The Issue of Data Protection and Data Security in the (Pre-Lisbon) EU Third Pillar

Maria O'Neill
University of Abertay Dundee

Abstract

The key functional operability in the pre-Lisbon PJCCM pillar[1] of the EU is the exchange of intelligence and information amongst the law enforcement bodies of the EU. The twin issues of data protection and data security within what was the EU's third pillar legal framework therefore come to the fore. With the Lisbon Treaty reform of the EU, and the increased role of the Commission in PJCCM policy areas, and the integration of the PJCCM provisions with what have traditionally been the pillar I activities of Frontex, the opportunity for streamlining the data protection and data security provisions of the law enforcement bodies of the post-Lisbon EU arises. This is recognised by the Commission in their drafting of an amending regulation for Frontex[2], when they say that they would prefer "to return to the question of personal data in the context of the overall strategy for information exchange to be presented later this year and also taking into account the reflection to be carried out on how to further develop cooperation between agencies in the justice and home affairs field as requested by the Stockholm programme."[3] The focus of the literature published on this topic, has for the most part, been on the data protection provisions in Pillar I, EC. While the focus of research has recently sifted to the previously Pillar III PJCCM provisions on data protection,[4] a more focused analysis of the interlocking issues of data protection and data security needs to be made in the context of the law enforcement bodies, particularly with regard to those which were based in the pre-Lisbon third pillar. This paper will make a contribution to that debate, arguing that a review of both the data protection and security provision post-Lisbon is required, not only in order to reinforce individual rights, but also inter-agency operability in combating cross-border EU crime. The EC's provisions on data protection, as enshrined by Directive 95/46/EC, do not apply to the legal frameworks covering developments within the third pillar of the EU. Even Council Framework Decision 2008/977/JHA, which is supposed to cover data protection provisions within PJCCM expressly states that its provisions do not apply to "Europol, Eurojust, the Schengen Information System (SIS)" or to the Customs Information System (CIS). In addition, the post Treaty of Prüm provisions covering the sharing of DNA profiles, dactyloscopic data and vehicle registration data pursuant to Council Decision 2008/615/JHA, are not to be covered by the provisions of the 2008 Framework Decision. As stated by Hijmans and Scirocco, the regime is "best defined as a patchwork of data protection regimes", with "no legal framework which is stable and unequivocal, like Directive 95/46/EC in the First pillar".[5] Data security issues are also key to the sharing of data in

[1] Police and Judicial Cooperation in Criminal Matters.
[2] Proposal for a Regulation of the European Parliament and the Council amending Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX) {SEC(2010) 149} {SEC(2010) 150}, COM(2010) 61.
[3] *ibid.* in pages 4-5 of the introduction.
[4] H. Hijmans and A. Scirocco; Shortcomings in EU data protection in the third and the Second Pillars, Can the Lisbon Treaty be expected to help? CMLRev. 46: 1485-1525, 2009.
[5] *ibid.* at p.1496.

O'Neill, M. (2010). 'The Issue of Data Protection and Data Security in the (Pre-Lisbon) EU Third Pillar', *Journal of Contemporary European Research*. Volume 6, Issue 2, pp. 211-235.
Available at: http://www.jcer.net/ojs/index.php/jcer/article/view/264/206

organised crime or counterterrorism situations. This article will critically analyse the current legal framework for data protection and security within the third pillar of the EU.

Keywords

Data protection; Data security; PJCCM; Europol; Eurojust; Schengen: Prüm

DATA PROTECTION LAWS ARE VERY MUCH A CHILD OF OUR TIMES, WITH "automated massive processing of personal data"[6], bringing the issue to the fore. Legal frameworks began to be developed in the 1960s, with much of their development happening during the 1970s and 1980s.[7] EU concepts underlying data protection have developed differently from those in other parts of the world, notably the United States, where the divide between the two "is a stark example".[8] The concepts of data protection and privacy are seen as being closely connected, with "a significant overlap between the two"[9], and privacy being "a contested legal concept".[10] The German Federal Constitutional Court[11] has developed what has become the EU approach on the matter.[12] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data were adopted in 1980[13], with the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data being signed in 1981.[14] The UN also published Guidelines Concerning Computerised Data files in 1990.[15] Most of these initiatives have been in the area of commercial data, with the intention of defending "individuals against the "intrusive" State."[16] The processing of data for counter-terrorism and law enforcement purposes have, however, not been so well addressed, with the drive for "security" coming to the fore post 9/11, requiring "affirmative action", which some have distinguished from the terms "safety" and "surveillance".[17] While there has been recent acknowledgment of the issues that arise with regard to EU law enforcement data collection[18], data protection in this area must be analysed in conjunction with the issue of data security. When these twin issues are analysed together, a very complex picture emerges, which should be re-examined in the post-Lisbon era. While Hijmans and Scirocco point out that "legal instruments facilitating the access to and exchange of information are a priority for the EU legislature"[19], much still needs to be done to anticipate all possible scenarios that may arise, in order to both protect the individual from a data protection perspective and facilitate properly directed law enforcement operations across the EU. As can be seen from the sketched outline in the following table, both the data protection and data security regimes for the EU law enforcement agencies are highly fragmented.

---

[6] de Hert, Papakonstantinou, 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, 25 (2009) *Computer Law & Security Review* 403-414, p.403.
[7] *ibid.*
[8] Birnhack, The EU Data Protection Directive: An engine of a global regime, 24 (2008) *Computer Law & Security Report* 508-520, p.509.
[9] Kuner, An international legal framework for data protection: Issues and prospects, 25 (2009) *Computer Law & Security Review* 307-317, p.309.
[10] Birnhack, n8 above, p.508.
[11] Bundesverdassunsgericht, Judgment of 15 December 1983, 65 BVerfGE 1.
[12] Kuner, n9 above, p.308.
[13] Birnhack, n8 above, p.511.
[14] *ibid.*
[15] *ibid.*
[16] De Hert, Papakonstantinou, n6 above, p.404.
[17] *ibid.*
[18] In particular, H. Hijmans and A. Scirocco; Shortcomings in EU data protection in the third and the Second Pillars, Can the Lisbon Treaty be expected to help? CMLRev. 46: 1485-1525, 2009.
[19] H. Hijmans and A. Scirocco, n4 above, p.1492.

Table 1: EU law enforcement data protection and data security overview

	Data protection	**Data Protection Supervisor**	**Data security standards**
Europol	Europol Documentation (Council Decision 2009/371/JHA)	Europol Data Protection Officer, post- 2009 reforms	Council Decision 2009/968/JHA
Eurojust	Eurojust Documentation (Council Decision 2002/187/JHA, to be replaced by Council Decision 2009/426/JHA, when it comes into force)	Eurojust Data Protection Officer since 2002	Council Decision 2001/264/EC as amended
Frontex (ex. EC)	Regulation 45/2001	European Data Protection Supervisor	None specified pre-reforms; Council Decision 2001/264/EC as amended, post-proposed Frontex reforms
Schengen	SIS I – none. SIS II – Articles 56 to 63 of Council Decision 2007/533/JHA on the second generation of Schengen	SIS I – none. SIS II - European Data Protection Supervisor	None specified; presumably Council Decision 2001/264/EC as amended
Prüm Council Decision	National data protection laws	National Data Protection Supervisors	None specified
Anything else ex. pre-Lisbon third pillar	CFD 2008/977/JHA	National Data Protection Supervisors	None specified

Caught between the panoptic demands[20] of the surveillance society, in a world of increasing securitisation, and the requirements of the European Convention on Human Rights and domestic privacy laws, to include the needs of the criminal law for due process before 'conviction' for a criminal offence, data protection laws have been attempting to keep up with rapidly developing technology and the growth, for a variety of reasons, of complex and detailed databases. The precursor to EC and EU law in the area of data protection was the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data. The definition of what is 'personal data' is still being refined, with the EU's Article 29 Working Committee, the "EU's data protection think tank"[21] often coming into conflict with national definitions of what is personal data, as was the case with the UK definition, as developed in the UK Court of Appeal ruling in *Durant* v. *FSA*.[22] Nevertheless, much has been written about data protection laws implemented pursuant to Directive 95/46/EC[23], which provides the legal framework for data protection in the first pillar of the EU, as it was known prior to the coming into force of the Lisbon Treaty[24], which specialises in commercial and civil law. More recently, the "complex relations between data protection and the activities of the State to ensure security" [25] has come to the fore in legal and political debates. Policing and other security agencies use of data, which needs to be protected by data protection legislation, is also required by society to be used in order to prevent and combat crime. In addition, the particular needs of the law enforcement community for data security, which is also affected by security classification issues, is highly relevant. Post-Lisbon these allied issues, and the requirements for the inter-operability of EU law enforcement agencies, need to be re-examined. Both the law enforcement community and society more generally require coherent and acceptable data protection and data security legal frameworks across the EU, both for the interoperability of databases in combating crime and the protection of the individual citizen who is caught up, either innocently or otherwise, in a law enforcement operation. As has been stated by the US General Accounting Office, "inaccurate and incomplete data may lead to restrictive measures being adopted on innocent people ("false positives"), at the same time impinging on the capacity to effectively target their real addressees ("false negatives")."[26]

The legal frameworks of both the data protection and data security regimes in the area of law enforcement appear quite fragmented, as set out in Table 1 above. They lack a joined-up approach which would increase their operability and the confidence of the general public in the system. In addition, the impact of both the regulatory authorities in this area and the EU Charter of Fundamental Rights are relevant. The coming into force of the Lisbon Treaty gives rise to opportunities to resolve a number of the issues discussed in this paper, should the EU Member States, and the various institutional actors in this field, choose to grasp this opportunity. What will become clear is that, as has been recognised by the Commission when drafting an amending regulation for Frontex[27], an "overall strategy for information exchange"[28] which is to be presented later in 2010, is required, which will take "into account the reflection to be carried out on how to further develop cooperation between Agencies in the justice and home affairs field as requested by the

[20] M. Foucault, *Discipline and Punish: The Birth of the Prison*, (Penguin 1977).
[21] Grant, Data protection 1998-2008, 25 (2009) *Computer Law & Security Review* 44-50, p.45.
[22] 2003 EWCA Civ. 1746.
[23] 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, OL L 281/31.
[24] 1st December 2009.
[25] H. Hijmans and A. Scirocco, n4 above, at p.1493.
[26] *ibid.* at page 1511.
[27] Proposal for a Regulation amending Council Regulation (EC) No 2007/2004, n2 above.
[28] *ibid.* at page 4 of the introduction.

