation the EDPS will be competent for the supervision of processing of personal data by Europol under a model of coordinated supervision with Member States' Data Protection Authorities.
- The Eurojust legal framework in force is not compatible with Article 16 TFEU because, as in the case of Europol, it does not allow for "*independent*" data protection monitoring by its JSB. Under the draft Commission proposal for a Eurojust Regulation the EDPS will be made responsible for supervision of all Eurojust personal data processing (presumably at a more direct level than in the case of Europol, a differentiated treatment that appears hard to explain).
- The EPPO, whenever established, is suggested by the Commission to have a special relationship with Eurojust (as also required by Art. 86 TFEU) and therefore, in the same context as in Eurojust, all its personal data processing is to be monitored by the EDPS.

If approached from a data protection perspective, fragmentation is the main characteristic of the legal framework in force in the EU agencies in the criminal justice and law enforcement area. As it will be evidenced in the analysis that follows, a multitude of EU agencies operates under their own, individual legal framework with little regard for harmonization, consistency or even compatibility among their personal data processing practices. The basic text that would supposedly set the common standard in the criminal justice and law enforcement area, the Data Protection Framework Decision, expressly excuses itself from assuming this role. This patchwork of legal (data protection) provisions and applicable models was perhaps to be expected given the origins of the EU agencies and bodies involved: each one emerged out of sector-specific needs and was forged under the constant developments in such basic EU notions as harmonization, enlargement and constitutionalism. However, despite such fragmentation, allegedly the data protection model at hand has been, and still is, a working model – an important finding that sets the bar for attempts to replace or amend it.

The coming into effect of the Treaty of Lisbon is a milestone that affected the field in more than one way. First and foremost, it placed an individual right to data protection in the list of basic EU fundamental rights. This upgrade demands concrete actions in the form of new law-making and review of the whole EU data protection edifice. Second, it abolished the pillar system, bringing old incompatibilities (eg. first pillar organisations onto third pillar institutions) to an end. Third, it upgraded the role of the European Parliament. Other relevant effects include the potential exemption for law enforcement and security agencies, the establishment of the EPPO, or the possibility of the EU to ratify the ECHR. All of the above suggests a review of the data protection architecture of the EU criminal justice and law enforcement area.

Such review came in the form of a series of important European Commission proposals released over the past few years. Today practically the whole EU criminal justice and law enforcement area is under regulatory restructure. Not only are the basic data protection texts under revision, as it will be shown under section 2 of this study, but also the agency-specific basic regulatory texts are also being reviewed. While the situation is still in flux,

with some texts having reached a final ("trilogue") phase and others still at Commission proposal level, for the purposes of this analysis attention will be given to the formal, finalized, texts at hand that, although unlikely to become final in their current wording, do reveal general guiding principles and law-making intentions.

The analysis that follows constitutes an attempt to map the field. After a brief review of the general legal framework, EU agencies and bodies are examined separately with a particular emphasis upon their applicable data protection legal regime and (data protection) cooperation among them.

1.1.1. The legal framework: Article 16 and Declaration 21 TFEU; the Data Protectio Framework Decision; Regulation 45/2001

Article 16 TFEU constitutes a central development in EU data protection, because it established an independent individual right to data protection, separate from any other right:

> "***Article 16****. 1. Everyone has the right to the protection of personal data concerning them. 2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities*".[1]

It is essentially these provisions that triggered the EU data protection overhaul currently under way, both horizontally (the EU data protection reform package, discussed below under 2) and the agency-specific new draft regulatory texts (in particular for Europol and Eurojust – see the analysis that follows).

However, of equal importance, at least to the purposes of this analysis, is Declaration 21 of the same Treaty:

> "***21. Declaration on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation.*** *The Conference acknowledges that specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 of the Treaty on the Functioning of the European Union may prove necessary because of the specific nature of these fields*".

Consequently, at the highest possible level is the criminal justice and law enforcement area, first, separated from any other personal data processing, and, second, awarded with the possibility to benefit from specific rules, fitted to its particular needs and purposes. Although such express exemption invites taking advantage of it, the Treaty's actual wording remains important: the field "may", but equally "may not", have special data protection rules applying to it.

The uniqueness of the criminal justice and law enforcement area was first formally acknowledged in the Data Protection Framework Decision "*on the protection of personal*

[1] See also Article 8 of the EU Charter of Fundamental Rights.

data processed in the framework of police and judicial cooperation in criminal matters"[2]. Such acknowledgement was admittedly inevitable, given the "pillar" EU system then in effect; despite however this structural necessity, the need to provide for special data processing rules to police and criminal justice work is made more than once evident in the Decision's actual text. In fact, the Data Protection Framework Decision failed to justify its title in a number of ways: with regard to harmonization, at Member State level it adopted a peculiar, to say the least, distinction in its scope that allowed Member States to continue applying their own national rules in the fields concerned.[3] It also allowed to any of their bilateral agreements with third countries to remain, regardless of the personal data processing they allow.[4] At EU agency level, the Data Protection Framework Decision expressly excuses itself from any attempt to affect the data protection provisions of, among others, the agencies that would otherwise fall within its scope (in the sense that they are involved in "*police and judicial cooperation in criminal matters*").[5] Even from a substantial law point of view the Framework Decision fails to justify its "*data protection*" naming, in the sense that basic data protection principles, enshrined not only in the EU Data Protection Directive[6] but also in Convention 108 of the Council of Europe[7], are watered down and weakened in its wording.[8]

The failure of the Data Protection Framework Decision to assume a standard-setting role in the pre-Lisbon EU law enforcement area (then, Third Pillar) in the same way that the Data Protection Directive had accomplished for all other personal data processing (then, First Pillar) may perhaps be explained by the fact that it came relatively late (in 2008) and at any event long after EU agencies and Member States had created their own rules in the fields concerned and in the framework of law enforcement measures proposed after the Madrid and London attacks. In addition, the fact that it essentially is a pre-Lisbon Council instrument that had to achieve unanimity among Member States and conform to the pillar system, is also of relevance. The Commission itself has expressly acknowledged that the limited scope of the Data Protection Framework Decision already leads to legal and practical deficiencies for the protection of personal data at EU level and leads to different levels of data protection in different Member States. It has also created legal uncertainty – both for data subjects and for competent authorities as to which rules should apply when personal data are processed by police and judicial authorities.[9] At any event, its shortcomings are

[2] Council Framework Decision 2008/977/JHA of 27 November 2008, OJ L 350/60, 30.12.2008 (the "*Data Protection Framework Decision*").
[3] Data Protection Framework Decision, Art. 1. On this distinction the European Commission commented that "*this distinction is difficult to make in practice: personal data which have been gathered in a purely domestic context can hardly be factually distinguished from data that have been subject to cross-border transmission*", European Commission Impact Assessment of the Data Protection Framework Decision (Annex 3), http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_annexes_en.pdf. See also 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 Market Law Review, Vol. 46, 2009, p.1494.
[4] Data Protection Framework Decision, Art. 26.
[5] Data Protection Framework Decision, Art. 28.
[6] 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 L 281 , 23/11/1995 (the "*Data Protection Directive*").
[7] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.1.1981 (the "*Convention 108*").
[8] See, for instance, Data Protection Framework Decision, Art. 3, 6 or 17. On the Data Protection Framework Decision shortcomings see, for instance, De Hert P/Papakonstantinou V, "The Data Protection Framework Decision of 27 November 2008 Regarding Police and Judicial Cooperation in Criminal Matters - A Modest Achievement However Not the Improvement Some Have Hoped for," *Computer Law & Security Review* 25 (2009): 403–14.
[9] See European Commission, Impact Assessment of the Data Protection Framework Decision, ibid.

expected to be remedied once the Police and Criminal Justice Data Protection Directive, currently in Commission proposal format, eventually replaces it (see below under 2.1.2).

Given the above, the Data Protection Framework Decision is of limited relevance to the purposes of this analysis: not only does it not affect the EU criminal justice and law enforcement agencies' data protection regime, but it also is currently under replacement. However, two important factors need to be kept in mind: first, its (Council-driven) model that excludes EU criminal justice and law enforcement agencies from its scope – one of the possible future scenarios that will be developed below (under 2.2.2); and, second, its basic underlying concept that the relevant personal data processing in this sector merits a different set of rules than any other type of its kind.

Finally, brief mention ought to be given also to Regulation 45/2001 "*on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data*".[10] Purpose of the Regulation, that was released only when the Treaty required it,[11] is to ensure that Community institutions "*shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data and shall neither restrict nor prohibit the free flow of personal data between themselves or to recipients subject to the national law of the Member States implementing Directive 95/46/EC*".[12] However, Regulation 45/2001, is essentially a first-pillar instrument that is only applicable on personal data processing performed by "*Community institutions and bodies insofar as such processing is carried out in the exercise of activities all or part of which fall within the scope of Community law*".[13] This in practice is interpreted as the Regulation being applicable only on the processing of staff data by the EU criminal justice and law enforcement agencies[14] – a limited approach that, as will be seen later (under 2) is at the same time limiting and unsuitable for the substantial changes brought by article 16 TFEU.

1.1.2. Europol

Europol, the EU law enforcement agency responsible for coordinating the fight against serious international crime and terrorism, was established in 1995 by means of a relevant Convention – the Europol Convention[15], that entered into effect on 1 October 1998. Europol itself became operational on 1 July 1999. The Europol Convention had been amended through altogether three Protocols (in 2000, 2002 and 2003 respectively) and a Council Decision (in 1998), before being itself replaced by a Council Decision entered in 2009[16] that remains in effect today. At the time of its establishment Europol was predominantly aimed at the exchange of information and the provision of analysis in support of criminal investigations. Its initial tasks essentially concerned the gathering, exchange and analysis of information and intelligence on criminal cases. Over the years these competences were expanded to cover a wide range of crimes including illicit drugs or human trafficking to illegal

[10] OJ L 8/1, 12.01.2001.
[11] See Article 286 of the Treaty of Amsterdam.
[12] Art. 1, Regulation 45/2001.
[13] Art. 3, Regulation 45/2001.
[14] See, for instance, Art. 39.6 of the Europol Council Decision.
[15] Convention on the Establishment of a European Police Office, OJ C316 of 27.11.1995,
[16] Council Decision of 6 April 2009 establishing the European Police Office (Europol), OJ L121/37 of 15.5.2009 (the "*Europol Council Decision*").

immigration, intellectual property crime and cybercrime[17]. Liaison between Europol and member States takes place through corresponding national units and liaison officers.

Data protection has evidently been a concern since the agency's establishment: Article 15 of the Europol Convention effectively referred to the Convention 108 provisions as applicable to Europol as well. The same remains true under the Council Decision still in effect today: the principles of Convention 108 are broadly applicable on Europol personal data processing.[18] In addition, a series of case specific provisions particularize the basic data protection rights into the Europol circumstances.[19] With regard to supervision, the same Council Decision appoints a Data Protection Officer, to "*act independently in the performance of his or her duties*",[20] as well as, a Joint Supervisory Body in order to review personal data processing performed by Europol and data transfers to third parties.[21] The Joint Supervisory Body[22] is to be composed of representatives of each Data Protection Authority of Member States.

