available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

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

Paul de Hert[a,b], *Vagelis Papakonstantinou*[c]

[a]*Vrije Universiteit Brussels (LSTS), Belgium*
[b]*Tilburg University (TILT), Netherlands*
[c]*University of Patras and Partner in PKpartners Law Firm, Athens, Greece*

Keywords:
Security data processing
Hague programme
Principle of availability
Data protection supervisory bodies
MDG

ABSTRACT

After more than three years in the making, that have witnessed much controversy, several working texts and at least two altogether different versions, the Data Protection Framework Decision "*on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters*" (hereafter, the DPFD) was finally adopted on 27 November 2008. The DPFD was supposed to be celebrated as the Data Protection Directive equivalent in European law enforcement (Third Pillar) processing. However, since its formal adoption, and even before that, data protection proponents (the European Data Protection Supervisor, the Article 29 Working Party, national Data Protection Commissioners, NGOs) lamented its adoption as the result of changes that ultimately compromised data protection. Is the DPFD a disappointment to the great expectations that accompanied its first draft, back in 2006? An attempt to address this question shall be undertaken in this paper.

1. Introduction

Data protection legislation was first introduced back in the 1960s, when the advent of computers threatened individual privacy at an, until then, unknown level. Although individual privacy was by then a right well founded and established in most countries (at least in continental Europe, but also in the USA),[1] computers that enabled automated massive processing of personal data changed the game altogether. At that point it was felt that the privacy of individuals had more to fear than their traditional right to privacy could protect. All the above led, during the 1970s and 1980s, to the release of national Data Protection Acts all around Europe.

This background information is relevant from several points of view to the purposes of this paper. The first point to be addressed is to identify the main sources of risk. In other words, who wants to use the personal data of individuals? Against whom ought individuals to be protected by data protection? Who threatens to unlawfully process their personal data, and for which purposes?

Arguably, the answer has differed over the years, following political, financial and social developments. When data protection was first conceived, back in the 1960s and the 1970s, the main source of risk was most of the times the State. Individuals had to be protected against public administrations that introduced computers in their bureaucratic processes, enabling them

[1] See the, by now mythological, paper of Warren and Brandeis on the Right to Privacy as late as 1864 («*The Right to Privacy*», Harvard Law Review, Vol. IV).

0267-3649/$ – see front matter © 2009 Paul De Hert and Vagelis Papakonstantinou. Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.clsr.2009.07.008

to undertake unprecedented surveillance of their citizens. Those were the times of May 1968 in Paris, of Watergate and of the Orwellian Big Brother and 1984. It was against this background that the first national Data Protection Acts should be placed.[2]

Subsequently, during the 1980s, it would appear that attention turned towards the private sector. The private sector saw commercial benefits in processing personal data. The drop on computer prices and the endless quest for even more effective marketing strategies made the extensive processing of personal data imperative. It was then that techniques such as profiling, data matching and data mining were first introduced.[3]

9–11 Changed that focus on the private sector. A single event turned forcedly attention from the private sector back to the State. After several terrorist attacks (in New York, London, Madrid and elsewhere) the State re-claimed the central role in the data processing scene, this time asking for increased processing opportunities in order to combat terrorism. After 2001, personal data processing by the State has been expressly aimed at serving 'security' purposes. This represents a qualitative change compared to the 1960s and 1970s, when instead of today's 'security', a word that somehow points at affirmative action (and not to be confused with 'safety', which is what individuals really need), the term 'surveillance' was used; a more benign expression. After 9–11, data protection, although encompassing such vast areas in the private sector such as banking or the Internet, arguably focused on state personal information processing once again.

All the above lead to the second point that needs to be noted here: the political element in data protection. The right to data protection is politically-charged. It inevitably follows the political agenda of its time. Back in the 1960s and 1970s, it constituted a newcomer in the human rights list against Orwellian Big Brother ideas and the 'panopticon' state. During the 1980s and 1990s data protection was used to defend individuals against the enthusiasm of business managers for information processing in order to "know their clients" and increase profits. In the early 2000s, when perhaps a new form of warfare emerged, and the State came in to process data in order to warrant security to its citizens,[4] data protection comes in to defend individuals against the "intrusive" State. The political agenda always has, and will continue, to give the tone to the right to data protection. Against this background, this paper discusses the Data Protection Framework Decision 2008/977/JHA of 27 November 2008 "*on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters*".[5] After a sketch of the EU institutional context on data protection (1.) and an account of the drafting process of the Framework Decision (2.), there follows a discussion of the main provisions of the text (3.) four critical observations (4.) and a conclusion (5.)

2. EU data protection background

EU institutions followed, if not helped shape, the above trends; however, their internal bureaucracy and power games, and of course the agendas of each EU Member State, have played their role as well.