Stockholm programme."[29] The same can be said about the data security provisions, which to even a non-security cleared outsider, without access to the relevant detail, look disjointed.

This article intends to critically examine these issues of data protection and data security as they arise in the context of law enforcement within the various EU agencies, such as Europol[30], Eurojust[31], and through the Schengen Information System[32], and to locate their provisions within the larger EU law enforcement picture.

Data protection in the pre-Lisbon first pillar

The most coherent legal framework on data protection has developed in the pre-Lisbon first pillar of the EU, pursuant to Directive 95/46/EC.[33] It is to be interpreted on the basis that data protection rights are not absolute, but are to be balanced with other fundamental rights, which in the *Promusicae* case required the balancing of the data protection rights with the right "to the protection of property".[34] This is despite the fact that the right to data protection is expressly provided for in Article 8 of the EU Charter on Fundamental Rights 2000. If the right to data protection, and its ancillary right to privacy can be counterbalanced by a right to property under the EC commercial law jurisprudence, then the right to data protection and privacy will all the more be compromised by the needs of the law enforcement community in legitimate crime detection and crime prevention activities. At the other end of the scale, as stated by Peers, the right to data protection would also appear to have to defer to "the right of freedom of expression and the right of access to documents" on the basis of the "democratic society" principle, which "would point towards the release of information concerning lobbying of public authorities and MEP's private interests".[35] In addition, in the pre-Lisbon *Neukomm* and *Rundfunk* judgement[36], the ECJ was prepared to compromise the right to data protection for the sake of the "proper management of public funds"[37], where the names of recipients of personal remuneration over a particular high threshold paid from the public purse were to be widely disclosed, as well as the amount of their remuneration. The data protection directive was interpreted in "light of Article 8 ECHR including the prospect of limitations under Article 8(2)".[38] References were made in the case to "Strasbourg case law and principles" to include "the specific objectives justifying a limitation on the right, the requirement that limits be 'prescribed by law' and 'necessary in a democratic society', the Strasbourg proportionality test and the margin of appreciation".[39] The right to data protection, therefore, is not an "absolute prerogative and can be subject to restrictions in the general interest".[40] It is only the "right to life and the right to be free from torture or

[29] *ibid.* at page 4/5 of the introduction.
[30] Europol Convention 1995, but to be replaced by the Europol Council Decision 2009/371/JHAof 6 April 2009 establishing the Europol Police Office (Europol), OJ L 121/6, which came into force on the 1st January 2010.
[31] Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, OJ L 63/1.
[32] Schengen Convention 1990.
[33] Directive 95/46/EC, n23 above.
[34] Case C-275/06 *Productores de Música de España (Promusicae)* v. *Telefónica de España SAU* [2008] ECR I-271.
[35] S. Peers: Taking Rights Away? Limitations and Derogations, p. 141, Chapter 6 in Steve Peers and Angela Ward (eds.) The EU charter of fundamental rights politics, law and policy, essays in European Law, Hart Publishing, Oxford and Portland Oregon, 2004, p.168.
[36] Joined Cases C-465/00, C-138/01 and C-139/01; *Neukomm* and *Rundfunk* [2003] ECR page I-04989.
[37] At paragraphs 50 and 94 of the Judgment, and paragraph 1 of the ruling.
[38] S.Peers, n35 above, p.144.
[39] *ibid.* p.144.
[40] *ibid.* p.143.

inhuman or degrading treatment or punishment" which can be seen to be absolute and non-derogable.[41]

The pre-Lisbon legal status of the Charter of Fundamental Rights was "something paradoxical"[42], given its status as "soft law"[43], not having any formal legal effect, being "merely a political statement"[44], but still having a profound effect on the operation of the EU in general, and the jurisprudence of the ECJ in particular. As Cartabia has pointed out, the Charter had given a new lease of life to the "creative ability of the European Court" pre-Lisbon.[45] This creative ability of the ECJ will continue to be relevant in the post-Lisbon framework, with the post-Lisbon Article 6.1 TEU upgrading the Charter to the same legal status as the Treaties.[46] It must be pointed out however, that this upgrading of the Charter is subject to a UK and Polish opt-out[47], to the extent that the Charter "will not be justiciable in British courts or alter British law".[48] The UK was, however, party to the "solemn proclamation at the Nice European Council of December 2000" which, according to Ward, "amounts to persuasive evidence in determining the content of fundamental rights that are judicially enforceable in the EU system".[49] The extent to which the UK and Polish opt-out from Article 6.1 TEU, post-Lisbon but still subject to the effect of the "solemn proclamation" at Nice, will have an effect on the impact of ECJ jurisprudence on these two Member States, to which they are still bound, has yet to be established. In addition, pre-Lisbon the European Union Agency for Fundamental Rights has already been set up[50] under the pre-Lisbon framework and the ECJ had already adjudicated on Directive 95/46/EC, using, not Article 8 of the EU Charter, but Article 8 ECHR.[51]

Article 16 TFEU expressly provides a treaty provision for data protection regulation post-Lisbon. This article provides little detail, however, apart from stating at Article 16.1 that "Everyone has the right to the protection of personal data concerning them". It does provide that the provisions in Article 16 are to be "without prejudice to the specific rules laid down in Article 39" TEU, which deals with data protection within the Common Foreign and Security Policy (CFSP). Article 16 TFEU does become subject to Article 6a of UK and Ireland's post-Lisbon Schengen Protocol,[52] which, quite logically provides that any data protection provisions adopted with regard to judicial cooperation and police cooperation which forms part of the Schengen *acquis*, which either country has not subsequently opted into, will not apply to them. A similar "even more complicated"[53] Schengen relevant derogation has also been provided for Denmark in its post-Lisbon Schengen protocol.[54]

---

[41] *ibid.* referring to the Case C-112/00, *Schmidberger* [2003] ECR p.I-05659
[42] M. Cartabia: Europe and Rights: Taking Dialogue Seriously, European Constitutional Law Review, 5: 5-31, 2009, p.15.
[43] J. Dine; Criminal Law and the Privilege Against Self-Incrimination, p. 269, Chapter 11 in Steve Peers and Angela Ward (eds.) The EU charter of fundamental rights politics, law and policy, essays in European Law, Hart Publishing, Oxford and Portland Oregon, 2004, p.270.
[44] M. Cartabia, n42 above, p.15.
[45] *ibid.* p.8.
[46] As elaborated further in Protocol (No. 8) Relating to Article 6(2) of the Treaty on European Union on the accession of the Union to the European Convention on the Protection of Human Rights and Fundamental Freedoms, attached to both the TEU and the TFEU.
[47] Protocol (No. 30) on the application of the charter of fundamental rights of the European Union to Poland and to the United Kingdom, attached to both the TEU and the TFEU.
[48] F. Ferretti, "The "Credit Scoring Pandemic" and the European Vaccine: Making Sense of EU Data Protection Legislation, 2009 (1) *Journal of Information, Law & Technology*, p.11.
[49] A. Ward; Access to Justice, p. 123, Chapter 5 in Steve Peers and Angela Ward (eds.) The EU charter of fundamental rights politics, law and policy, essays in European Law, Hart Publishing, Oxford and Portland Oregon, 2004, p.127.
[50] Regulation (EC) No. 168/2007 of 15 February 2007, OJ L 53/2 22.2.2007.
[51] Joined Cases C-465/00, C-138/01 and C-139/01; *Neukomm* and *Rundfunk* [2003] ECR page I-04989.
[52] Protocol (No. 21) on the position of the United Kingdom and Ireland in respect of the Area of Freedom, Security and Justice.
[53] H. Hijmans and A. Scirocco, n4 above, p.1516.
[54] Article 7 of Protocol (No 22) on the Position of Denmark.