While the analysis on whether Europol substantive law conforms to the basic EU data protection standards, particularly after ratification of the Lisbon Treaty, exceeds the limits of this analysis,[23] obvious supervision and monitoring issues raised in the text of the Council Decision in effect today refer, among others, to the facts that:

(a) No mention to the European Data Protection Supervisor is made in its text[24],

(b) The Europol Data Protection Officer is not afforded the independence warranties applicable in other EU agencies[25] and also needs to first submit any matter to the Europol management before referring to the Europol Joint Supervisory Body,

(c) The monitoring role of the Joint Supervisory Body is limited and does not apply to all data protection infringements and the JSB can only refer cases to the Management Board of Europol itself,

(d) The Europol JSB does not fulfil the requirements of independence under the Treaties, and

(e) Individuals do not have the right to refer any alleged violation of their data protection rights to the CJEU. Since 1 December 2014 the CJEU has competence to review decisions of Europol, but the extent of this competence is still unclear.

[17] See Europol's operational activities at https://www.europol.europa.eu/content/page/mandate-119.
[18] See Europol Council Decision, Art. 27.
[19] See, for instance, Articles 30, 31 and 32 of the Europol Council Decision.
[20] See Europol Council Decision, Art. 28.
[21] See Europol Council Decision, Art. 34.
[22] See http://europoljsb.consilium.europa.eu/about/members.aspx?lang=en
[23] However, even from a structural point of view data protection difficulties had been highlighted even in 2008: "*The tension arising between the respective responsibilities of the Member States and of Europol. The JSB is concerned only with data held and used by Europol. Data used on Europol's premises for bilateral exchanges belong to the Member States involved and not to Europol; they are therefore not subject to Europol's rules on data protection, or to supervision by the JSB, but they will be subject to the data protection rules of the Member States. Likewise, all the data on Europol's databases come from a Member State. Until inputted into Europol's databases they are the sole responsibility of the Member State, and even after they have been inputted the Member State retains a responsibility*." (UK House of Lords report, EUROPOL: coordinating the fight against serious and organised crime, HL Paper 183, November 2008, p.57).
[24] In fact, any EDPS competence is based on Article 46 (f) (ii) of Regulation 45/2001. Apparently, EDPS competence with regard to Europol activities mostly refers today to the Europol staff (see also Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision establishing the European Police Office (EUROPOL), (COM (2006) 817 final, p.12 p.11).
[25] See Article 24 of Regulation (EC) Nr. 45/2001.

The Lisbon Treaty affected Europol not only indirectly (the Council Decision is said to have been adopted before the end of 2008 expressly in order to avoid the Lisbon Treaty being ratified and coming into force[26]) but also directly, through Article 88 of the Treaty on the Functioning on the European Union (TFEU). Its par. 2 expressly requires that a Regulation be adopted "*in accordance with the ordinary legislative procedure, [that] shall determine Europol's structure, operation, field of action and tasks*". In this context, the Commission presented its proposal for a Regulation on the European Union Agency for Law Enforcement Cooperation and Training (Europol) in early 2013.[27] In turn, the Parliament adopted its first reading on the Commission proposal in February 2014[28] and so did the Council a few months later.[29] The proposal has therefore entered the 'trilogue' stage. From its part, the Europol Joint Supervisory Body reacted to the Commission proposal with very limited enthusiasm.[30]

While a detailed elaboration on the Commission proposal is of limited value to the purposes of this analysis given the diverging approaches on a number of important issues adopted by the Parliament and the Council respectively and the unforeseeable end result of the 'trilogue' currently under way, here only brief mention shall be made to some of its main data protection provisions regarding supervision and cooperation (as per the original Commission proposal):[31]

(a) Rather than referring to Convention 108, a 'self-sufficient' data protection regime setup has been opted for, influenced by the Data Protection Framework Decision and Regulation 45/2001,

(b) The Data Protection Officer's position has been strengthened,

(c) With regard to individual redress, an individual can turn to Europol for compensation for unlawful personal data processing or an action incompatible with the pro-visions of this Regulation,

(d) The European Data Protection Supervisor will be competent for the supervision of processing of personal data by Europol under a model of coordinated supervision with Member States' Data Protection Authorities,

(e) Decisions of the European Data Protection Supervisor shall be brought before the Court of Justice of the European Union.

[26] See UK House of Lords report, ibid, p.15.
[27] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA, COM(2013) 173 final, 27.3.2013 (the "*draft Europol Regulation*").
[28] European Parliament legislative resolution of 25 February 2014 on the proposal for a regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA (COM(2013)0173 – C7-0094/2013 – 2013/0091(COD).
[29] See Note from the Presidency to the Council of the European Union on the Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA, ENFOPOL 142, CODEC 1323, CSC 109, 10033/14, 28 May 2014.
[30] See Joint Supervisory Body of Europol, first (http://europoljsb.consilium.europa.eu/media/257072/13-31%20jsb%20opinion%20on%20europol's%20regulation%20proposal.pdf), second (http://europoljsb.consilium.europa.eu/media/259439/13-56%20second%20jsb%20opinion%20europol%20regulation%201-6-5.pdf) and third (http://europoljsb.consilium.europa.eu/media/266161/jsb%27s%20third%20opinion.pdf) Opinions.
[31] See also the relevant Commission list found at pp.8-9 of its original proposal.

1.1.3. Eurojust

Eurojust was established in 2002 by virtue of the 2002/187/JHA Decision[32] in order to enhance the effectiveness of the competent judicial authorities of the Member States when dealing with the investigation and prosecution of serious cross-border and organised crime.[33] Eurojust's main role is to promote cooperation and coordination among such authorities when they are involved in investigations and prosecutions of "*serious cross-border criminal cases*", which might include, among others, drug trafficking, counterfeiting, environmental crime or terrorism.[34] In particular Eurojust facilitates international mutual legal assistance and the implementation of extradition requests. However, Eurojust was set up without itself having the power to initiate an investigation or to request national authorities in a binding manner to take procedural steps; in fact, it has been found that the "*the institutional framework drawn up by the 2002 Decision stands out as a genuine embodiment of the concept of the third pillar; one representing an intergovernmental-style structure where there is no attempt to approximate the standing of the national members or even to lay a common set of minimum powers so that national members could enjoy equal footing when exercising their competencies*".[35] This finding, that remains relevant until today, constitutes an important policy option that ought to be examined in parallel both with discussions on the establishment of the European Public Prosecutor (see the analysis that follows) and the Commission proposal for a Directive (see below, under 2.1.2). Like Europol, Eurojust has its headquarters in The Hague. Each EU Member State is expected to appoint a national member at Eurojust that may be either a prosecutor, a judge or a police officer with equivalent competences – this judicial element is of critical importance also for the data protection purposes relevant to this analysis. In order to carry out its tasks, Eurojust maintains "privileged" relations with the EJN, Europol, OLAF and Frontex.[36]

The Eurojust Decision has been amended twice since its adoption, in 2003 and in 2008.[37] The 2008 amendment[38], among others, formalizes the relationship between Eurojust and Member States, by means of placing upon the latter an obligation to transmit information to Eurojust (in its Article 13), as well as, encourages the cooperation with other EU bodies, through appropriate agreements or working arrangements, and third states and other organisations (in particular, Interpol).[39] However, any relevant agreement for the exchange of information ought to be consulted with the Eurojust Joint Supervisory Body. In general, the 2008 amendment did not take into consideration the Treaty of Lisbon, not yet in force at that time, and did not consequently accommodate any of its ideas in its text.[40]

Data protection supervision and cooperation difficulties within the Eurojust regime refer to:

[32] Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (2002/187/JHA), OJ L 63/1, 6.3.2002 (the "Eurojust Decision"). All article references will be made with regard to its consolidated version, 5347/3/09 REV 3, 15 July 2009.
[33] See also European Parliament, The future of Eurojust, Study for the LIBE Committee, 2012, pp.13ff.
[34] See Eurojust website, at http://www.eurojust.europa.eu.
[35] European Parliament, The future of Eurojust, p.20.
[36] Information, with relevant links, available at the Eurojust website (http://ec.europa.eu/justice/criminal/judicial-cooperation/eurojust/index_en.htm).
[37] See European Parliament, The future of Eurojust,, pp.25ff.
[38] Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime OJ 2009 L 138/14.
[39] See also Blas D A, *The New Council Decision Strengthening the Role of Eurojust: Does it also Strengthen Data Protection at Eurojust?* in Gutwirth S/Poullet Y/De Hert P, Data Protection in a Profiled World, Springer, 2010, pp.193ff.
[40] See European Parliament, The future of Eurojust, p.35.

(a) Lack of accountability towards other EU institutions or individual suspects in the processing of whose personal data Eurojust has been involved[41],

(b) The EDPS has only a consultative function and no formal supervisory role over Eurojust personal data processing.

The Lisbon Treaty expressly refers to Eurojust: Article 85 TFEU defines its mission, "*to support and strengthen coordination and cooperation between national investigating and prosecuting authorities in relation to serious crime affecting two or more Member States* […]" while in Article 86 TFEU it is stated "*in order to combat crimes affecting the financial interests of the Union, the Council, by means of regulations adopted in accordance with a special legislative procedure, may establish a European Public Prosecutor's Office from Eurojust*". In this context on 17 July 2013 the European Commission presented a "Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Criminal Justice Cooperation (Eurojust)"[42] together with a proposal for a Council Regulation on the establishment of the European Public Prosecutor's Office (EPPO, see the analysis that follows). The Commission proposal is expressly aimed at increasing the "*democratic legitimacy of Eurojust*" as well as "*streamlining its functioning and structure*" in line with the Lisbon Treaty[43]. At the time of drafting of this study the positions on the Commission proposal of both the Parliament and the Council are still pending. From its part, however, the Eurojust Joint Supervisory Board showed very limited enthusiasm with the texts at hand (that, after all, threatens to effectively replace it with the European Data Protection Supervisor).[44]

While the Commission proposal still needs to be finalized, and the end result is likely to differ substantially from the original text, from a data protection point of view issues that merit mention with regard to Eurojust data protection supervision, monitoring, cooperation and accountability refer to[45]:

(a) Regulation 45/2001 is to apply to all processing operations at Eurojust,

(b) The EDPS is made responsible for supervision of Eurojust personal data processing, (as regards "EU activities or activities at EU level" (See Article 35(2)),

(c) Appointment of the Eurojust Data Protection Officer is to take place under the Regulation 45/2001 criteria; his/her position within Eurojust is further strengthened,

(d) The cooperation between Eurojust and other partners, particularly Europol, is better clarified in the Commission proposal,

(e) Eurojust shall be liable for the quality of personal data provided by EU bodies, third countries or international organisations, (and also for personal data retrieved by it from publicly available sources),

(f) Article 36 clarifies the right for individual redress, but the issue of a judicial challenge of EDPS or national DPA decisions is not expressly addressed.

[41] See European Parliament, The future of Eurojust, p.49.
[42] COM(2013) 0535 final (the "*draft Eurojust Regulation*").
[43] Information available at http://ec.europa.eu/justice/criminal/judicial-cooperation/eurojust/index_en.htm
[44] See Eurojust JSB critical position in "*Opinion of the Joint Supervisory Body of Eurojust regarding data protection in the proposed new Eurojust legal framework*", 14 November 2013.
[45] See also Weyembergh A, An Overall Analysis of the Proposal for a Regulation on Eurojust, Eucrim 2013/4, pp.127ff.