The first point to be noted with regard to the EU data protection refers to the fundamental, internal (and perhaps temporary, if the Lisbon Treaty receives the green light), distinction between processing of personal information within the so-called First Pillar, and processing of personal data within the Third Pillar. Following the Pillar structure established by the Treaty of Maastricht,[6] processing of personal data under the First Pillar essentially includes all commercial processing, that is, processing normally performed by private parties in the course of their business. Processing of personal data under the Third Pillar refers to all processing performed by law enforcement State agencies (for instance, the police, customs agencies, judicial processing) executing their powers and tasks (crime prevention and investigation, State security, etc.).

The data protection regulatory framework up until the adoption of the DPFD was completely uneven between the two Pillars.

Commercial personal data processing (data protection in the First Pillar) benefits from a comprehensive legal framework. In 1995, the Data Protection Directive[7] was released, setting the regulatory basis for the EU system for individual privacy protection. Its scope, however, expressly excludes security-related processing,[8] although several EU Member States actually applied their national Data Protection Acts that implemented the Directive in order to restrict processing by state authorities.

The European Commission, after all, could not harmonize State processing through the Data Protection Directive back in 1995, even if it wanted to and this due to internal EU complexities: the Commission does not have the right to regulate State security, an activity that remains at the core of the sovereignty of Member States (together with defense or foreign policy). As long as the EU remains an economic union, such hardcore sectors do not fall under the regulatory powers of EU institutions. Admittedly, different Member States tend to approach the EU issue differently; some wish for it to expand and ultimately become a political union too, while others oppose to the very idea of further integration and wish for the EU to remain exactly as it is today, if not retreat a few steps. This reasoning, and the resulting Member States' agendas, has played a significant role in the DPFD law-making process; in particular it helps to explain the otherwise inexplicable limited scope of the Framework Decision (see below).

At any event, the Data Protection Directive has since become the basic standard-setting text for the processing of personal data for (in principle) commercial purposes. It essentially follows the basics of the first Data Protection Acts

[2] See Flaherty D, *Protecting Privacy in Surveillance Societies*, 1989, The University of North Carolina Press, Hondius F, Emerging Data Protection in Europe, 1975, Elsevier.

[3] See Papakonstantinou V, *A Data Protection Approach to Data Matching Operations Among Public Bodies*. International Journal of Law and Information Technology, Vol. 9 No. 1.

[4] See The Economist series on *Terrorism and Civil Liberty* back in 2007, in particular, *Civil liberties: Surveillance and Privacy*, 27.09. 2007.

[5] Council Framework Decision 2008/977/JHA, OJ L 350/60, 30.12. 2008.

[6] At the time of this paper the future of the Treaty of Lisbon, particularly after the result of the Irish referendum, remained unknown.

[7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31, 23.11.1995.

[8] See Art. 3 par. 2 of the Data Protection Directive.

introduced in Europe in the 1960s and 1970s. It is composed of a set of fundamental data protection principles and a set of individual rights, accompanied by the establishment of independent national supervisory authorities in each Member State to warrant their implementation. The Data Protection Directive was subsequently accompanied by sector-specific Directives that built upon its premises.[9] All Member-States harmonized their national legal systems with the above set of Directives, ensuring thus a uniform level of protection.

What was therefore in place by the time the DPFD was released within the EU with regard to commercial, First Pillar, processing was an impressive volume of *acquis communaitaire*: regulations, institutions, case law and research, notably through the European Commission,[10] the Article 29 Working Party,[11] several European Court of Justice (ECJ) judgments and, of course, the European Data Protection Supervisor (EDPS[12]). Substantial work at national level was also already in place in most Member States, through the national Data Protection Authorities or Commissioners, legal theory and case law.

Security-related, Third Pillar, processing of personal data largely lagged behind. Contrary to what was happening in the First Pillar, where the Data Protection Directive was dominating the field, no standard-setting text existed, or was even initiated, until the release of the DPFD for Third Pillar, security-related, processing. The standard-setting role was supposedly assumed by the European Council's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (which opened for signature back in 1981), as amended by a Protocol[13] and complemented by a couple of Recommendations,[14] but the Convention, by the year 2008, was admittedly too broad and partly outdated.[14a]

Despite the fact that security-related processing within Europe lacked a common regulatory basis until 2008, specific sectors did go ahead alone: most notably in the context of the Schengen Agreement,[15] but also Europol[16] and Eurojust[17] Agreements, or even the Prum Decision[18] that came in a bit later. They all included detailed data protection procedures and established institutions in their respective texts. What had happened, actually, was that whenever there had been a need for security data protection legislation, this was resolved on an *ad hoc* basis, using admittedly as basic principles and procedures those introduced in the Data Protection Directive.[19] In this way however the normal law-making flow was reversed: rather than first releasing the standard-setting text and then the sector-specific texts (very much in the way it happened in the First Pillar), in the Third Pillar sector-specific texts preceded the standard-setting one. This paradox played its role in the law-making process of the DPFD, and is elaborated later in detail.[20]

Sector-specific legislation within the Third Pillar sometimes also came from unexpected sources. This is the case, for instance, with so-called PNR processing. Passenger Name Records (PNR) are the data that airlines use for the booking of flights. After 9–11 they gained in importance, first in the USA, as they became essential in their data processing strategy against terrorism. European airlines were threatened to be denied landing in US territory if they did not surrender their PNR data to American security authorities. The European Commission intervened and entered a first PNR Agreement with the USA, thinking that the whole PNR scene fell under its First Pillar regulating power (because commercial airlines did). The case was brought to the ECJ by the European Parliament (because of political reasons rather unrelated with the PNR

[9] For instance, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, or Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.