The drafting of updates to the EU data protection provisions, therefore, needs to be clear on whether it is to form part of the core EU provisions, or to be subject to the various continuing Schengen opt-out provisions. Nevertheless, it is fair to say, that the Lisbon Treaty "improves the judicial protection of citizens"[55] for pre-Lisbon second and third pillar issues. As has been pointed out by Hijmans and Scirocco, this will happen, in particular, "after the expiry of the transitional period of 5 years" set out in Protocol no. 36 attached to the TEU and TFEU, which "despite" the provision contained in Protocol no. 30, "on the application of the Charter of Fundamental Rights of the European Union to Poland and to the United Kingdom".[56]

Directive 95/46/EC has been complemented by Regulation 45/2001[57] to provide data protection to "data subjects" when their data is being processed by EC institutions and bodies. Frontex, a pillar I law enforcement agency provides[58] that Regulation 45/2001 is to apply to its processing of personal data. Article 8.3 of the 2000 Charter requires that "compliance with these [data protection] rules shall be subject to control by an independent authority". Such an authority is the European Data Protection Supervisor (EDPS) whose position was established by Regulation 45/2001/EC.[59]

This coherent structure set up for Pillar I activities, to include Pillar I law enforcement activities, was not transferred to Pillar III Police and Judicial Co-operation (PJCCM) activities, which of itself becomes an issue in the post-Lisbon framework. Both previous pillars have now been reintegrated into the unitary post-Lisbon treaty framework, all be it with continuing exceptions for the Common Foreign and Security Policy (CFSP), which now has its own data protection provisions under Article 39 TEU. "Public security, defence, state security…. and the activities of the State in the areas of criminal law" were expressly provided as exceptions to Directive 95/46/EC[60], as were the activities of "Titles V and VI of the Treaty on European Union"[61], *i.e.* the then CFSP and PJCCM policy areas. Equally, standard data protection rules could be curtailed where data originally collected for non-law enforcement matters were now required for law enforcement purposes, to include taxation matters.[62] A clear division between the commercial and law enforcement data protection activities had always been envisaged. In addition, the EDPS did not, in the pre-Lisbon framework, have competence to supervise the activities of "bodies established outside the Community framework".[63] A fractured structure develops when the provisions of the pre-Lisbon third pillar is examined. Now that the PJCCM agencies are to be brought into the post-Lisbon EU framework, their data protection and data security provisions need to be re-examined.

Not only were PJCCM policy areas more politically contentious than perhaps those in the EC pillar, but "police information is something completely different"[64] from data processed by the private sector for commercial purposes. As pointed out by de Hert and Papakonstantinou, police data can often, until an investigation develops, be "based on uncertain facts or on assumptions and hearsay", which does not match the nature of hard

[55] H. Hijmans and A. Scirocco, n4 above, p.1523.
[56] *ibid.*
[57] Regulation (EC) No. 45/2001 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8/1.
[58] At paragraph 19 to the preamble to Council Regulation (EC) No 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, OJ L 349/1.
[59] Regulation (EC) No. 45/2001, n57 above, at Articles 41 to 48.
[60] Directive 95/46/EC, n.23 above, at Article 3.2 first indent.
[61] *ibid.* at Article 3.2 first indent.
[62] *ibid.* at Article 13.1.
[63] Regulation (EC) No. 45/2001, n57 above, at paragraph 16 of the Preamble.
[64] De Hert, Papakonstantinou, n6 above, p.408.

data covered by the mainstream data protection directive.[65] While the pillar issues may have been resolved by the Lisbon Treaty, the nature of data being used in law enforcement operations remains quite different to commercial data post-Lisbon and will probably continue to require a separate legal regime.

In addition, the issue of data security comes squarely into the picture when dealing with police intelligence and covert surveillance 'data'. While provisions are made in Regulation 45/2001 to deal with issues of professional secrecy by the EDPS "with regard to any confidential information which has come to their knowledge in the course of the performance of their official duties"[66], this is not quite the same issue as the law enforcement security classifications covered in Council Act of 3 November 1998[67], which deals with Europol data security classifications.

Provisions were made for data security provisions in the EC, and throughout the EU, but outwith Europol, by Council Decision 2001/264/EC[68] as subsequently amended.[69] While some of these provisions focus on industrial security, namely Council Decision 2005/952/EC, it is clear that national security is also covered, with the EU classifications of "EU Top Secret", "EU Secret", "EU Confidential" and "EU restricted" being mapped, not only against national security classifications of the EU Member States, but also those of the military organisations of NATO and the Western European Union.[70] The proposed reform of the Frontex legal framework will make express reference to the application of Commission Decision 2001/844/EC, ECSC, Euratom, which brings with it the security classification regime set out in Council Decision 2001/264/EC.[71]

The pre-Lisbon third pillar: the 'standard' rules

While accepting that policing relating data may require a separate legal regime from the one being used for commercial data, but reflecting "the tension between the quest for effectiveness on the one hand and the preservation of state sovereignty on the other"[72], it is regrettable to note that there is not one policing data protection regime, but many. Council Framework Decision 2008/977/JHA[73] appears to give a unitary response to the issue of data protection for EU law enforcement activities, but its provisions are subject to so many exceptions that the question does arise as to its actual applicability. The Framework Decision, which is deemed to form part of the Schengen *acquis*[74], purports to provide "a high level of protection of the fundamental rights and freedoms of national persons, in particular their right to privacy"[75] for PJCCM related data processing. However,

---

[65] *ibid.*
[66] Regulation (EC) No. 45/2001, n57 above, at Article 45. .
[67] Council Act of 3 November 1998 adopting rules on the confidentiality of Europol information 1999 OJ C 316/1.
[68] Council Decision 2001/264/EC of 19 March 2001 adopting the Council's security regulations, OJ L 101/1.
[69] Council Decision 2004/194/EC of 10 February 2004 amending Decision 2001/264/EC adopting the Council's security regulations, (2004/194/EC) OJ L 63/48, Council Decision of 12 July 2005 amending Decision 2001/264/EC adopting the Council's security regulations (2005/571/EC), OJ L 193/1, Council Decision of 20 December 2005 amending Decision 2001/264/EC adopting the Council's security regulations (2005/952/EC), OJ L 346/18, and Council Decision of 18 June 2007 amending Decision 2001/264/EC adopting the Council's security regulations, (2007/438/EC),OJ L 164/24.
[70] *ibid.*
[71] Proposed new Article 11.b at point 15 of Proposal for a Regulation amending Council Regulation (EC) No 2007/2004, n2 above.
[72] V. Mitsilegas; The third wave of third pillar law. Which direction for EU criminal justice, E.L.Rev. 2009, 34(4), 523-560, p.560.
[73] Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350/60.
[74] With not only the UK and Ireland opting into these provisions, but also involving Norway, Iceland, Switzerland and Lichtenstein.
[75] Council Framework Decision 2008/977/JHA, n.73 above, at Article 1.

its actual scope is "very limited".[76] As one would expect, the "transmission of personal data by the judiciary, police or customs (…) in the context of criminal proceedings" is excluded.[77] The issue of data protection in the case of law enforcement activities solely within one Member State remains a matter for individual Member States to address.[78] While the Council Framework Decision 2008/977/JHA provisions are not only "without prejudice to essential national security interests and specific intelligence activities in the field of national security"[79] which may be across EU borders[80], also exempted are the "data protection provisions of (…) Europol, Eurojust, the Schengen Information System (SIS) and the Customs Information System (CIS)".[81] Paragraph 39 of the Preamble also removes from its ambit data being processed pursuant to Council Decision 2008/615/JHA, the Prüm Decision[82], which applies (only) to all EU Member States. As has been pointed out, "it is questionable how these limitations are to work in practice".[83] In addition, for Framework Decision 2008/977 to apply, it must be foreseeable, "at the moment of the collection of personal data by a police authority" that the "data might at a later stage be used in a cross-border context".[84] Police enquiries often develop in unexpected directions, so it would appear that it is only planned transnational operations that were envisaged as being the subject matter of this Framework Decision, which are not to use any of the EU transnational policing structures. While the intention behind the Framework Decision was to develop a more comprehensive legal framework than what eventually emerged, its precursor "negotiations proved lengthy and controversial", with EU Member States making "a number of attempts to water down the text" and tabling "a number of [amending] proposals".[85] De Hert and Papakonstantinou point out that the Framework Decision "attempted to strike an admittedly difficult to find balance between instruments already in effect and their provisions". The resulting legal provisions in Framework Decision 2008/977 is such that Hijmans and Scirocco are of the view that it "does not fulfil the criteria of Article 16 TFEU", thereby placing and obligation on the EU legislators "to replace it by a new legislative instrument."[86] It is argued here that the entire data protection and data security structure needs to be reviewed.