1.1.4. European Public Prosecutor'S OFFICE (EPPO)

The European Public Prosecutor's Office is not yet an established EU agency, but rather a proposal by the European Commission still in the law-making process. The Commission envisages "*an independent Union body with the authority to investigate and prosecute EU-fraud and other crimes affecting the Union's financial interests*".[46] In particular, the Commission tabled its proposal for the establishment of a European Public Prosecutor Office on 17 July 2013[47] together with the draft Eurojust Regulation (see above) as well as with a communication on OLAF. As the Council and the Parliament are yet to adopt their own final position,[48] the Commission proposal will form the basis of the analysis; however, the EPPO is of limited influence to the purposes of this analysis due to the fact that, even if the proposal goes through and the EPPO is indeed established, it is yet to be seen which position it will have in the EU criminal justice and law enforcement area.

Although the Commission filed its proposal for establishment of an EPPO only recently, the background for the establishment of the European Public Prosecutor is at least a decade old and should be examined in parallel with that of Eurojust.[49] In fact, the proposal at hand is not the first time that the Commission attempted to establish a European Public Prosecutor: in 2000, in the context of the 2000 IGC the Commission put forward an initiative to create a supranational-style European Public Prosecutor in order to establish an institution having sufficient powers to fight crimes committed against the EC's financial interests, including the power to prosecute such crimes before the national courts of Member States.[50] However, the 2000 IGC chose not to take up the Commission's initiative and opted for the establishment of Eurojust instead: with this decision the Member States opted for a more horizontal, intergovernmental-style coordinating body rather than transferring more substantive powers to an independent institution with the power to prosecute – an approach, that as seen above, is still in effect today.

The ratification of the Lisbon Treaty re-opened discussions over establishment of the EPPO. Article 86 TFEU states that "*in order to combat crimes affecting the financial interests of the Union, the Council, by means of regulations adopted in accordance with a special legislative procedure, may establish a European Public Prosecutor's Office from Eurojust*". The phrase "*from Eurojust*" opened up a number of possibilities, whose elaboration however lies outside the limits of this analysis.[51] As far as data protection oversight and co-operation are concerned, the Commission proposal:

(a) Perhaps expectedly, deals extensively with the relationship between Eurojust and the EPPO, detailing the "*special links*" that "*tie them together*", among others granting access to the Case Management System (CMS) of Eurojust to the EPPO.

(b) Instructs Eurojust to provide a series of support services to the EPPO, among which technical support, security services, IT services or accounting services.

[46] Information from http://ec.europa.eu/justice/criminal/judicial-cooperation/public-prosecutor/index_en.htm
[47] Proposal for a Council Regulation on the establishment of the European Public Prosecutor's Office, COM(2013) 534 final, 17.7.2013.
[48] The Parliament has, however, adopted its interim report with the EP *resolution of 12 March 2014 on the proposal for a Council regulation on the establishment of the European Public Prosecutor's Office,* (COM(2013)0534 – 2013/0255(APP)).
[49] See European Parliament, The future of Eurojust, pp.16ff.
[50] See European Parliament, The future of Eurojust, ibid.
[51] On the various possible approaches to the Treaty wording see, for instance, Ligeti K/Simonato M, *The European Public Prosecutor's Office: Towards a truly European Prosecution Service?* New Journal of European Criminal Law, Vol. 4, Issue 1-2, 2013, pp.10ff, White S, *A Decentralised European Public Prosecutor's Office: Contradiction in Terms or Highly Workable Solution?* eurcrim, 2/2012, pp.67-74.

(c) Europol and OLAF also receive specific mention in the Commission proposal, that requires them to cooperate with the EPPO.

(d) Entrusts the supervision of all personal data processing in the context of the activities of the European Public Prosecutor's Office to the European Data Protection Supervisor.

1.1.5. European Judicial Network

The European Judicial Network (EJN) is basically a horizontal network and does not qualify as an European agency. In essence, EJN is a network of national Member State contact points for the facilitation of judicial co-operation in criminal matters "*both in general and for certain forms of serious crime, such as organized crime, corruption, drug trafficking or terrorism*".[52] Other purposes include the provision of information to the public in order to facilitate their access to national judicial systems as well as the implementation of an online information system directed at EU citizens.[53] The EJN is composed of contact points of the Member States as well as of the European Commission and of a Secretariat based in The Hague. It was established by Joint Action 98/428/JHA of 29 June 1998,[54] preceding therefore the establishment of Eurojust by several years. It was however the need, among others, to "*clarify the relationship*" between the two and also to "*facilitate their communication*"[55] that led to the repeal of the Joint Action in 2008, by a Council Decision[56] that remains in effect today.

The EJN apparently does not process personal data until today and is therefore of marginal interest to the purposes of this analysis. A single point of interest might refer to the fact that EJN makes available to Eurojust its information tool and a secure telecommunications connection that may be linked to Eurojust's CMS.[57] It should be noted, however, that this finding will most likely change in the foreseeable future, when the EJN website will be incorporated into the European e-Justice Portal.[58] The latter ("*a future electronic one-stop-shop in the area of justice*")[59] poses significant data protection issues by itself that have already attracted a Commission Decision[60] and a relevant EDPS response,[61] even before becoming operational at least in the criminal justice and law enforcement field examined in this study.

[52] Information from the EJN website, http://www.ejn-crimjust.europa.eu/ejn/EJN_StaticPage.aspx?Bread=2#

[53] Information from the European Commission website, http://ec.europa.eu/justice/civil/judicial-cooperation/european-network/index_en.htm

[54] 98/428/JHA: Joint Action of 29 June 1998 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, on the creation of a European Judicial Network), OJ L191 7.7.1998.

[55] Information from http://europa.eu/legislation_summaries/other/l33055_en.htm

[56] Council Decision 2008/976/JHA of 16 December 2008 on the European Judicial Network, OJ L 348, 24.12.2008 (the "*EJN Decision*").

[57] See EJN Decision, Art. 9 and Eurojust Decision, Art. 16; see also Boehm F, *Information Sharing and Data Protection In the Area of Freedom, Security and Justice: Towards Harmonised Data Protection Principles for Information Exchange At Eu-Level* (Springer, 2012), p.255.

[58] Information found in the EU Justice website, http://ec.europa.eu/justice/criminal/european-e-justice/portal/index_en.htm.

[59] See the relevant website, at https://e-justice.europa.eu.

[60] Commission Decision of 5 June 2014 on the protection of personal data in the European e-Justice Portal (2014/333/EU).

[61] Opinion of the European Data Protection Supervisor on the Commission Decision on the protection of personal data in the European e-Justice Portal, 5 September 2014.

1.1.6. OLAF

The European Anti-Fraud Office (OLAF) was established in 1999 by a Commission Decision[62], that was subsequently complemented by a Regulation,[63] in order to address internal mismanagement (including protection of the Euro against counterfeiting); it is therefore part of the Commission, although independent in its investigative functions,[64] and does not constitute an EU agency. OLAF's task is to investigate internal and external fraud and any other illegal activity affecting the financial interests of the EU. In this context, OLAF carries out administrative, not criminal investigations. Its competences do not cover only offences but any irregularity that might affect adversely the financial interests of the EU. OLAF may not itself initiate criminal proceedings but instead forwards the relevant information to the competent authorities of the Member States. The above limitations and special characteristics of OLAF have led to the question whether it actually fits into the landscape of the European criminal law area at all.[65]

At any event, OLAF does process personal information in the course of executing its duties. To this end, the OLAF Regulation refers extensively to personal data processing, covering several data protection issues (for instance, access to databases or confidentiality of processing). With regard to supervision and cooperation, the OLAF Regulation allows OLAF to designate a data protection officer (Art. 10.4), while general supervision appears to be vested upon the EDPS (by virtue of Regulation 45/2001 that apparently finds general application with regard to OLAF personal data processing). Specific provisions are dedicated to cooperation of the Office with Eurojust[66] and Europol ("*where necessary*") as well as third countries and international organisations (Art. 13 and 14 respectively). While it is still early to assess the effectiveness of implementation of the new data protection provisions on OLAF personal data processing, as they only came into effect on 1 October 2013, notice should be given to the facts that Regulation 45/2001 finds general application and the EDPS consequently assumes the supervisory role, as well as, that intra-agency cooperation is fostered "*where necessary*" in anticipation of the EU criminal law regulatory environment.

1.1.7. The role of the European Data Protection Supervisor

The European Data Protection Supervisor (EDPS) office is essentially a (pre-Lisbon) first pillar instrument that is normally of limited relevance to (pre-Lisbon) third pillar personal data processing. Consequently, one would expect that the criminal justice and law enforcement agencies discussed in this study have little to do with the EDPS office. This assumption, however, has been breached in two ways by now. First, by the first EDPS own

[62] Commission Decision 1999/352/EC of 28 April 1999 establishing the European Anti-Fraud Office (OLAF), OJ L 136/20 31.5.1999, as amended by Commission Decision 2013/478/EU.

[63] Regulation 1073/1999 of the European Parliament and the Council of 25 May 1999 concerning investigation conducted by the European Anti-Graud Office (OLAF), OJ L 136/31 31.5.1999, in the meantime replaced by Regulation 883/2013 Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999, OJ L 248/1 18.9.2013 (the "*OLAF Regulation*").

[64] Information from the OLAF website, at http://ec.europa.eu/anti_fraud/policy/cooperation-with-eu-institutions/index_en.htm

[65] See Covolo V, From Europol to Eurojust – towards a European Public Prosecutor: Where Does OLAF Fit In? eucrim 2 / 2012 pp.83ff.

[66] Although Commission Decision 2013/478 expressly promises to consider its amendment "*in the event that a European Public Prosecutor's Office is established*".

policy-making, that strived, and to a large extent achieved, to extend as far as possible the relevance of his office.[67] And, second, by the fact that practically all of the Commission recent proposals on the law enforcement agencies (ie. the draft Europol, Eurojust and EPPO Regulations) award to the EDPS office a role of increased importance for supervisory matters on these agencies.

The institution of the European Data Protection Supervisor was introduced in 2001, by means of a relevant chapter in Regulation 45/2001 (Chapter V). Its purpose is to ensure "*that the fundamental rights and freedoms of natural persons, and in particular their right to privacy, are respected by the Community institutions and bodies*" (Art. 41.2). It was therefore the need to address personal data processing executed by Community institutions, that until that time remained unregulated,[68] that led to its establishment after the general legal environment (Art. 286 of the Treaty of Amsterdam) required it. To this end, the EDPS office was equipped with supervisory, co-operation and advisory functions.

Involvement of the EDPS in security-related personal data processing has been limited until today, because until now he only supervises personnel data processing and not the processing of individuals within the system – that task more or less lies within Member State DPAs and intra-agency boundaries (the Data Protection Officers and Joint Supervisory Boards concerned). Even between the EDPS office and the agency-specific Data Protection Officer no formal hierarchy exists under the legal framework in force. Despite all of the above, the EDPS demonstrated active interest in all developments in the field, among others, "*attending a number of meetings of the Joint Supervisory Bodies with deal with information systems in the area of police and justice*"[69] and issuing several opinions on all law-making initiatives on the agencies concerned, participating actively in their formulation.[70]

The current Commission proposals constitute a decisive moment in the EDPS office development. The Commission, in line with the general EU approach,[71] opts for the EDPS to undertake a formal supervisory role not only of personnel but also of data subject files in the system as well. After all, this is consistent with Commission's interpretation of Regulation 45/2001, according to which "*with the entry into force of Article 16 TFEU (replacing the former Article 286 EC), the scope of application of Regulation (EC) No 45/2001 extends automatically to all data processing activities of Union institutions within the scope of Union law*".[72] Admittedly, such award of a formal supervisory role has been suggested by the Commission at different tones – for instance, more directly in Eurojust and less so in Europol. Despite such differences (that may be hard to explain at times), given also that a clear hierarchy has also been suggested between the intra-agency data protection officials and the EDPS office, the EDPS office is positioned to undertake crucial new powers that until today lie well beyond its boundaries.

[67] See De Hert P/Papakonstantinou V, *The EDPS as a Unique Stakeholder in the European Data Protection Landscape, Fulfilling the Explicit and Non-Explicit Expectations*, in Hijmans H/Kranenborg H (eds.), *Data Protection Anno 2014: How to Restore Trust? Contributions in Honour of Peter Hustinx, European Data Protection Supervisor (2004-2014)*, Intersentia, 2014, 237–52.

[68] In fact, it has been noted that "*that Regulation 45/2001 is the implementation of that Directive [Directive 95/46] at the European level*", P. Hustinx, "Data Protection in the European Union," *Privacy & Informatie* 2 (2005): 62–65.

[69] See the EDPS website, https://secure.edps.europa.eu/EDPSWEB/edps/Cooperation.

[70] See the relevant "comments" and "opinions" webpages in the EDPS website.

[71] See the 2012 Overhaul on Decentralised Agencies (http://europa.eu/about-eu/agencies/overhaul/index_en.htm) and in particular the Guidelines on the prevention and management of conflicts of interest in EU decentralised agencies of 10 December 2013.

[72] See European Commission, Impact Assessment, ibid.

1.1.8. The role of the Article 29 Working Party

Although a (pre-Lisbon) first pillar instrument, the Article 29 Data Protection Working Party merits some mention for the purposes of this analysis. As per its name, this group was set up under Article 29 of the Data Protection Directive. Its scope was limited to the scope of the Directive (eg. non ex third pillar matters), but after the Lisbon Treaty it decided to take over also "police matters". The Article 29 Data Protection Working Party is an independent body, tasked to advise on issues such as harmonisation of national measures, level of protection in the EU and other countries, codes of conduct and other data protection issues. Its members comprise national DPAs and the EDPS. It issues opinions that, given their origins, can be very influential within the EU. However, courts, Member States and DPAs are not legally required to follow these opinions, and, because its decisions are approved by simple majority, an individual regulator who disagrees with the majority may decide not to follow its interpretation.

However, the Article 29 Working Party could become of relevance in the criminal justice and law enforcement personal data processing field when the EU data protection reform package is adopted (see below under 2.1). Under the Commission original proposal for a General Data Protection Regulation the Article 29 Working Party would become the European Data Protection Board; accordingly, the draft Directive provides that the same Board, established by the General Data Protection Regulation, exercises its tasks also in relation to processing activities within the scope of this Directive. However, most importantly, the Board will have only advisory tasks in the law enforcement area.

1.2. Inter-agency cooperation in the EU criminal justice and law enforcement area

KEY FINDINGS

- All agencies and bodies within the EU criminal justice and law enforcement area are in one way or another involved in exchanges of personal information both among them and with third countries or international organisations, such exchanges playing a crucial role in the execution of their duties. To this end they have entered formal written bilateral agreements (as listed in their respective websites).
- A clear set of data protection rules in all bilateral intra-EU agencies' cooperation agreements is not to be found. Given that the same agencies lack a common data protection regime and a common data protection monitoring mechanism, this is an important legal gap that needs to be remedied.
- Europol, Eurojust and presumably OLAF are active in entering cooperation agreements either with third countries or with international organisations in the course of executing their duties. Apart from these agreements the same agencies have the legal power to conduct single, isolated personal data exchanges with third countries. JITs also apparently fall under the same category. These personal data exchanges are only partially charted (only the agreements in force are provided in the relevant websites) and take place unmonitored by any (single, coordinated) data protection mechanism.

From a data protection perspective inter-agency cooperation within the EU criminal justice and law enforcement area is a derivative of information exchange among the agencies concerned. In essence, all of the agencies referred to above are in one way or another involved in exchanges of information both among them and with third parties or even countries, such exchanges playing a crucial role in the execution of their duties. The rules and methods under which these information flows take place lie outside the limits of this analysis. Here only the data protection aspects of any such information exchanges are of interest. From this point of view, attention shall be given to:

(a) institutional cooperation, meaning the data protection regime under which (any) personal data exchanges take place

(b) technical cooperation, meaning the data protection measures (if any) implemented in the infrastructure used for the above personal data flows, and

(c) data protection monitoring and supervision.

At this point two definitional clarifications need to be made. As per Europol classification, intra-agency cooperation agreements are distinguished into "strategic" and "operational" ones: the former concern all exchanges of data other than personal while the latter also include the exchange of personal data.[73] Another clarification refers to the fact that for the purposes of this analysis the term "EU agencies" shall be used to denote all of the above bodies (Europol, Eurojust, EPPO, OLAF, EJN), regardless of their actual legal status.

1.2.1. Institutional cooperation

Given their shared role as crime combating mechanisms, information exchanges among the agencies involved in the criminal justice and law enforcement area within the EU constitute an essential prerequisite for successful execution of their duties. This is an understanding also embedded in their constitutional legal documents: in practice each one of the EU agencies referred to above bears concrete obligations to exchange information with some or all of the others. Such obligations might be explicit and described in detail in the same constituting legal text or they may be derived from the same agencies' common goals and interests. Regardless therefore of their legal basis, it appears that information exchanges among the said EU agencies are as follows:

(a) **Europol – Eurojust**. Europol formal cooperation with Eurojust has been a prerequisite, almost since the Eurojust establishment (through its Protocol of 2003), and has been in effect ever since. Article 26 of the Eurojust Decision and Article 22 of the Europol Decision prescribe exactly that. A cooperation agreement (*operational*, as per the above distinction) has therefore been entered, in its latest version in 2010,[74] and a secure communication link was established since 2007.

(b) **Europol – OLAF**. Europol and OLAF have entered a (*strategic*, as per the above distinction) administrative agreement in 2004.[75]

[73] See Council Decision 2009/934/JHA of 30 November 2009 adopting the implementing rules governing Europol's relations with partners, including the exchange of personal data and classified information, Article 1.

[74] Available at the Eurojust website, at http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/agreements/Agreement%20between%20Eurojust%20and%20Europol%20%282010%29/Eurojust-Europol-2010-01-01-EN.pdf

[75] Administrative agreement on cooperation between Europol and OLAF, 8 April 2004, available at http://ec.europa.eu/anti_fraud/press_room/pr/2004/09.pdf

(c) **Eurojust – EPPO**. Although the EPPO is yet to be seen in its final format, the Commission proposal already outlines their special relationship (see, for instance, its Article 3), which also includes access of the EPPO to the Eurojust files (CMS, see its Article 57).

(d) **Eurojust – OLAF**. Article 26 of the Eurojust Decision asks for formal cooperation between the two agencies; in this context, a Practical Agreement on Arrangements of Cooperation has been entered since 2008.[76]

(e) **Eurojust – EJN**. Article 16.3 of the Eurojust Decision allows for the Eurojust CMS to be linked to the secure telecommunications connection of the EJN.

The table above demonstrates that information exchanges are customary and well established by now among the EU law enforcement and criminal area agencies. However, the data protection regime applicable to such information exchanges, whenever they include personal information, remains unclear, inconclusive and piecemeal. For instance, in the Europol and Eurojust agreement some data protection provisions are indeed included (namely, on the right of access, rectification and confidentiality), as well as a general term outlining that "*transmission of information shall only take place in accordance with the establishing act of the transmitting Party*" and that "*further processing of information received under this Agreement shall be limited to the purposes for which the information was communicated*",[77] but this is as far as any data protection goes in its text. On the other hand, the Eurojust and OLAF agreement seems to be more detailed with regard to data protection provisions (its whole Chapter 3 is dedicated to them) but each agency appears "enclosed" within its boundaries, specifically mentioning that for each one its own data protection regime applies, while at the same time not appointing a supervisor or even a way through which the exchange data protection rules are to be enforced in practice (ie. through allocating responsibilities between the data protection officers concerned).

In addition, it should be noted that Europol and Eurojust are benefiting from special rules of procedure for the exchange of personal data;[78] these are referred to directly, for instance, in exchanges between Eurojust and OLAF but it is not clear whether they apply at all times in exchanges where no special agreement exists (for instance, in the cases of personal data exchanges between Europol and OLAF) or their proper placement within the EU data protection edifice.

Given that all of the above EU agencies lack a common data protection regime, whereby a common piece of legislation (such as Regulation 45/2001) would set the common data protection rules and a central authority (such as the EDPS) would assume the role of monitoring all personal data processing regardless whether intra- or cross-agency, the general legal expectation would be for a clear set of data protection rules to be included in all cooperation agreements or relevant legal provisions in the EU law instruments involved. Nevertheless, this is not the case. In practice, in no cooperation agreement among the above agencies are any special data protection rules involved, that address the, admittedly diffi-

[76] Available at the Eurojust website, at http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/agreements/Practical%20Agreement%20on%20arrangements%20of%20cooperation%20between%20Eurojust%20and%20OLAF%20%282008%29/Eurojust-OLAF-2008-09-24-EN.pdf

[77] See its Article 13 par .1 and 2 respectively.

[78] For Europol see Council Decision 2009/934/JHA of 30 November 2009 adopting the implementing rules governing Europol's relations with partners, including the exchange of personal data and classified information. For Eurojust see Rules of Procedure on the Processing and Protection of Personal Data at Eurojust, 2005/C 68/01, OJ C 68/1, 19.3.2005, especially its Art. 28.

cult, issue of supervision and monitoring. Similarly, substantive data protection provisions, where available, are piecemeal and incoherent

The above evidence a legal gap: in practice, there are no clear data protection rules governing intra-agency cooperation within the EU. Given the volume of information exchanges that take place customarily among the same agencies, most of which information expectedly pertaining to personal data, this is an important legislative gap that needs to be covered in future legal initiatives given the, new, Article 16 TFEU and the culmination of an independent individual right to data protection within the EU.

1.2.2. Technical cooperation

Given the lack of data protection rules described above, there appears to be little interest on the technical means of information exchange among the EU agencies concerned; after all, in view of the legislative gap, whether each agency's processing system provides automated/continuous or manual/one-off access on its data to other agencies, or whether this is performed through "push" or "pull" technologies, is of secondary importance. However, brief mention will be made here to some technical details on such information exchanges only with the aim to demonstrate their volume and importance that, in turn, emphasize the need for legal, data protection, intervention.