The data protection and security regime at Europol

The agency that has led the way in dealing with law enforcement issues at the EU level is Europol. The Europol Convention 1995 was necessarily drafted against the backdrop of a legal framework on data protection, and transnational law enforcement which is now outdated, when compared with the provisions of the recent Europol Council Decision.[87] The Europol Convention had been updated by three Protocols[88], and a number of Council

[76] V. Mitsilegas, n72 above, p.559.
[77] Council Framework Decision 2008/977/JHA, n.73 above, at paragraph 18 of the Preamble.
[78] *ibid.* at paragraph 6 of the Preamble.
[79] *ibid.* at Article 1.4.
[80] *ibid.* at Article 1.4.
[81] *ibid.* at paragraph 39.
[82] Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ.L 210/1.
[83] H. Hijmans and A. Scirocco, n4 above, p.1494.
[84] *ibid.*
[85] V. Mitsilegas, n72 above, p.558.
[86] H. Hijmans and A. Scirocco, n4 above, p.1519.
[87] Council Decision 2009/371/JHA establishing the European Police Office, OJ L121/37.
[88] Council Act of 30 November 2000 drawing up on the basis of Article 43(1) of the Convention on the establishment of a European Police Office (Europol Convention) of a Protocol amending Article 2 and the Annex to that Convention (2000/C 358/01) OJ C 358/1(the Money laundering protocol, in force 29th March 2007), Council Act of 28th November 2002 drawing up a Protocol amending the Convention on the establishment of a European Police Office (Europol Convention) and the Protocol on the privileges and immunities of Europol, the members of its organs, the deputy directors and the employees of Europol, (2002/C 312/01) OJ C 312/1 (the Joint Investigations Teams Protocol, in force 29th March 2007), and the Council Act of

acts.[89] The Europol Council Decision, which moves the focus from organised crime to serious crime, thereby "broadening Europol's mandate"[90], takes into account these various updated pieces of legislation in its drafting of a new legal framework for Europol. The general EU principle of public access to documentation, as set out in Regulation (EC) No. 1049/2001[91], while enshrined in the Europol Council Decision[92], has to be understood against the backdrop of Europol data protection, data security and security classification provisions.

The key function of Europol is the processing of data for the purposes of crime prevention and enforcement, with the new Europol legal basis providing for the "intensification of data collection, analysis and exchange", which is to be allied to a "new system" for the processing of data".[93] Data protection provisions at Europol would therefore cover a very high volume of personal data which is being processed in the context of law enforcement. The use of personal data at Europol, under the Council Decision, is therefore restricted for the purposes of preventing and combating "crimes in respect of which Europol is competent, and [preventing and combating] other serious forms of crime" with Europol being empowered to use such data "only for the performance of its tasks."[94] The Council Decision does, however, increase the time limit for data storage to "three plus three years".[95] The Council Decision also envisages greater access to Europol data by national Europol units, access by outside experts to Europol analysis work files, for example US law enforcement agencies for relevant cases or operations, and access to data relevant to them, to a diverse range of other agencies and bodies,[96] to include third states and Interpol.[97]

A control mechanism has been put in place "to allow the verification of the legality of retrievals from any of its automated data files"[98] with all such requests being logged, and audited upon request[99] by Europol, its National Supervisory Bodies[100], and the Joint Supervisory Body.[101] The roles of the National and Joint Supervisory Bodies remain

---

27th November 2003 drawing up, on the basis of Article 43() of the Convention on the Establishment of a European Police Office (Europol Convention), a Protocol amending that Convention, (2004/C 2/01), OJ C 2/1 (The "Danish" Protocol, in force the 18th April 2007).

[89] Council Act 1999/C 26/01, of 3 November 1998 adopting rules applicable to Europol analysis files, OJ C 26/1. Act of the Management Board of Europol of 15 October 1998 concerning the rights and obligations of liaison officers, (1999/c 26/09), OJ C 26/86, Council Act of 3 November 1998 adopting rules on the confidentiality of Europol information (1999/C 26/01) OJ C 26/10, which contains the security classifications for data, Council Act of 18 January 1999 adopting the Financial Regulation applicable to the budget of Europol (1999/C 25/01) OJ C 25/1, Council Act of 3 November 1998 laying down rules concerning the receipt of information by Europol form third parties, (1999/C 26/03), OJ C 26/17, Act of the Management Board of Europol of 15 October 1998 laying down the rules governing Europol's external relations with European Union- related bodies (1999/C 26/0) OJ C 26/89, Council Act of 3 November 1998 laying down rules governing Europol's external relations with third States and non-European Union related bodies (1999/C 26/04) OJ C 26/19, Council Act of 12 March 1999 adopting the rules governing the transmission of personal data by Europol to third States and third bodies (1999/C 88/01) OJ C 88/01, as amended, by Council Act of 28 February 2002 amending the Council Act of 12 March 1999 adopting the rules governing the transmission of perusal data by Europol to third States and third bodies (2002/C 58/02), OJ C 58/12 (which is really about onward transmission of data),

[90] V. Mitsilegas, n72 above, p.551.

[91] Regulation (EC) No. 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council, and Commission documents, OJ L 101/1.

[92] Council Decision 2009/371/JHA, n87 above, at Article 45.

[93] V. Mitsilegas, n72 above, p.551.

[94] Council Decision 2009/371/JHA, n87 above, at Article 19.1.

[95] V. Mitsilegas, n72 above, p.552.

[96] To include Eurojust, OLAF, Frontex, CEPOL, the European Central Bank and the European Monitoring Centre for Drug Addiction.

[97] V. Mitsilegas, n72 above, p.552.

[98] Council Decision 2009/371/JHA, n87 above, at Article 18.

[99] *ibid.*

[100] *ibid.* at Article 33.

[101] *ibid.* at Article 34.

essentially the same as those which operated under the Europol Convention 1995, with "any person" having the right to ask his or her national supervisory body to "ensure that the input or communication to Europol of data concerning him or her in any form and the consultation of the data by the Member State concerned are lawful"[102], with that right to be "exercised in accordance with the national law of the Member State in which the request is made".[103] The Joint Supervisory Body is more interested in the processes used by Europol, with their role being to "review (…) the activities of Europol" ensuring that individual rights "are not violated by the storage, processing and use of the data held by Europol".[104] The Joint Supervisory Body is also to ensure that the transfer of data to other organisations from Europol is permissible.[105] Should the Joint Supervisory Body identify any violations in "the storage, processing or use of personal data", then it will require the Director of Europol to address the issue within a set time limit.[106]

The standard of data protection continues to be those of the Council of Europe[107], rather than the standards set out in Directive 95/46/EC[108] or even Regulation 45/2001.[109] Equally, no reference is made to Council Framework Decision 2008/977/JHA[110], which one would assume must have been familiar to the drafters of the 2009 Europol Council Decision.[111] It is possible, however, that different teams were responsible for drafting various pieces of legislation, hence the lack of joined-up thinking evident from their comparative analysis. The standard rule on data protection at Europol, under the Council Decision, is that data shall only be held "for as long as is necessary" for Europol to perform its tasks[112], with data to be reviewed every three years, with "Europol [to] automatically inform the Member States three months in advance of the expiry of the time limits for reviewing the storage of data".[113]

A new development at Europol is the appointment of a data protection officer[114], who, while being a member of staff of Europol, is to act independently. He or she will "have access to all the data processed by Europol and to all Europol premises"[115], so presumably the data protection officer will have all the necessary clearances to review top secret as well as other secret, confidential and restricted materials held at Europol, as classified by Council Act of 3 November 1998[116], as amended[117], in order to properly comply with this requirement. The Europol Data Protection Officer is required, *inter alia*, to cooperate with the Joint Supervisory Body in fulfilling his tasks, and it would be expected from their joint responsibility on data protection matters, and the protection of individuals, that this relationship with the Joint Supervisory Body would be quite close. Nevertheless, the individual complaints on personal data being processed by Europol would still be directed

[102] *ibid.* at Article 33.2.
[103] *ibid.* at Article 33.2.
[104] *ibid.* at Article 34.1.
[105] *ibid.* at Article 34.1.
[106] *ibid.* at Article 34.4.
[107] *ibid.* at Article 27, which refers to Council of Europe Convention of the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 and of Recommendation No. r (87) 15 of the Committee of Ministers of the Council of Europe of 17 September 1987.
[108] Directive 95/46/EC, n23 above.
[109] Regulation (EC) No. 45/2001, n57 above.
[110] Council Framework Decision 2008/977/JHA, n.73 above.
[111] Council Decision 2009/371/JHA, n87 above.
[112] *ibid.* at Article 20.1.
[113] *ibid.*
[114] *ibid.* at Article 28.
[115] *ibid.* at Article 28.3.
[116] Council Act of 3 November 1998, n67 above.
[117] Council Act of 5 June 2003 amending the Council Act of 3 November 1998 adopting rules on the confidentiality of Europol information, (2003) OJ C 152/01, and now, for the most part, reiterated in Council Decision 2009/968/JHA of 30 November 2009 adopting the rules on the confidentiality of Europol information, OJ L 332/17, which came into force on the 1st January 2010.

to the relevant National Supervisory Body. All parties entering data onto the Europol data processing systems remain responsible for ensuring, both from a data protection perspective, and law enforcement perspective, that data entered is correct, and also complies with rules on the legality of the collection of that data, as well as the rules on the "storage time limits" of that data.[118]