Technical cooperation among the EU agencies in the law enforcement and criminal area got off to a bumpy start: for several years after their incorporation, systems apparently remained fragmented and trust among agency officials and Member States was low. Back in 2008 it was recommended that data transfers from Member States to Europol be performed "*by means of creating automatic data transfer instruments*",[79] denoting therefore that such did not exist at the time, at least not for all Member States. Integrity and trust in Europol information systems, and lack thereof, were also highlighted as difficulties by Member States impeding data transfers[80]. Problems were also identified with regard to system maintenance and technological update.[81] In addition, at least as far as Eurojust was concerned back in 2008, the agency was displeased that Europol supplied data and results to Eurojust only "*as far as allowed under its legal framework and this Agreement*" and even then only "*when appropriate*" as well as by its own limited access into Europol's working files.[82]

These issues apparently have been solved by now.[83] This may be at least inferred by study of the annual reports of the agencies' concerned, where the level of file exchanges is documented[84] without any mention to related obstacles.

From a structural point of view, work within the agencies concerned is based on information management systems, to which access rights are granted or refused as appropriate. The technical details of such systems are regulated in the establishing documents of the agen-

[79] Freedom, Security, Privacy—European Home Affairs in an open world—Report of the Informal High-Level Advisory Group on the Future of European Home Affairs Policy ("The Future Group"), Document 11657/08, cited in UK House of Lords report, p.16.
[80] UK House of Lords report, p.22.
[81] UK House of Lords report, p.29.
[82] See UK House of Lords report, p.49.
[83] However, on Europol – OLAF limited cooperation see Cavolo V, *ibid*, p.85 with further references.
[84] See, for instance, the Eurojust 2013 annual report stating that it cooperated with Europol on 53 cases and held 75 coordination meetings; similarly, see the Europol Review 2013 where it is stated that "*Eurojust remains an important partner of Europol at a strategic and operational level*" without however any number data to support this statement.

cies concerned (see for instance the Eurojust Decision on its CMS in Art. 16) as might be also the case with access rights to them (as is the case between Eurojust and the EPPO[85]). In all other cases apparently technical implementation follows the rules set by the inter-agency cooperation agreements in effect. However, while the level of legislative intervention on technical aspects in case management systems setup might at times be surprising (see, for instance, the express establishment of "*temporary work files*" and an "*index*" in Eurojust or the Europol Information System detailed legislative content and management), this is not also the case with management of third party access rights: apart from rare occasions (namely, only the Eurojust and the EPPO relationship) this is an issue left to be regulated in the relevant cooperation agreement – where, however, technical guidance usually remains high level and lacks detail.[86]

1.2.3. Interaction with third countries and international organisations

As per Europol's relevant webpage "*Europol assists EU Member States in combating organised crime within the European Union, but because organised crime does not stop at international borders, it is also essential to have cooperation initiatives with non-EU countries and international organisations*".[87] To this end Europol has entered a series of operational agreements with altogether twelve non-EU states (among which Canada, Australia and the USA[88]) as well as six strategic agreements with similarly non-EU states (among which the Russian Federation); as far as international organisations are concerned, it has entered an operational agreement with Interpol and a strategic agreement with the World Customs Organization and the UN Office on Drugs and Crime. Although an analysis of the data protection provisions of each one of the above operational agreements lies beyond the purposes of this study, here it is enough to be noted that data protection-related provisions are generally kept at a minimum[89] while supervision and monitoring is not performed by any single mechanism; instead, each agency is responsible within its own limits.

From its part, Eurojust has entered a series of agreements with third countries (for instance, the USA, the Principality of Liechtenstein, the Republic of Moldova) and international organisations (among which, Interpol or the UN Office on Drugs and Crime). With regard to the former, Eurojust has admittedly adopted a more detailed approach to data protection than Interpol[90]. This approach is in accordance with Article 26a of the Eurojust decision where, in order for such agreements to be entered, both the JSB needs to be consulted and the third party needs to be "*subject to the Council of Europe Convention of 28 January 1981 or after an assessment confirming the existence of an adequate level of data protec-*

[85] See Articles 41 and 57 of the Eurojust and EPPO Commission proposal respectively.

[86] For instance, Chapter 3 of the Europol – Eurojust agreement lists the cases of cooperation (communication of information, right of initiative, right of association) but access rights are not regulated therein.

[87] See the Europol external cooperation webpage, at https://www.europol.europa.eu/content/page/external-cooperation-31

[88] Particularly with regard to the USA agreement and certain intra-agency cooperation problems with its JSB, see Bigo D/Bonelli L/Chi D/Olsson C, Mapping the Field of the EU Internal Security Agencies, 2007, p.25 (available at http://bigo.zgeist.org/documents/Mapping.pdf).

[89] See, for instance, the Supplemental Agreement between the Europol Police Office and the USA on the Exchange of Personal Data and Related Information, Articles 6, 9, 10 and 12, or Articles 7, 10 and 11 of the Agreement between Interpol and Europol.

[90] In essence, it appears to have inserted a, more or less, standard set of data protection provisions in all its agreements with third countries: see, for instance, Articles 9-17 of its Agreement with the USA and Articles 12-17 of its Agreement with Liechtenstein (this is, however, not the case with its Agreement with Switzerland). In all of the agreements that fall under the same "template" it is expressly stated that "*the parties recognize that the handling and processing of personal data they acquire from each other is of critical importance to preserving confidence in the implementation of this Agreement*".

tion ensured by that entity". However, the fact remains that as far as supervision and monitoring are concerned no special provision has been made, leaving therefore each agency responsible for the processing within its own boundaries (and, therefore, unaware of what may have happened to the data it transmitted to the other). On the other hand, with regard to international organisations, Eurojust has apparently opted to enter agreements ("*memorandum of understanding*") with them that expressly exclude the exchange of personal information,[91] resolving thus radically any data protection issues (but perhaps affecting its own efficiency by such self-limitation).

Other than the above entered agreements between Europol and Eurojust and third countries and international organisations, **the possibility for single, isolated personal data exchanges ought not be overlooked**. This is provided expressly in their documents on rules of procedure respectively;[92] these cases, given also their urgent and one-off character, present very limited data protection safeguards.[93] In addition, under the same category ought to be listed any Joint Investigation Team activity among EU Member States and third countries[94] that to-date remains largely unchartered, at least from a data protection point of view.

OLAF states on its website that "*in its role of coordinating the fight against fraud at EU level, OLAF cooperates closely with its counterparts, including police, customs and judicial bodies, both within the EU and beyond its borders. The aim being to ensure a rapid exchange of information and swift follow-up actions*".[95] However, limited information is provided on any relevant agreements: apparently, OLAF makes use of any agreements with third countries that the EU has entered on mutual administrative assistance in customs matters, which also provide for the exchange of personal data.[96] Nevertheless, little data protection relevance is to be found in these agreements. Finally,[97] EJN, essentially being a network, provides a list of "partners" on its website, but it is not clear whether personal data are being exchanged between them and, if yes, under what (data protection) circumstances.

The above findings further strengthen the general picture of fragmentation and lack of adequate data protection supervision when it comes to personal data processing in the law enforcement and criminal area in the EU. Each agency has entered its own agreements with third countries and international organisations, as it is of course entitled to do, but under its internal data protection processes (if any) and data protection mechanisms and safeguards are applicable only within its own limits – meaning that there is effectively no way of knowing what happens to personal data once they exit the EU boundaries neither is there any body or organisation empowered to find out and report on that. In addition,

[91] See, for instance, for instance, its Agreement with Interpol (Art. 4) or its Agreement with the UN Office on Drugs and Crime (Art. 7).

[92] For Eurojust see Art. 28 of its Rules of procedure on the processing and protection of personal data at Eurojust as adopted unanimously by the College of Eurojust during the meeting of 21 October 2004 and approved by the Council on 24 February 2005; for Europol see Art. 14 of Council Decision 2009/934/JHA.

[93] See, in particular, the wording of Art. 14.3 of Council Decision 2009/934/JHA.

[94] See Council Framework Decision of 13 June 2002 on joint investigation teams (2002/465/JHA), as well as information in the relevant website (JITs Network), http://www.eurojust.europa.eu/Practitioners/JITs/jitsnetwork/Pages/JITs-network.aspx.

[95] See OLAF website at http://ec.europa.eu/anti_fraud/investigations/partners/index_en.htm

[96] See the relevant OLAF webpage at http://ec.europa.eu/anti_fraud/about-us/legal-framework/customs_matters/index_en.htm

[97] With regard to the EPPO, the Commission proposal provides that the EPPO may request the support of Eurojust in the transmission of its decisions or requests for mutual legal assistance in cases involving Member States which are not Member States of the EPPO or third countries (Art. 57). In addition, the Eurojust Regulation provides that Eurojust shall make use of its agreements with third countries and its liaison magistrates in order to support the cooperation of the EPPO with third countries (in Art. 41).

these agreements have been entered without Parliament's participation and even with limited control by the Council and the Commission, at least if compared to international agreements of the EU.[98] Moreover, under their current applicable legal regime, their internal data protection mechanisms, even if involved in the negotiation process, are awarded with very little space for intervention in the event that they are not pleased with the end result from a data protection point of view.

[98] See also Hijmans H/Scirocco A, ibid, p.1501.

2. FUTURE DATA PROTECTION ARCHITECTURE OF THE EU CRIMINAL JUSTICE AND LAW ENFORCEMENT AREA

KEY FINDINGS

- Although no data protection reform text (either general or agency-specific) is yet finalized (or even found at an advanced place in the law-making process), and therefore their current wording cannot be considered final, the Commission's preferred architecture is by now evident: the draft Police and Criminal Justice Data Protection Directive is to replace the Data Protection Framework Decision but not to affect any agency-specific personal data processing. This task will be undertaken by Regulation 45/2001 (or its successor) and the EDPS. This architecture is taken for granted by the authors because, regardless of its merits or drawbacks, other than the Commission also the Parliament has shown no substantial objection to it (in its opinion on the EU data protection reform package and on the Europol and EPPO draft Regulations respectively).

The ratification of the Treaty of Lisbon is the catalyst that brought change in the EU criminal justice and law enforcement area, at least from a data protection perspective. Among others, the culmination of a standalone individual right to data protection and the involvement of the Parliament in any decision-making in the field are crucial factors that enabled an, admittedly much needed, change. The Commission took into consideration the new regulatory environment and presented a series of legislative proposals over the past few years: these pertain both to scene-changing texts, such as the draft General Data Protection Regulation[99] and the Police and Criminal Justice Data Protection Directive[100], and agency-specific amendments, namely the Europol and Eurojust draft Regulations. More change is still under way: the Commission has promised to replace Regulation 45/2001 in order for the EDPS to be properly placed within the current regulatory environment.[101]

The Commission proposals, at least to the authors' point of view, generally respected the new post-Lisbon environment and awarded data protection with the priority it ought to receive under the new circumstances. However, there is limited merit in assessing these proposals, because there is little chance that these will also be the final texts to be adopted. Elaboration by the Council and the Parliament, as well as the ensuing "trilogue", are expected to affect them significantly. On the other hand, at the time of writing of this study there appears equally little chance that the basic architecture suggested by the Commission will change: although several Member States opposed at first both basic data protection regulatory instruments (the Regulation and the Directive) and preferred the old regime (a Directive and a Framework Decision), the possibility of overturning that is by now reduced – or, at least, this shall constitute a basic premise of this study. The same applies to the

[99] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 25.01.2012, COM(2012) 11 final.

[100] Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, 25.01.2012, COM(2012) 10 final, (the "Police and Criminal Justice Data Protection Directive").