Data security provisions within Europol were initially set out in Article 25 of the Europol Convention, now Article 35 of the Europol Council Decision, and has been supplemented by a number of secondary legal instruments. In addition, the Europol Council Decision now expressly refers to the EU system of classified information in Article 46, requiring Europol to "apply the security principles and minimum standards set out in Council Decision 2001/264/EC[119] with regard to EU classified information, which has since been amended.[120] The issue of the confidentiality of information, with the allocation of classifications Europol 1, 2 and 3 being allocated to what both the UK and Ireland would classify as "confidential", "secret" and "top secret", was originally covered in Council Act of 3 November 1998.[121] The "confidential" classification was then sub-divided in 2003 to cover a "Europol Restricted" and a "Europol Confidential" classification level, with the new default classification to be "Europol Unclassified not for public dissemination".[122] The purpose for this re-alignment of security classifications in 2003 was in order "that they correspond as far as possible to the levels currently applied within the institutions of the European Union and to existing international standards".[123] The EU-wide classification standards, which does not include Europol, had been put in place pursuant to Council Decision 2001/264/EC,[124] and has been subsequently amended and elaborated upon.[125] In addition, Europol has developed its own security manual.[126]

Member states providing the data to Europol select the security classification appropriate for the information[127], taking into account both the need for "operational flexibility" within Europol, as well as "the classification of the information under (…) national regulations".[128] All information between 2003, and up to and including 2009, was normally given the marking "Europol Unclassified not for public dissemination" unless a classification level had been assigned to it.[129] This situation is now dealt with by ensuring that "all information processed by or through Europol" is "subject to a basic protection level within Europol and in the Member States", unless such information "is expressly marked or is clearly recognisable as being public information".[130] Higher classifications are to be "assigned (…) only where strictly necessary and for the time necessary"[131], "taking account of the detrimental effect which unauthorised access, dissemination or use of the information might have on the interests of Europol or the Member States."[132] Packages of information can be classified together, with the highest classification of an individual piece of

[118] Council Decision 2009/371/JHA, n87 above, at Article 29.1.
[119] Council Decision 2001/264/EC, n68 above.
[120] Council Decision 2004/194/EC of 10 February 2004 amending Decision 2001/264/EC adopting the Council's security regulations, OJ L 63, 28/02/2004 p. 48.
[121] Council Act of 3 November 1998, n67 above.
[122] Council Act of 5 June 2003 amending the Council Act of 3 November 1998, adopting rules on the confidentiality of Europol information, (2003) OJ C 152/01, at Article 1.2.
[123] *ibid.* at paragraph 1 of the preamble.
[124] Council Decision 2001/264/EC, n68 above.
[125] Council Decision 2004/194/EC, n120 above.
[126] Council Act of 3 November 1998, n67 above, at Article 6, and reiterated in Council Decision 2009/968/JHA of 30 November 2009 adopting the rules on the confidentiality of Europol information, OJ L 332/17, at Article 7.
[127] Council Decision 2009/968/JHA of 30 November 2009, adopting the rules on the confidentiality of Europol information, OJ L 332/17, at Article 11.1.
[128] *ibid.* at Article 11.2.
[129] Council Act of 5 June 2003, n122 above, at Article 8(1) of the 1998 Act as amended.
[130] Council Decision 2009/968/JHA, n127 above, at Article 10.1.
[131] *ibid.* at Article 10.3.
[132] *ibid.* at Article 10.4.

information in the package, applying to the package of information as a whole.[133] In addition, it is possible for a package of information to be given a higher classification than the sum of its parts.

Europol may come "to the conclusion that the choice of classification level needs changing" and will, in such a case, "inform the Member State concerned" with a view to obtaining agreement to such change.[134] In the event that agreement to the change is not forthcoming, Europol has no power to "specify, change, add or remove a classification level without such agreement".[135] If Europol manages to generate its own information, it will obtain consent from the Member State which provided the basic information as to the classification level to be applied to the information.[136] If there was no such basic information from a Member State, Europol will determine itself which security classification applies to the information.[137] Amendments of classification levels is also possible, as information gains a greater or lesser importance as operations develop, with the member state supplying the information maintaining control over its security classification.[138]

At Europol, the security of data is controlled by the Europol Security Committee, "consisting of representatives of the Member States and of Europol"[139], the Security Coordinator[140] who is "directly answerable to the Director of Europol", and security officers.[141] The Security Coordinator is to hold "security clearance to the highest level under the regulations applicable in the Member State of which the Security Coordinator is a national".[142] This security clearance level will now have to cover those levels of relevance to counter-terrorism operations. The 2009 reforms bring in provisions for a number of security officers, more than the original one, under the 1998 regulations, who are now to "be security cleared to the appropriate level required by their duties" in accordance with "the laws and regulations applicable in the Member States of which they are a national".[143] All of these structures operate within the framework set down in the security manual[144], which was adopted "by the Management Board after consultation with the Security Committee".[145] The processing of data by Europol will only be done by people who "by reason of their duties or obligations, need to be acquainted with such information or to handle it"[146] and who have obtained "an appropriate security clearance and shall further receive special training".[147] Subject to a veto by the supplying Member State,[148] an exception to the strict security clearance rules can be granted by the Security Coordinator, after consulting a security officer, and following the specified exceptions laid down in the Council Decision. This exception is limited to access to EU secret material, where their security clearance only grants them access to EU confidential material. This could be, for reason that "if, by reason of their duties or obligation, in a specific case,"[149] a particular

[133] *ibid.* at Article 10.4, paragraph 3.
[134] *ibid.* at Article 11.3.
[135] *ibid.*
[136] *ibid.* at Article 11.4.
[137] *ibid.* at Article 11.5.
[138] *ibid.* at Article 12.
[139] *ibid.* at Article 4.
[140] *ibid.* at Article 5.
[141] *ibid.* at Article 6.
[142] *ibid.* at Article 5.
[143] *ibid.* at Article 6.2.
[144] *ibid.* at Article 7.
[145] *ibid.*
[146] *ibid.* at Article 13.1.
[147] *ibid.*
[148] *ibid.* at Article 13.4.
[149] *ibid.* at Article 13.3.a.

individual needs "to have access to specific information classified up to Secret UE/EU Secret".[150]

While the new security classification system is now in place for EU activities, to include military activities, Europol continues to maintain a separate classification system pursuant to the 1998 Council Act, as amended. The requirement on Europol is to maintain at least the standards as used by the rest of the EU.[151] Presumably Europol is of the view that its standards are higher, in order to maintain a separate classification regime. The issues here are not so much the over-interconnectedness of databases, but the lack of such connections, due to different data security provisions, with intelligence, for example, collected by Frontex on trafficking in human beings by organised crime across the external border of the EU, not being shareable with organised crime police who share their intelligence via Europol. The connections between Europol and Eurojust are similarly fractured. While commercially collected data may well become available to law enforcement officers, law enforcement data is highly controlled, and will not, at least without a criminal offence having been committed by somebody legitimately in possession of such data, become available for other purposes.

At some point, interoperability of databases and inter-agency collaboration in law enforcement activities needs to be facilitated. The proposed reforms to Fontex[152], a traditional pillar I law enforcement body, will give an express but limited mandate to process personal data "related to the fight against criminal networks organising illegal immigration".[153] It will also be given its own Data Protection Officer.[154] The entirety of Frontex operations are to be under the supervision of the European Data Protection Officer[155] and operate under the EU provisions on data security, [156] rather than the Europol ones.[157] One can only ask as how effectively data can be exchanged in this emerging situation between Europol and Frontex in areas of overlapping operational competence and interest, while still meeting the requirements of data protection due to the data subject.

The changes brought in by the Lisbon Treaty should not make any significant difference to the Europol data protection and security classification system, with the exception that future updates of the Europol legal framework may well be through Regulation. Worth commenting on, however, is the ability for Europol to operate within a full data protection regime, with the appointment of an independent data protection officer, something that Eurojust was in a position to deal with some years ago, but had been problematic for the law enforcement community for so many years. If Europol is now in a position to have its own data protection officer, why then is there not a coherent unified data protection framework for all law enforcement provisions, recognising that the data protection provisions originally designed for pillar I EC activities may not be the most appropriate structure for transferral to policing activities.

[150] *ibid.*
[151] Council Decision 2001/264/EC, n68 above.
[152] Proposal for a Regulation amending Council Regulation (EC) No 2007/2004, n2 above.
[153] *ibid.* in page 4 of the introduction to the Proposal.
[154] *ibid.* in the proposed new Article 11a. at point number 15 of the proposal.
[155] *ibid.* in paragraph 25 of the introduction to the proposal.
[156] Council Decision 2001/264/EC, n68 above.
[157] Council Decision 2009/968/JHA, n127 above.