[101] See the EDPS letter to the European Commission, *Application of the proposed General Data Protection Regulation GDPR to EU institutions and bodies*, 9 December 2013, available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2013/13-12-09_GDPR_comments_EN.pdf

agency-specific instruments: despite some opposition, it appears that the two draft Regulations under consideration (for Europol and Eurojust respectively) will in one way or another be adopted. Consequently, this study takes the suggested basic architecture for granted: it is the interplay among the above instruments that will attract attention in the scenarios' analysis that follows (under 2.2) and not the instruments themselves.

However, before embarking upon the presentation and analysis of these scenarios, a brief review shall be made of the EU data protection reform package, consisting of proposals for a General Data Protection Regulation and a Police and Criminal Justice Data Protection Directive. This is considered essential in order to properly describe the current situation before attempting to outline possible future scenarios affecting it.

2.1. The EU data protection reform package

In early 2012 the Commission presented its proposals for the EU data protection reform package. Such "package" comprises a proposal for a Regulation, the General Data Protection Regulation, intended to replace the Data Protection Directive and a proposal for a Directive, the Police and Criminal Justice Data Protection Directive, intended to replace the Data Protection Framework Decision. On 12 March 2014, the European Parliament adopted its first reading position on the two proposals.[102] At the time of writing this study, the Council is yet to adopt its first reading (general approach), after which the relevant "trilogue" can take place.

2.1.1. The General Data Protection Regulation

The proposed General Data Protection Regulation is an ambitious text aimed not only at replacing the Data Protection Directive, and hence resolve harmonisation issues across the EU, but also at bringing EU data protection law in line with modern personal data processing. To this end a series of changes have been suggested by the Commission aimed at serving this double role: detailed data protection provisions intend to exclude or limit the need for any local Member State legislative intervention, while new data protection tools (e.g. impact assessments, the right to be forgotten, data portability etc.) aim at bringing the EU data protection view into the new era. Although the proposed General Data Protection Regulation is an exciting text, admittedly finding more general public appeal than texts aimed at the criminal justice and law enforcement area, it is of no relevance to the purposes of this analysis because it does not affect the type of personal data processing that is of interest here.

[102] See, for the Directive, European Parliament, Report on the proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, (COM(2012)0010-C7-0024/2012-2012/0010(COD)), A7-0403/2013, 22 November 2013, and, for the Regulation, Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD), A7-0402/2013, 21 November 2013.

2.1.2. The Police and Criminal Justice Data Protection Directive

The draft Police and Criminal Justice Data Protection Directive presented by the Commission as part of its EU data protection reform package is intended to replace the Data Protection Framework Decision in order primarily to resolve its basic limitation in scope:[103] once the Directive comes into effect it shall regulate also national Member State personal data processing and not only intra-Member States exchanges of data, as is the case today. Although this already constitutes ambitious target-setting, the draft Police and Criminal Justice Data Protection Directive is a text of other merits as well: it strengthens individual data protection and addresses several shortcomings in applying the basic data protection principles that the Data Protection Framework Decision presents. The Parliament first reading more or less moves along the above Commission priorities; the Council's position is yet to be seen.

With regard to the purposes of this analysis, the original Commission text intended to leave the current criminal justice and law enforcement architecture unaffected, exempting its regulatory instruments from the scope of the draft Police and Criminal Justice Data Protection Directive, at least for the immediate future.[104] The Parliament did not differ substantially in that regard in its own position, because it left the relevant provisions unaffected but only made subtle, indirect, changes[105] and also reduced a bit the time limit within which agency-specific personal data processing provisions ought to be brought within the scope of the Directive.[106] However, the Parliament's first reading appears inconsistent: in the Europol Regulation (as well as in its opinion on the EPPO so far), although the Parliament goes into considerable length strengthening individual data protection, it effectively stays away from removing the basic reference to Regulation 45/2001, or its successor, the draft Directive.[107] Given the above, it probably appears unlikely that the draft Police and Criminal Justice Data Protection Directive will affect the agency-specific regulatory instruments in force today in the EU criminal justice and law enforcement area, at least in the foreseeable future.

2.2. Possible future scenarios for the data protection architecture of the EU criminal justice and law enforcement area

KEY FINDINGS

- The "unified model" scenario, under which the Police and Criminal Justice Data Protection Directive would regulate all the EU criminal justice and law enforcement area (including therefore the EU agencies operating therein) is least likely to occur not only due to the current wording of the Directive (as also broadly approved by the Parliament) but also due to legal restrictions: namely, it is not clear whether a Directive can regulate EU agencies.
- The "segregated model" scenario, under which the Police and Criminal Justice Data Protection Directive would leave EU agencies' personal data processing outside its

[103] See the draft Police and Criminal Justice Data Protection Directive, p.5 and also de Hert and Papakonstantinou, "The Data Protection Framework Decision", p.410.
[104] See Articles 59 and 61 of the draft Police and Criminal Justice Data Protection Directive.
[105] See Amendment 60 (as well as amendment 6) of the Parliament Report on the Directive.
[106] See Amendment 125 (Article 61) of the Parliament Report on the Directive.
[107] See Amendment 28 (Recital 32) of the European Parliament legislative resolution of 25 February 2014 on the proposal for a regulation on Europol.

scope (as is currently the situation under the Data Protection Framework Decision), while perhaps preferred by the agencies' themselves, invites unavoidable concerns over fragmentation and adequate data protection, particularly with regard to "independent" supervision, as required by Article 16 TFEU.

- The "interim segregated model" scenario is perhaps the one preferred to-date by the Parliament: under this model the segregated approach would last only for a few years and then EU agencies would have to bring their data protection under the Police and Criminal Justice Data Protection. This model presents two main difficulties: a legal one (it is not clear whether a Directive can regulate EU agencies) and a pragmatic one: new Europol, Eurojust and EPPO texts are being introduced right now and any interim term they may be given at this stage would ultimately undermine individual data protection for such, interim, period.
- Making use of Regulation 45/2001, or its successor, as an "alternative unified model", as per the Commission original proposals, presents the merits of a unified model approach but, if ultimately adopted, may raise important questions as to the relationship between this Regulation and the Directive – the EDPS would unavoidably have to apply both, each under different circumstances.
- The alternative of preserving the current architecture, in the sense that neither the Police and Criminal Justice Data Protection Directive nor Regulation 45/2001 affect the agencies' data protection regimes, that remain in effect independently based on their own (revised) provisions, presents the risk of (continued) fragmentation while it is not certain that, even under revised legal regimes, the agencies themselves will warrant "independent" data protection supervision, as required by Article 16 TFEU.
- Under the last scenario analysed in this study, Regulation 45/2001 will not be amended and agency-specific data protection provisions will supplement its current text: this would be a problematic development, because Regulation 45/2001 is essentially a (pre-Lisbon) first-pillar instrument that is not suited for the processing needs of the EU criminal justice and law enforcement area. The fact that this scenario appears plausible at least in the immediate future (given the current draft Europol, Eurojust and EPPO Regulations and the fact that the Commission has not made any amendment proposal for Regulation 45/2001 public) further endangers individual data protection.
- Finally, it is suggested that the European Parliament plays its role in order to ensure that the Commission timely adopts a proposal replacing Regulation 45/2001, ensuring that the new rules for the EU level enter into force at the same date as the new rules for the national level.

The analysis that follows outlines several possible future scenarios for the data protection architecture of the EU criminal justice and law enforcement area. While doing this, as already noted above, the basic players in the field shall be taken for granted. As the basic legal-instrument architecture suggested by the Commission (a Regulation and a Directive as regards the EU general data protection texts, and agency-specific Regulations with regard to EU criminal justice and law enforcement agencies), despite previous heavy criticism, appears to be more or less accepted by now, attention will not be paid to these instruments *per se* (ie. what *could have been* if these were not the legal instruments chosen) but rather to the interplay and interconnection among them.

It is to this end that the following scenarios have been identified, with the aim of assessing each one's potential strengths and weaknesses in particular with regard to the applicable legal regime and data protection supervision.

2.2.1. The "Unified Model" approach: the draft Police and Criminal Justice Data Protection Directive replaces the agency-specific data protection provisions

This, as discussed above under 2.1.2, is an unlikely to occur scenario. Effectively, the Commission wishes for the Police and Criminal Justice Data Protection Directive to not affect, at least in the immediate future, the agency-specific instruments already in place and, as seen, this is not very far away from the Parliament's line of thinking. Such an approach is also in line with the Data Protection Framework Decision currently in effect (see its Article 28). Accordingly, all agency-specific draft instruments currently under elaboration (the Europol, Eurojust and EPPO Regulations respectively) make passing or no mention at all to the draft Directive. Although the Council's views are yet to be seen, it appears unlikely that this approach will change in the future.

At any event, under this scenario the Police and Criminal Justice Data Protection Directive would find uniform application in all EU criminal justice and law enforcement personal data processing. This would include both Member States and Union agencies. Sector-specific legal instruments, particularly addressed to Union agencies, could make the Directive's provisions concrete into their circumstances – the fact however that a single standard-setting text would exist for all EU relevant processing would create beneficial side-effects also to sectors not strictly related to such agencies' processing, as could for instance the case be for PNR processing or international personal data processing agreements entered at EU level.

Despite the conceptual appeal of a "unified model" approach under the Police and Criminal Justice Data Protection Directive, that would also decidedly resolve the difficulties created by the "segregated model" below, the current legal environment does not seem accommodating to such a development. First and foremost, the legal instrument at hand appears ill-suited to achieve these purposes: a Directive is aimed at Member States and could not easily regulate Union agencies. In addition, immediate corresponding changes would have to be made to the legal instruments already under elaboration, ie. the Europol, Eurojust and EPPO Regulations – a development hardly foreseeable under contemporary circumstances. Even if the above structural difficulties were resolved, still the Police and Criminal Justice Data Protection Directive would have to address a number of significant issues, among which the data protection supervision model for Union agencies and, ultimately, its own relationship with Regulation 45/2001 or its successor (see below).

Given therefore the difficult decisions and significant structural changes that need to be made in order for this model to be realized, and taking into account current law-making developments, this model appears unrealizable, at least in the foreseeable future.

2.2.2. The "Segregated Model" approach: The draft Police and Criminal Justice Data Protection Directive does not replace the agency-specific data protection provisions

Under this "segregated model" the Police and Criminal Justice Data Protection Directive will not affect in any way the agency-specific data protection provisions. As this appears to be a compatible approach between the Commission and the Parliament (see above, under

2.1.2), at least in the immediate future, this appears a very likely future scenario (complemented by extended application of Regulation 45/2001 or its successor, see below under 2.2.4). Under it, each agency would retain its case-specific data protection regime, as set in its own constituting legal text, and the Police and Criminal Justice Data Protection Directive would only apply to Member States and processing falling outside said agencies' scope. Accordingly, data protection supervision could remain as in effect today, vested upon an intra-agency data protection officer and a Joint Supervisory Board.

Insistence in basically preserving the agency-specific data protection regime as in effect today presents obvious benefits: because the current model is reproduced, there will be no (or, significantly less) adaptation time requirement for the agencies concerned. An overhaul of their legal environment would pose a substantial burden upon them, that could ultimately affect their effectiveness. All this would be avoided if things were more or less left unchanged, and their constituting texts only included additional data protection safeguards in order to satisfy Art. 16 TFEU requirements. However, this scenario would not be in conformity with EU law, since a JSB does not fulfil the requirements of independence under EU law. In order, to fulfil these requirements the JSB should become a fully equipped independent supervisory authority, probably modelled on the EDPS and with sufficient staff. Creating such a separate, second EU authority would not be very cost effective.

On the other hand, maintenance of the current data protection model means that already identified and important problems remain unresolved. Lack of adequate data protection supervision and individual redress are central issues that, particularly after Art. 16 TFEU, may no longer be overlooked. A reproduction of the model at hand would mean that these problems are perpetuated for the years to come, rather than addressed in line with the new EU constitutional environment. In this context, an "intermediate" solution on supervision could perhaps include integrated supervision in a more unified and independent body (such as the EDPS in cooperation with DPAs). Although such a model would be conceivable, parallel existence of agency-specific rules (and consequently, agency-specific mechanisms such as JSBs and internal data protection officers) and external monitoring by a body (the EDPS) whose constituting and reference legal texts are otherwise expressly excluded from the same agencies' respective legal texts seems at best legalistic, if not confusing and even misleading (in particular, as to the actual EDPS role and competence with regard to these specific agencies as opposed to its other, usual, work). This scenario has as its most important disadvantage that it creates legal uncertainty for the data subject.

From a conceptual point of view, any segregated model unavoidably invites thoughts of fragmentation and patchwork of (data protection) provisions. The continued existence of agency-specific data protection regimes ultimately means that the level of data protection afforded to individuals is reduced. Even under the best (data protection) law-making intentions the fact remains that a single individual, if found within the interest of the EU criminal justice and law enforcement agencies, will require considerable effort only to comprehend the multitude of data protection provisions that are uniquely each time applicable to his or her situation. From a co-operation and monitoring point of view, multiple legal regimes inevitably lead to co-operation difficulties (ie. need for customization work) and lack of effective oversight. Ultimately, lack of common rules may benefit intra-agency problem-solving but could be harming the greater EU data protection picture. Despite of the fact that this appears a convincing scenario under current circumstances, the conceptual flaws underneath it ought not be overlooked or underestimated.

2.2.3. An "*interim* Segregated Model" approach: the draft Police and Criminal Justice Data Protection Directive places a time limit for the replacement/adaptation of the agency-specific data protection provisions

An intermediate scenario would involve the interim maintenance of the agency-specific data protection regime: in exactly the same way as the draft Police and Criminal Justice Data Protection Directive sets a time limit for member States in which to amend their bilateral data exchange agreements with third countries (see its Article 60), it could be set that EU agencies may continue applying their own data protection rules, perhaps appropriately amended in order to remedy already identified deficiencies and shortcomings, but these will need to be harmonized as per the Directive's general principles, in the foreseeable future. After all, this appears practically to be the Parliament's viewpoint for the time being.

Such a scenario would perhaps constitute a sensible solution, given that agencies would not need to hurry to change their personal data processing practices but will have enough time to prepare themselves. Such time allocation would also allow the roles between the different institutions referred to in the Directive (the DPAs, the Board, the EDPS) to be clarified and streamlined, in order for the agencies to enter an already running model instead of one currently under development. This policy option would also follow better its legal mandate: because the draft Directive is the result of the new Article 16 TFEU, and because application of Declaration 21 is after all voluntary, the EU criminal justice and law enforcement agencies would demonstrate better adherence to the EU constitutional documents.

However, such pragmatic approach could prove equally problematic with the previous two models it wishes to combine: As already noted, legal doctrine is against such a scenario because a Directive is only addressed to Member States. In addition, new constituting texts are currently being elaborated for Europol, Eurojust and the EPPO. Unless these are immediately abandoned or (re-)amended, if they are allowed to be implemented in their current wording the EU might end up with the impossible situation of *ex ante* undermined legal texts. In other words, if the texts currently under elaboration are permitted to implement the "segregated" data protection model but the draft Directive includes a provision undermining this policy option (setting a time limit after which it will expire), this will lead to unnecessary duplication of work and intermediate confusion, because the agencies whose newly acquired data protection regimes will again need to change within a few years would be constantly facing the dilemma, which provisions to apply each time. This is why, although such an interim solution may be better suited for Member States, that may manage on their own their bilateral agreements, as far as EU agencies are concerned that are currently witnessing their constituting texts being amended it could prove ineffective and counterproductive.

2.2.4. Regulation 45/2001 as an "alternative Unified Model" approach: an agency-specific data protection model that is however aligned under the EDPS?

Under this scenario the role of the data protection standard-setting text for all EU criminal justice and law enforcement agencies would be assumed not by the draft Police and Criminal Justice Data Protection Directive but by Regulation 45/2001, as in effect today or as amended in the future. This, in effect, constitutes the Commission's preference, as demonstrated in its proposals for the Europol, Eurojust and EPPO respectively. Given also that the Parliament and the Council, at least with regard to the Europol draft Regulation, did not reject in principle this approach, it appears that this constitutes the most likely scenario to be adopted in the future.

This policy option addresses the applicable legal regime question in a possibly straightforward way: Regulation 45/2001, or its successor, will set the general data protection principles, that will be complemented and particularized by each agency's constituting legal document. Accordingly, data protection supervision would be vested centrally upon the EDPS for all the agencies concerned; the latter would probably keep only their internal data protection officer and abolish their current Joint Supervisory Board(s). Although this appears a clear-cut approach, its implementation to-date leaves space for doubt: while under this scenario ideally each one of the Commission's agency- specific proposals (Europol, Eurojust, the EPPO) would include explicit reference to Regulation 45/2001 and would equally explicitly restrain themselves to "*particularizing and complementing*" its provisions, this does not constitute a uniform approach by the Commission: while it is explicit in the Eurojust and EPPO Regulations,[108] it is far from conclusive in the Europol Regulation.[109]

From a conceptual point of view this scenario presents the merits of a "unified model" approach and, accordingly, resolves all "segregated" approach difficulties highlighted above. Nevertheless, it does so at a price: two, rather than one, texts assume the same role, that of the standard-setting text. Consequently, an apparent question refers to the relationship between the two: does any one of them, the Police and Criminal Justice Data Protection Directive or the Regulation 45/2001 (or its successor), take precedence over the other? Which one should be aligned to which one's provisions? What happens in the event of a conflict between their provisions? And, in particular with regard to supervision, which one will serve as a text of reference for the EDPS, the text establishing its office or the text to which the former should be aligned (at least, as per the Parliament's approach)?[110]

Notwithstanding the above, under this scenario the actual final wording of the related provisions matters. Even if the applicable legal regime is in principle clear, this might not be the case with regard to role partition between the data protection supervisory authorities: the EDPS, Member State DPAs, the Board and any intra-agency officials. In the same context, as correctly pointed out by the Eurojust JSB, Regulation 45/2001 is essentially a first pillar instrument that is today both outdated and probably ill-suited to serve criminal justice and law enforcement area needs and requirements. Despite of the fact that in practice the EDPS has gained valuable experience in overseeing, other, third pillar issues (Eurodac law enforcement part, VIS and SIS), Article 16 TFEU anyway asks for its replacement. The Commission has promised to do so in the future, however today there is no sample of its approach on this subject. Therefore, until the successor of Regulation 45/2001 is seen, here only hypotheses may be made as to its potential to succeed in its increased role promised under this scenario. For the time being, given the difficulty already highlighted above with regard to Europol, limited enthusiasm ought to be spent upon this possibility actually coming true.

2.2.5. Preserving the current data protection architecture (the "segregated model" continued): Regulation 45/2001, amended or not, does not apply to the EU criminal justice and law enforcement agencies

Under this scenario the current data protection situation in the EU criminal justice and law enforcement area is more or less left as it is. In other words, neither the draft Police and Criminal Justice Data Protection Directive nor Regulation 45/2001 (or its successor), find

[108] See their Art. 27 and 37 respectively.
[109] See Recital 39 of the Europol Regulation.
[110] See its amendment 6 on the Directive.

any application in the field.[111] Instead, each EU agency continues to benefit from and apply its own data protection rules – that may or may not be amended as per the current Commission proposals. This effectively means that the current cooperation and supervision model, in the form of agency-specific Joint Supervisory Board(s) and Data Protection Officer(s) that answer only to their Management Boards, is maintained more or less unaffected.[112]

Under this scenario the difficulties highlighted in the first part of this analysis are preserved. As demonstrated above, fragmentation, lack of adequate (independent) oversight and monitoring, lack of intra-agency data protection cooperation are all consequences of the data protection legal patchwork currently in effect. However, these difficulties apart from being ineffective in themselves, also contradict by now Article 16 TFEU: in essentially adhering to the pillar system that is by now abolished, they fail to observe the requirements of the new individual right to data protection – regardless of Declaration 21 that after all, apart from its voluntary character, enables separate legal instruments but not a reduced data protection level.

On the other hand it could be argued that the Commission proposals for Regulations currently under elaboration could address these issues. These proposals could increase the intra-agency data protection level in order to meet Article 16 TFEU standards but otherwise not affect the current data protection system architecture. After all, this is the preferred approach of at least one JSB involved in the process (that of Eurojust), that has publicly opted for this solution. However, such an approach faces inherent difficulties. Independent data protection supervision is expressly required by Article 16 TFEU and has been always highlighted as a shortcoming of current data protection in the agencies concerned. Awarding data protection oversight to an internal officer, regardless of the safeguards vested upon him or her, and an equally internal council that only rarely convenes, and in any way cannot reach any further than the agency management concerned, by no means qualifies as independent. Independence of the control in one way or another will have to include an external actor. Such actor ought in addition be fully (and constantly) operational and an expert in the field; the EDPS is an obvious choice to this end. However, the EDPS abides by its own constituting rules that could not possibly be abandoned each time he or she is called upon to exercise monitoring duties on a criminal justice and law enforcement EU agency. This is why a unified model approach, under Regulation 45/2001 or its successor (or even the Police and Criminal Justice Data Protection Directive, if it ever came to that), is ultimately inevitable, imposed both by Article 16 TFEU and current EU data protection system architecture constraints.

2.2.6. Regulation 45/2001 is not revised; agency-specific data protection provisions supplement its current text

This constitutes an unlikely scenario, given Article 16 TFEU and the Commission intention to revise Regulation 45/2001. It is however listed here for two reasons: first, in order to

[111] It should be noted, however, that according to the Commission, Regulation 45/2001 "*extends automatically to all data processing activities of Union institutions within the scope of Union law*" (see Commission's Impact Assessment Report, ibid). Under such a reading of the legal texts already at hand this scenario is obsolete, because Regulation 45/2001 already applies to the agencies examined. Nevertheless, the Commission's reading does not seem to have found application in practice until today, because the agencies concerned apparently have continued to grant limited supervisory authorities to the EDPS, as was exactly the case before the Treaty of Lisbon came into effect.

[112] On the potential "integrated model" approach, whereby agency-specific instruments would not preclude supervision (also by) the EDPS see the analysis above, under 2.2.2.

achieve picture completeness; and, second, because, however unwanted, it is a likely scenario for the immediate future given time synchronization between the various legislative initiatives currently under way.