The data protection and security regime at Eurojust

At some point in an investigation, both Europol and Frontex will want to engage the services of Eurojust in their operations. Set up as the partner organisation to Europol, Eurojust was created pursuant to Council Decision 2002/187/JHA[158], and had, from its very beginning, provisions on data protection[159] and security[160], to include the provisions for its own "specially appointed Data Protection Officer, who shall be a member of the staff"[161], a provision which the Europol reforms have just provided for, and the proposed reforms to Frontex will also cover. Eurojust, which calls itself the network for investigating and prosecuting magistrates, but which also has a role for senior police officers when they are allocated the role of leading police investigations in a particular jurisdiction[162], was updated pursuant to Council Decision 2003/659/JHA.[163] This deals with its budgetary and financial provisions. Eurojust is about to be much more substantially revised pursuant to Council Decision 2009/426/JHA[164], which is to come into force "no later than 4 June 2011".[165] Much of the original provisions on data protection and data security continue unaltered by the 2009 Council Decision. The capacity for Eurojust to engage in data "collection, processing and exchange" has however "been extended quite considerably".[166] A new Article 39a has been inserted into the Eurojust legal framework, dealing with classified information, with Eurojust to adopt the "security principles and minimum standards" of the EU security classification system, as set out in Council Decision 2001/264/EC[167] discussed above, and not those being used by its partner institution, Europol. If indeed there is a difference between the EU and Europol security classification frameworks, and if Eurojust, after the coming into force of the 2009 Council Decision is to provide a 27/4 legal advice service to Europol (and possibly also to Frontex), with the role of senior investigating police officers and investigating magistrates being serviced by the Eurojust legal framework, rather than that of Europol, why then is Eurojust taking a different line on these issues than Europol? These two organisations need to work more closely together than does Eurojust with any other law enforcement framework or body. This has been recognised by the fact that Eurojust and Europol have been co-located at The Hague. In addition, both Eurojust and Europol could be involved in joint investigation teams, set up by the 2000 EU Convention on Mutual Assistance on Criminal Matters. An opportunity to align the two organisations in a more streamlined fashion would appear to have been missed in the drafting of the two 2009 Council Decisions on Europol and Eurojust.

Data protection and security issues relating to the Schengen Information System (SIS)

Cross-EU law enforcement activities are not limited to the activities of the EU's law enforcement agencies. Point to point law enforcement contact between EU Member States is facilitated by the Schengen Information System (SIS), which is also known as SIRENE. The SIS has been set up to meet the needs of both visas, asylum, etc. issues and

[158] Council Decision 2002/187/JHA, n.31 above.
[159] *ibid.* at Articles 14 to 21, and Article 24.
[160] *ibid.* at Article 22.
[161] *ibid.* at Article 17.
[162] *ibid.* at Article 2.
[163] Council Decision 2003/659/JHA of 18 June 2003 amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime, OJ L 245/44.
[164] 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 L 138/14.
[165] *ibid.* at Article 2.1.
[166] V. Mitsilegas, n72 above, at page 555.
[167] Council Decision 2001/264/EC, n68 above.

policing matters, with the UK and Ireland only using the system for policing matters, with the rest of the EU using the system for policing and visas, asylum, etc. issues.

The provisions on data protection and data security for the SIS were drafted in 1990. They are comprised in Articles 102 to 118 of the Schengen Convention, with no reference being made to data protection officers, security classifications, or many of the newer provisions dealing with data protection and data security. Reference is made in Article 119 to the 1981 Council of Europe Convention[168] and to supporting Council of Europe materials. No attempt appears to have been made over the years to update the SIS I legal framework. However, with the development of the new SIS II information system, a new legal framework has been put in place.[169] The SIS II is to come into force when "the necessary technical and legal arrangements" have been put in place.[170] While it would appear that the legal frameworks have been in place for some time, there has been some delay from a technical point of view in getting the computer system to work. If and when the SIS II formally comes into operation, data security provisions will be found in Article 10 for Member States, and Article 16 for the whole system, with data protection provisions to be found in Articles 56 to 63.

An interesting development with regard to data protection for SIS II is the use of the (commercially focused) European Data Protection Supervisor (EDPS)[171], who in conjunction with the national data protection supervisors, will "ensure coordinated supervision of SIS II."[172] There is no separate reference to security classifications in SIS II, which is also of interest, as terrorism had been added to the SIS capability.[173] Counter-terrorism information has been part of the SIS framework since 2005.[174] From an outsider's viewpoint, this would bring with it security classification issues. Presumably the new EU-wide security classification system[175] now applies to SIS I and to SIS II as and when it comes into operation. If the argument for hiving off the policing provisions from the mainstream EC Data Protection structure was because policing essentially uses different types of data in different ways from that of the commercial world, an argument that this writer is prepared to accept[176], why then is the policing part of the SIS under the control of the "commercially focused" EDPS? Has the EDPS gone through the various security clearance requirements to render an effective service to citizens on the subject of high level classified information? If the EDPS is in a position to render an effective service, why then has Europol and Eurojust been hived off into – different from each other – packages of information, to be separately monitored for data protection purposes?

In this writer's opinion, the Council Framework Decision 2008/977/JHA[177] was a missed opportunity to develop a coherent and standardised data protection and data security classification framework for the entirety of the cross-border EU law enforcement

[168] Council of Europe Convention of the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981.
[169] Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) OJ L 205/63.
[170] *ibid.* at Article 71.3.b.
[171] *ibid.* at Article 62.
[172] *ibid.* at Article 62.1.
[173] Council Decision 2006/628/EC of 24 July 2006 fixing the date of application of Article 1(4) and (5) of Regulation (EC) No 871/2004 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism, OJ L 256, 20/09/2006 p. 15, which has since been repealed by Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 381/4.
[174] Council Decision 2005/211/JHA of 24 February 205 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism, OJ L 68/44.
[175] Council Decision 2001/264/EC, n68 above.
[176] De Hert, Papakonstantinou, n6 above, p.408.
[177] Council Framework Decision 2008/977/JHA, n.73 above.

framework. If that could not have been achieved, then at least Europol and Eurojust should have been better aligned, at the highest level, in order to ensure a free flow of information between the two organisations, without data protection and security classification issues having the potential, at any time, to hinder that flow of information, while still creating a coherent structure giving the necessary protection to the data subject.

Data protection and security issues relating to the Prüm Decision

The above complex and fractured framework for both data protection and data security is added to by further legal provisions such as those contained in the recently enacted Prüm Council Decision[178], which was based on the preceding Treaty of Prüm. This piece of legislation was passed in controversial circumstances, with the EDPS gaining an even more forceful voice within the EU, being in a position to issue a "detailed opinion"[179] on the development, which was enacted before the Council Framework Decision 2008/977/JHA.[180] The EDPS was very critical of the then lack of "a general rule on data protection in the third pillar".[181] Writing now, after the passing of the Council Framework Decision 2008/977/JHA, problems remain, as the Prüm Decision[182] relies on "local and possibly inconsistent data protection laws"[183], based on the Council of Europe Convention.[184] The Prüm Council Decision was drafted, primarily by Germany, and was presented in controversial circumstances "without an explanatory memorandum, an impact assessment, nor an estimate of the cost to Member States, or time for proper consultation with Member States and the European Parliament".[185] There is no surprise, therefore, that there is a gap in what needs to be a coherent legal framework for data protection and data security issues for the purposes of cross-border EU law enforcement.

Not only has no attempt been made for Framework Decision 2008/977/JHA to amend the Prüm Decision, but at paragraph 39 of the preamble, it expressly states that the Prüm Decision "should not be affected by this framework decision". An opportunity to close a gap in the protection of personal data, as identified by the EDPS, would appear to have been missed. While provision is made for the confidentiality[186] and security of processing[187] of personal data, it is interesting to note that no reference is made to security classification. This is despite the fact that the Prüm Decision also covers the "supply of information in order to prevent terrorist offences".[188] No reference is made in either Council Decision 2008/977/JHA, or its implementing decision Council Decision 2008/616/JHA[189], to data security classifications. Presumably the default provision in Council Decision 2001/264/EC with regard to the Council's security regulations would apply in this case.[190]

---

[178] Council Decision 2008/615/JHA, n82 above.
[179] Kierkegaard, The Prüm decision-An uncontrolled fishing expedition in "Big Brother" Europe, 24 (2008) *Computer Law & Security Report*, 243-252, p.250.
[180] Council Framework Decision 2008/977/JHA, n.73 above.
[181] Kierkegaard, n179 above, p.250.
[182] Council Decision 2008/615/JHA, n82 above.
[183] Kierkegaard, n179 above, p.250.
[184] CoE 1981 Convention, n168 above.
[185] Kierkegaard, n179 above, p.244.
[186] Council Framework Decision 2008/977/JHA, n.73 above, at Article 21.
[187] *ibid.* at Article 22.
[188] *ibid.* at Article 16.
[189] Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/616/JHA on the stepping up of cross-border cooperation particularly in combating terrorism and cross-border crime, OJ L 210/12.
[190] Council Decision 2001/264/EC, n68 above.

Other provisions on data in the pre-Lisbon third pillar

There have been some efforts to develop some joined-up thinking in the area of law enforcement, with the development of a joint data protection secretariat being set up between Europol, the Customs Information System (CIS),[191] and the Schengen Information System (SIS II) in Council Decision 2000/641/JHA.[192] One could ask why this joint development was not between Europol and Eurojust, who were both located within the same legal framework, and in the same town, when organisations based in different EU legal pillars could manage to develop this secretariat. No reference is made to classified information in this Council Decision, although presumably classified information would have to be transferred between Europol, the CIS and the SIS, who, by the way, have different data security provisions, as discussed above. The role of the joint data protection secretariat is to provide support to the joint supervisory bodies of Europol, the CIS and the SIS, and to fulfil "the tasks provided for the joint supervisory bodies as laid down in the respective Rules of Procedure of those bodies".[193]

Further data exchange between the EU Member States[194] is also facilitated by Council Framework Decision 2009/315/JHA[195], which provides for the exchange of criminal record information. This document is deigned to supplement the EU Convention on Mutual Assistance in Criminal Matters 2000.[196] Reference is made[197] to the Council of Europe Convention on data processing 1981, and to "fundamental rights" as set out in the pre-Lisbon Article 6 of the TEU and the Charter of Fundamental Rights of the European Union.[198] However, as the 2000 Convention was not expressly excluded from Council Framework Decision 2008/977/JHA[199], it would appear that the default PJCCM provisions on data protection apply in this instance. Specific provisions on security classifications are not made in Council Framework Decision 2009/315/JHA, so the default EU provisions on data security classification would also appear to apply.[200] The above legal framework is added to by Council Decision 2009/316/JHA[201] which establishes a European Criminal Records Information System (ECRIS).

Council Framework Decision 2006/960/JHA is an interestingly titled document "on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union".[202] It does not, however, cover in any great detail, the subject matter of this paper. Also applicable to Norway, Iceland and Switzerland, the intention behind Council Framework Decision 2006/960/JHA was to

---

[191] The CIS was set up pursuant to the Convention on the Use of Information Technology for Customs Purposes, OJ C 316/33.
[192] Council Decision 2000/641/JHA of 7 October 2000 establishing a secretariat for the joint supervisory data-protection bodies set up by the Convention on the Establishment of a European Police Office (Europol Convention), the Convention on the Use of Information Technology for Customs Purposes and the Convention implementing the Schengen Agreement on the gradual abolition of checks at the common borders (Schengen Convention) OJ L 271/1.
[193] *ibid.* at Article 1.
[194] Building on previous laws, to include Council Decision 2005/876/JHA of 21 November 2005 on the exchange of information extracted from the criminal record, OJ L 322, 9.12.2005, p.33, which are thereby repealed.
[195] Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States, OJ L 93/23.
[196] *ibid.* at Article 12.
[197] *ibid.* at paragraph 13 of the Preamble.
[198] *ibid.* at paragraph 18 of the Preamble.
[199] Council Framework Decision 2008/977/JHA, n.73 above.
[200] Council Decision 2001/264/EC, n68 above.
[201] Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA, OJ L 93/33.
[202] Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386/89.

improve cross-border communication by police like agencies across the EU, excluding the intelligence services[203], which remain outside the EU legal framework, even post-Lisbon. It does not prevent earlier or future provisions going further than the provisions of this Framework Directive.[204] While reference is made to confidentiality[205], no express mention is made to data security classification. Data protection issues are given greater coverage, with the first reference in legislation to the need to "strike [an] appropriate balance between fast and efficient law enforcement cooperation"[206] and "data protection, fundamental freedoms, human rights and individual liberties".[207] The Framework Decision is to be without prejudice to "bilateral or multilateral agreements (…) between Member States and third countries"[208] or agreements amongst EU member states on "mutual legal assistance or mutual recognition",[209] and is not to modify any rights or legal principles enshrined in the pre-Lisbon Article 6 EU.[210] What the Framework Decision does provide is that "established rules on data protection", whatever they are supposed to be, should be used when exchanging "information and intelligence provided for by this Framework Decision."[211] The only transnational laws referred to in this particular Framework Decision are those of the Council of Europe.[212] In effect, national laws on data protection are to be applied in operating the provisions of Council Framework Decision 2006/960/JHA. No reference is made to any of the other EU data protection or data security provisions when exchanging information and intelligence under this Framework Decision.

Operating as a stand-alone measure, not connected to any of the above is Council Decision 2005/671/JHA.[213] This legal document provides procedures to be followed in exchanging terrorist-related data, either via Europol or Eurojust,[214] but, again strangely, no reference is made in this document to either data protection or data security provisions. As these are the only two methods of transmission of data under this Council Decision, then the data protection and data security provisions of these two organisations, which differ in both respects, would apply, depending on the channels of communication used.

Prospects for future post-Lisbon cooperation and conclusion

Society is best served by more effective targeting of law enforcement activities, which is facilitated by improved intelligence. Intelligence is more than information, but is about targeting better available resources[215], with "policing beginning to think more strategically".[216] Intelligence should lead to "informed decision making"[217], allowing for the "targeting of offenders" as the "best way to use our scarce police resources".[218] A better streamlining of the structures facilitating the sharing of data between the law enforcements authorities across the EU, now that the relevant general principles have been conceded by national authorities, can be facilitated not only by structural innovation such as Europol and the Schengen Information System, but also through a more coherent

[203] *ibid.* at Article 2.a.
[204] Paragraph 8 of the Preamble to Council Framework Decision 2006/960/JHA.
[205] Council Framework Decision 2006/960/JHA, n202 above, at Article 9.
[206] *ibid.* at paragraph 11 of the Preamble.
[207] *ibid.* at paragraph 11 of the Preamble.
[208] *ibid.* at Article 1.2.
[209] *ibid.*
[210] *ibid.* at Article 1.7.
[211] *ibid.* at Article 8.1.
[212] *ibid.* at Article 8.2.
[213] Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences, OJ L 253/22.
[214] *ibid.* at Article 2.1 and 2.
[215] J. Ratcliffe; *Intelligence-Led Policing*, Willan, 2008, p.179.
[216] *ibid.* at page 213.
[217] *ibid.* at page 212
[218] *ibid.* at page 63.

data security regime, married with a more coherent data protection regime, for the protection of the individual caught up in a law enforcement investigation. As stated by the EDPS, in the context of EU frontier databases, "The sheer number of these proposals and the seemingly piecemeal way in which they are put forward make it extremely difficult for the stakeholders (European and national Parliaments, data protection authorities including EDPS, civil society) to have a full overview". [219] Exactly the same can be said for the law enforcement data protection and data security structures within the EU, from the point of view of both the data subject and the law enforcement professional. The EDPS called for "evidence that there is a master plan for all these initiatives, giving a clear sense of direction".[220] In this writer's opinion, a master plan for the law enforcement data protection and data security structures also needs to be written, and is now capable of being written under the post-Lisbon Treaty framework.

Some would argue that the development of cross-EU law enforcement provisions in the absence of cross-EU criminal defence provisions is an error, with Dine pointing out that the "relationship between national criminal law, EU criminal provisions, the jurisprudence of the European Court of Human Rights and the impact of the Charter [is] likely to fuel a highly complex debate."[221] It may well be that the post-Lisbon Article 6.1 TEU upgrading the formal status of the EU Charter on Fundamental Rights 2000 to the same legal status as the Treaties, together with Article 6.2 TEU's provisions on the European Convention for the Protection of Human Rights and Fundamental Freedoms, will prove to be the green light for the ECJ to develop an effective jurisprudence in this area. That, however, is an issue for another paper.

This article has focussed on the much narrower issue of data protection and data security, both of which have already been legislated for in the area of cross-border EU law enforcement, with both showing fissures in the EU legal framework which need to be addressed. As stated by Mitsilegas, the "proliferation of data collection mechanisms" [222] has "not been accompanied by a coherent framework for the protection of personal data and privacy".[223] The different drafting teams, over different time periods, have established hard fought for principles, against the background of the difficult legal tools that were available in the pre-Lisbon third pillar. With the decanting of the third pillar into the post-Lisbon unitary EU pillar, the possibility of streamlining the legal framework in this area becomes a reality. As Mitsilegas has pointed out, "the aim of reaching a coherent data protection legal framework for the exchange of information in criminal matters is far from being achieved".[224] Similar issues arise with regard to data security classifications.

Over time a variety of principles appear to have been accepted, to include the need for data protection supervision of active policing data, as evidenced by the provisions in the Europol Council Decision. This now appears to be feasible, despite the high levels of security classification necessary at times. Any excuses for not now providing such protection to the balance of cross-border active policing data exchange will no longer

---

[219] Preliminary Comments of the European Data Protection Supervisor on: - Communication from the Commission to the European Parliament, the council, the European Economic and Social Committee and the Committee of the Regions, "Preparing the next steps in border management in the European Union", COM (2008) 69 final – Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Examining the creation of a European Border Surveillance System (EUROSUR)", COM (2008) 68 final; - Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Report on the evaluation and future development of the FRONTEX Agency", COM(2008) 67 final, available at: http://www.edps.europa.eu/EDPSWEB/edps/pid/1

[220] *ibid.*

[221] J. Dine, n43 above, p.270.

[222] V. Mitsilegas, n72 above, p.557.

[223] *ibid.* at page 557/558.

[224] *ibid.* at page 559.

hold. The issue of whether this data protection should be provided at the national level, as is the case with the Prüm Council Decision, [225] or at the supra-national level, as with Europol, Eurojust, Frontex and the SIS, also needs to be resolved.

In addition, differences in data protection and security classification regimes between the key institutions of Europol and Eurojust no longer appear to be justified. If both institutions are to operate in a high security classification regime, married to a robust data protection framework, and both readily exchange data between themselves, then differences in regimes at the two, co-located, institutions must be inexcusable. The details of their various provisions are to be found in classified security manuals. What appears to the outside observer, however, is that different regimes operate. It can only be presumed that differences will then arise in their two security manuals, which in due course, may well give rise to problems in exchanging data, the prevention and pursuit of criminals, and the prevention of terrorism. This cannot be allowed to happen if we are truly in the business of building an Area of Freedom, Security and Justice. Newspaper headlines have followed previous failures of law enforcement and intelligence communities to share intelligence due to underlying structural failures. In particular, in the US post-9/11 a "National Criminal Intelligence Sharing Plan" had to be drafted to overcome "key problems with information and intelligence sharing across the US".[226] Anticipated problems across the EU, as well as within each of our Member States, should be avoided.