Regulation 45/2001 is by no means an instrument well-suited for the post-Lisbon era. It was released under a different legal system (the pillar system) with different purposes (to regulate general EU institutions' personal data processing). In the meantime it has been affected not only by significant case law[113] but also by actual EDPS practices that are unlikely to be abandoned in the future.[114] All this would have required its revision anyway, even without Article 16 TFEU.

Particularly with regard to the criminal justice and law enforcement area, Regulation 45/2001 in its current wording faces basic limitations coming from the fact that it does not take into account any personal data processing performed in the relevant context. However, this type of processing is different than general personal data processing, as after all acknowledged also in the EU data protection reform package itself, that distinguishes between a Regulation and a Directive. The fact that, unlike past conditions back in 2001, Regulation 45/2001 would now have to accommodate the needs of agencies with well-established and operating data protection systems will set a first for it, that is however not needed in view of efficiency and effectiveness of protection. All of the above point to the need for its revision; even if complemented by each agency's specific instrument(s), the deficiency of the architecture (a first pillar instrument to regulate law enforcement processing) cannot be remedied.

However, this is probably a likely scenario for the immediate future: because Commission proposals for the EU data protection reform package and for agency-specific instruments have well progressed, while not even a draft Commission communication exists for a revision of Regulation 45/2001, we might come to a situation where new agency-specific legal instruments will use as their text of reference an outdated and out of place legal instrument that itself awaits its replacement. Evidently, it will take a skilled EDPS to overcome such a difficult situation; however the fact remains that Regulation 45/2001 amendment process ought to be brought to speed in order to be aligned with other agency-specific proposals, if not the EU data protection reform package as well, in order to warrant efficiency of implementation and a possibly minimized transition period.

[113] See Court of Justice, Joined cases C-317/04 and C-318/04, 30 May 2006.
[114] See De Hert and Papakonstantinou, "The EDPS as a Unique Stakeholder in the European Data Protection Landscape."

3. CONCLUSIONS - FINDINGS

Developing the future data protection architecture of the EU criminal justice and law enforcement area is by no means an easy task. Among the factors of complexity is first and foremost the fact that the new edifice is not being built from scratch: a rich background of EU agency-specific rules, general legal texts, police and law enforcement needs, as well as the pre-Lisbon pillar itself set a scene that cannot be overlooked while planning for the future. Another factor refers to the legal instruments at hand: the new framework has to make use of the available law-making tools (Regulations, Directives and Decisions) in order to regulate in the best possible way a multitude of actors processing personal data, by Member States police as well as Europol, or within international data transfer agreements. The interplay and limitations of each one of the above mentioned tools is important for effective regulation purposes. Finally, general law-making syncronisation also appears to further complicate things: the EU seems to attempt to carry out at the same time the herculean task of amending all of its basic data protections texts (the Data Protection Directive and the Data Protection Framework Decision) together with all basic agency-specific texts (the Europol and Eurojust Decisions) and also to establish a new important institution (the EPPO), while at the same time an important text (Regulation 45/2001) eagerly awaits its own turn to be amended. And still one does not, and could not, assess what will happen once the EU accedes to the ECHR and changes to Convention 108, also currently being amended, become effective. Syncronisation among all these important developments is difficult (if not impossible) and a basic cause for concern.

On the other hand a series of enabling factors make an admittedly long-needed change imperative. Article 16 TFEU sets concrete data protection requirements on all EU personal data processing. The pillar system is abolished; the European Parliament plays an increased role in the law-making process; and law enforcement authorities processing personal data in the EU present serious data protection loopholes. All of the above elements make the EU law-making institutions' (the Commission, the Council and the Parliament) herculean task described above worth the effort: a unique opportunity has presented itself to execute at once a data protection regime's overhaul within the EU and, hopefully, resolve many important (and stagnating over the past years) data protection problems.

Within this context, the Commission made a series of policy options over the past few years for the future data protection architecture of the EU criminal justice and law enforcement area and has incorporated them in the legal instruments it presented to the Parliament and the Council and that are currently under elaboration. As per the Commission proposal, the draft Police and Criminal Justice Data Protection Directive is to replace the Data Protection Framework Decision and constitute the general data protection text in the field but with the important limitation that it will leave the EU level personal data processing alone. This is to be regulated by a general text, Regulation 45/2001 and its successor, which will be further specified and complemented by agency-specific data protection regulations. The EDPS will hold the general monitoring role, in cooperation with the agency-appointed data protection officials – today's Joint Supervisory Board will be abolished.

Given the limitations mentioned above, the edifice suggested by the Commission makes legal sense. Article 16 TFEU requires data protection amendments and independent supervision; Declaration 21 TFEU allows for agency-specific instruments "where necessary"; a Directive could not easily regulate EU agencies and bodies; the EDPS is an established, operating and permanent data protection supervisory mechanism. All these are important supporting arguments for the Commission suggested architecture. On the other hand a series of things could go wrong: the balance between the Police and Criminal Justice Data Protection Directive and Regulation 45/2001 or its successor could be missed; Regulation

45/2001 could take a lot of time to be amended allowing an unsuited pre-Lisbon first-pillar instrument to do third-pillar work for a prolonged period of time; the agency-specific instruments (the Europol, Eurojust and EPPO Regulations) could not be aligned among them, raising questions on effectiveness (and eyebrows on the *raison d'etre* of different treatment); or, simply unforeseeable political or other developments (such as the recent USA Snowden case) could distract an already overstretched law-making agenda.

It is at this point that the Parliament is called upon to perform its, newly acquired, law-making function with regard to the above instruments. While doing this, it is perhaps important to revert to Article 16 TFEU,[115] that after all started all this, and assess what it does, and what it does not, prescribe. Although the discussion over what exactly "*the right to the protection of personal data*" entails could be long and open-ended, the authors believe that the following constitute relevant data protection priorities:

- Article 16 TFEU allows the Parliament to think of data protection not in terms of the EU internal market or the old pillar system or any other similar limitations, but in terms of an independent, separate individual right that needs to be respected in all the EU;
- Article 16 TFEU asks for effective, independent oversight. While independent oversight is most likely external, effective oversight may be a combination of internal and external mechanisms. To this end, already installed and operating oversight mechanisms do not necessarily need to be replaced under the new EU data protection environment;
- Data protection and Article 16 TFEU are neutral towards fragmentation. Although fragmentation may be counter-productive or cost-inefficient, the data protection basic rules may be equally observed in one, all-encompassing, or in several, agency-specific, data protection legal texts;
- Perhaps more importantly, Article 16 TFEU asks for simple and straightforward individual access to justice. This in turn requires clear and direct replies to the basic questions of legal standing (who can sue data controllers in court), scope of judicial review (what can the judge assess), remedies available (monetary indemnity) and cost of the whole process. These answers need to be clear and accessible to individuals across the EU, regardless of the legal instruments they are based on.

The above priorities may be served both within the Commission suggested model, with amendments mostly pertaining to individual access to justice, and through a single all-encompassing text, such as the Police and Criminal Justice Data Protection Directive, if properly supplemented and further specified by agency-specific legal instruments. So far the Parliament has published its views on the EU data protection reform package and the Europol Regulation – an already advanced position in comparison to the Council that has only given feedback on the latter. The "trilogue" phase follows. While the Parliament may, or may not, choose to support the architecture put forward by the Commission, the authors believe that its best possible contribution to the future data protection regime would be to pay particular attention to the new individual right to data protection (set out by Article 16 TFEU) and to review closely the priorities identified in the Commission's proposals, regardless of the organizational structure that will ultimately be chosen.

[115] See also the relevant analysis in Hijmans H/Scirocco A, ibid, pp.1517ff.

REFERENCES

- Bigo D/Bonelli L/Chi D/Olsson C, *Mapping the Field of the EU Internal Security Agencies*, 2007, (available at http://bigo.zgeist.org/documents/Mapping.pdf).
- Blas D A, *The New Council Decision Strengthening the Role of Eurojust: Does it also Strengthen Data Protection at Eurojust?* in Gutwirth S/Poullet Y/De Hert P, *Data Protection in a Profiled World*, Springer, 2010.
- Boehm F, *Information Sharing and Data Protection In the Area of Freedom, Security and Justice: Towards Harmonised Data Protection Principles for Information Exchange At EU level*, Springer, 2012.
- Covolo V, *From Europol to Eurojust – towards a European Public Prosecutor: Where Does OLAF Fit In?* Eucrim 2/2012.
- De Hert P/ Papakonstantinou V, *The Data Protection Framework Decision of 27 November 2008 Regarding Police and Judicial Cooperation in Criminal Matters - A Modest Achievement However Not the Improvement Some Have Hoped for*, Computer Law & Security Review 25 (2009).
- De Hert P/Papakonstantinou V, *The EDPS as a Unique Stakeholder in the European Data Protection Landscape, Fulfilling the Explicit and Non-Explicit Expectations*, in Hijmans H/Kranenborg H (ed.), *Data Protection Anno 2014: How to Restore Trust? Contributions in Honour of Peter Hustinx, European Data Protection Supervisor (2004-2014)*, Intersentia Ltd, 2014.
- EDPS, *Opinion of the European Data Protection Supervisor on the Proposal for a Council Decision establishing the European Police Office (EUROPOL)*, COM (2006) 817.
- EDPS, *European Data Protection Supervisor*, Letter of 13 November 2013 to Mr Juan Fernando López Aguilar, Chair of the LIBE-Committee of the European Parliament concerning the data protection supervision on Europol
- EDPS, *European Data Protection Supervisor letter to the European Commission, Application of the proposed General Data Protection Regulation GDPR to EU institutions and bodies*, 9 December 2013.
- EDPS, *Opinion of the European Data Protection Supervisor on the Commission Decision on the protection of personal data in the European e-Justice Portal*, 5 September 2014.
- Eurojust, Joint Supervisory Body of Eurojust, *Opinion of the Joint Supervisory Body of Eurojust regarding data protection in the proposed new Eurojust legal framework*, 14 November 2013.
- Europol, Joint Supervisory Body of Europol, *Opinion 13/31*, 10 June 2013.
- European Parliament, *The future of Eurojust*, Study for the LIBE Committee, 2012.
- 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 Market Law Review, Vol 46, 2009.
- Hustinx P, *Data Protection in the European Union*, Privacy & Informatie , 2005.
- Ligeti K/Simonato M, *The European Public Prosecutor's Office: Towards a truly European Prosecution Service?* New Journal of European Criminal Law, Vol. 4, Issue 1-2, 2013.
- UK House of Lords report, *EUROPOL: coordinating the fight against serious and organised crime*, HL Paper 183, November 2008.

- Weyembergh A, *An Overall Analysis of the Proposal for a Regulation on Eurojust*, Eucrim 2013/4.
- White S, *A Decentralised European Public Prosecutor's Office: Contradiction in Terms or Highly Workable Solution?* Eucrim, 2/2012.

EUROPEAN PARLIAMENT

CATALOGUE QA-07-14-089-EN-N

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C
CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

Role

Policy departments are research units that provide specialised advice to committees, inter-parliamentary delegations and other parliamentary bodies.

Policy Areas

- Constitutional Affairs
- Justice, Freedom and Security
- Gender Equality
- Legal and Parliamentary Affairs
- Petitions

Documents

Visit the European Parliament website: **http://www.europarl.europa.eu/studies**

PHOTO CREDIT: iStock International Inc.

ISBN: 978-92-823-6339-3
DOI: 10.2861/133

Publications Office