Not only is the potential for law enforcement hindered by the fractures in the EU legal framework analysed above, but the role of both the data security and data protection supervisory bodies are compromised when some parts of the data relevant to a particular investigation fall outside their area of supervision. In particular, the Joint Data Protection Secretariat set up pursuant to Decision 2000/641/JHA[227], while encompassing Europol, the CIS and the SIS, has the glaring omission of Eurojust, the organisation which co-ordinates the role of investigating magistrates/senior investigating police officers. In addition, the EDPS has been given some role in this area, but not for all law enforcement data protection issues. In this writer's view, either the EDPS should be given the entirety of the data protection role in law enforcement matters, assuming that he and his team have the necessary security clearance to deal with high-level security classified data, such as counter-terrorism data, or the entirety of the data protection supervision role in law enforcement should be given to one such person or body to deal with, separate from the commercially focused EDPS. In addition, organisations such as Europol cannot operate in a vacuum. Files need to be transferred or shared with Eurojust as investigations develop and the issue of cross-border prosecutions and arrests come to the fore. Equally, Frontex, Eurojust and Europol will also find that they have shared interests in investigating and prosecuting criminals involved in human trafficking and illegal immigrant smuggling into the EU. Their different data protection and data security regimes, as some point out, are going to pose a problem.

Post-Lisbon the opportunity arises to revisit the variety of documents reviewed in this article, which have different histories and different authors under the auspices of the Council, with should benefit of the joined-up thinking which can be normally found within the Commission. The splitting of the old Justice and Home Affairs portfolio into two departments within the Commission, post-Lisbon, the Justice, Fundamental Rights and Citizenship Directorate-General, and the new Home Affairs Directorate-General, should allow the latter some space to focus on these issues. They should be in a position to develop a more coherent and less fragmented legal framework, using the more efficient legal tools now available in this policy area, namely regulations and directives. While the

[225] Council Decision 2008/615/JHA, n82 above.
[226] J. Ratcliffe, n215 above, p.122.
[227] Council Decision 2000/641/JHA, n192 above.

discourse in the more commercially focused debate on data protection may well be issues of privacy, the more fundamental issues of effective, and better targeted, law enforcement and the protection of individual rights in the course of law enforcement activity are key to the debate in this area.

***

References

Treaties

Treaty of Rome 1957, as amended.
Council of Europe Convention of the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981.
Schengen Convention 1990.
Treaty of European Union, 1992, as amended.
Europol Convention 1995.
Convention on the Use of Information Technology for Customs Purposes, OJ C 316, 27.11.1995.
Treaty on European Union 2009.
Treaty on the Function of the European Union 2009.
Protocol (No. 8) Relating to Article 6(2) of the Treaty on European Union on the accession of the Union to the European Convention on the Protection of Human Rights and Fundamental Freedoms, attached to both the TEU and the TFEU
Protocol (No. 21) on the position of the United Kingdom and Ireland in respect of the Area of Freedom, Security and Justice, attached to both the TEU and the TFEU.
Protocol (No 22) on the Position of Denmark, attached to both the TEU and the TFEU.
Protocol (No. 30) on the application of the charter of fundamental rights of the European Union to Poland and to the United Kingdom, attached to both the TEU and the TFEU.

EU Legislation

Regulations

Regulation (EC) No. 168/2007 of 15 February 2007, OJ L 53/2 22.2.2007.
Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 381, 28/12/2006 p. 4.
Council Regulation (EC) No 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, OJ L 349, 25/11/2004 p. 1.
Regulation (EC) No. 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council, and Commission documents, OJ L 101, 11.4.2001, p.1.
Regulation (EC) No. 45/2001 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8/1.

Directives

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, OL L 281/31.

Council Framework Decisions

Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States, OJ L 93, 07/04/2009 p. 23.
Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350/60.
Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386, 29/12/2006 p. 89.

Council Decisions

Council Decision 2009/968/JHA of 30 November 2009, adopting the rules on the confidentiality of Europol information, OJ L 332/17.
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 L 138/14.
Europol Council Decision 2009/371/JHAof 6 April 2009 establishing the Europol Police Office (Europol), OJ L 121/6.
Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA, OJ L 93/33.
Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/616/JHA on the stepping up of cross-border cooperation particularly in combating terrorism and cross-border crime, OJ L 210/12.
Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ.L 210/1.
Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) OJ L 205/63.
Council Decision 2006/628/EC of 24 July 2006 fixing the date of application of Article 1(4) and (5) of Regulation (EC) No 871/2004 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism, OJ L 256/15.
Council Decision 2005/876/JHA of 21 November 2005 on the exchange of information extracted from the criminal record, OJ L 322/33.
Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences, OJ L 253/22.
Council Decision 2005/211/JHA of 24 February 2005 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism, OJ L 68/44.
Council Decision 2004/194/EC of 10 February 2004 amending Decision 2001/264/EC adopting the Council's security regulations, OJ L 63/48.
Council Decision 2003/659/JHA of 18 June 2003 amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime, OJ L 245/44.
Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, OJ L 63/1.

Council Decision 2001/264/EC of 19 March 2001 adopting the Council's security regulations, OJ L 101/1.
Council Decision 2000/641/JHA of 7 October 2000 establishing a secretariat for the joint supervisory data-protection bodies set up by the Convention on the Establishment of a European Police Office (Europol Convention), the Convention on the Use of Information Technology for Customs Purposes and the Convention implementing the Schengen Agreement on the gradual abolition of checks at the common borders (Schengen Convention) OJ L 271/1.

Council Acts

Council Act of 5 June 2003 amending the Council Act of 3 November 1998, adopting rules on the confidentiality of Europol information, (2003) OJ C 152/01.
Council Act of 3 November 1998 adopting rules on the confidentiality of Europol information OJ 1999 C26/10.

EU policy documents and proposals for legislation

Preliminary Comments of the European Data Protection Supervisor on: - Communication from the Commission to the European Parliament, the council, the European Economic and Social Committee and the Committee of the Regions, "Preparing the next steps in border management in the European Union", COM (2008) 69 final – Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Examining the creation of a European Border Surveillance System (EUROSUR)", COM (2008) 68 final; - Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Report on the evaluation and future development of the FRONTEX Agency", COM(2008) 67 final.
Proposal for a Regulation of the European Parliament and the Council amending Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX) {SEC(2010) 149} {SEC(2010) 150}, COM(2010) 61.

EU Case law

Joined Cases C-465/00, C-138/01 and C-139/01; *Neukomm* and *Rundfunk* [2003] ECR page I-04989.
Case C-275/06 *Productores de Música de España (Promusicae)* v. *Telefónica de España SAU* [2008] ECR I-271.

UK Case law

Durant v. *FSA*. 2003 EWCA Civ. 1746.

Secondary sources

Birnhack, M. 'The EU Data Protection Directive: An Engine of a Global Regime', 24 (2008) *Computer Law & Security Report*, 508-520.
Cartabia, A. 'Europe and Rights: Taking Dialogue Seriously', 5 (2009) *European Constitutional Law Review*, 5-31.

de Hert, P. and 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', 25 (2009) *Computer Law & Security Review*, 403-414.

Dine, J. 'Criminal Law and the Privilege Against Self-Incrimination', in S. Peers and A. Ward (eds), *The EU Charter of Fundamental Rights: Politics, Law and Policy.* Hart Publishing, Oxford and Portland, Oregon, 2004.

Ferretti, F. 'The "Credit Scoring Pandemic" and the European Vaccine: Making Sense of EU Data Protection Legislation', 1 (2009) *Journal of Information, Law & Technology*.

Foucault, M. *Discipline and Punish: The Birth of the Prison*. Penguin, 1977.

Grant, H. 'Data Protection 1998-2008', 25 (2009) *Computer Law & Security Review*, 44-50.

Hijmans, H. and Scirocco, A. 'Shortcomings in EU Data Protection in the Third and the Second Pillars: Can the Lisbon Treaty Be Expected to Help?', 46 (2009) *CMLRev.*,1485-1525.

Kierkegaard, S. 'The Prüm Decision:An Uncontrolled Fishing Expedition in "Big Brother" Europe', 24 (2008) *Computer Law & Security Report*, 243-252.

Kuner, C. 'An International Legal Framework for Data Protection: Issues and Prospects', 25 (2009) *Computer Law & Security Review*, 307-317.

Mitsilegas, V. 'The Third Wave of Third Pillar Law: Which Direction for EU Criminal Justice?', 34 (2009) *E.L.Rev.* 2009, 523-560.

Peers, S. 'Taking Rights Away? Limitations and Derogations', in S. Peers and A. Ward (eds), *The EU Charter of Fundamental Rights: Politics, Law and Policy.* Hart Publishing, Oxford and Portland, Oregon, 2004.

Ratcliffe, J. *Intelligence-Led Policing*. Willan, Cullompton, 2008.

Ward, A. 'Access to Justice', in S. Peers and A. Ward (eds), *The EU Charter of Fundamental Rights: Politics, Law and Policy*. Hart Publishing, Oxford and Portland, Oregon, 2004.

***