[10] By now, DG Justice, which succeeded to DG Internal Market, a switch of authorities of significant semantic value, see relevant Statewatch coverage available at http://www.statewatch.org/news/2005/jul/06eu-data-prot.htm.

[11] Officially named the Working Party on the Protection of Individuals with regard to the processing of Personal Data, established by Article 29 of the Data Protection Directive. See the relevant webpages under the European Commission's Data Protection website (DG Freedom, Security and Justice), available at http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm.

[12] See http://edps.europa.eu/.

[13] Additional protocol to Convention 108 regarding supervisory authorities and transborder data flows (ETS No. 181).

[14] Work within the Council of Europe on Convention 108, as it has been code-named, may be followed at http://www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/.

[14a] See De Hert P/Bellanova R, Data Protection In The Area Of Freedom, Security And Justice: A System Still To Be Fully Developed?, Study requested by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE)., Brussels, European Parliament, 2009, http://www.europarl.europa.eu/activities/committees/studies/download.do?language=en&file=25213, p. 5.

[15] Actually referring to Schengen I (Agreement between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, entered in 1985) and Schengen II or CIS (Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, entered in 1990). By noting which Member States participate in these security-related "unionist" attempts and which do not, one gains an accurate picture as to how the "scope" of the DPFD negotiations process played.

[16] See The EUROPOL Convention (consolidated text) at http://www.europol.europa.eu/index.asp?page=legal.

[17] See Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (2002/187/JHA), OJ L 63/1.

[18] Council Decision of 27 February 2007, on the stepping up of cross-border cooperation, particularly in combating terrorism, and cross-border crime (available at: http://register.consilium.europa.eu/pdf/en/07/st06/st06566.en07.pdf).

[19] Except in the case of the Convention implementing the Schengen Agreement, which actually predated the Data Protection Directive.

[20] De Hert P. & De Schutter, B., 'International Transfers of Data in the Field of JHA: The Lessons of Europol, PNR and Swift', in Bernd Martenczuk & Servaas van Thiel (eds.), Justice, Liberty, Security: New Challenges for EU External Relations, VUBPress, Brussels, (I.E.S. series nr. 11), 2008, (295 p.), pp. 303–340.

Agreement itself); the ECJ ruled that PNR Agreement fell in fact under the Third Pillar (because security agencies ultimately are involved). The First PNR Agreement thus had to be annulled. Subsequently another[21] PNR Agreement was entered with the USA through security representation by the EU (the Council), but the fact remains that EU entered into hard negotiations with the Americans on sector-specific security-related personal data processing without any standard-setting text which could be used as a reference (in fact, at the time the PNR Agreement was being elaborated, the DPFD was in the making).

Until late 2008 therefore, what was in place within the EU Third Pillar was a series of sector-specific provisions accompanied by an International Convention that only broadly regulated the field. The DPFD aims (-ed) at amending these shortcomings. Although it came late (only in 2008, while its First Pillar equivalent, the Data Protection Directive, had been released in 1995), its ambition is (was), supposedly, to attract the same attention and play the same central role in data protection matters as the Directive has been playing in its own field over the years.

3. The DPFD drafting

3.1. General

Work on the DPFD, at least in the form in which it was released in 2008, officially began back in 2005. A series of reasons led to such work being initiated at that time.

Firstly, there were a series of practical explanations: the 1981 Convention regulated processing done by law enforcement authorities without taking into account the specific characteristics of contemporary exchanges of data by police and judicial authorities. International data exchanges were increasing, partly due to further integration and facilitated by legal instruments such as the Schengen Agreement. At the same time, methods of data gathering and data exchange were multiplying, some of them facilitated by (First Pillar) initiatives such as the Data Retention Directive.[22] Finally, the sector-specific regulations had finally reached their limits, and it was felt that adequate data protection supervision required more integration of the already existing supervisory bodies for Europol, Eurojust and the Schengen Information System.

The above factual grounds were well-noted back in 2005, but it remained nevertheless questionable whether legislative action was generally felt as a priority, particularly as earlier attempts to draft a DPFD had been unsuccessful.[23]

In fact, the real driving force behind the initiative was very much related with the political agenda at that time. The Council had promised to the European Parliament to adopt such a Framework Decision during the voting on the 2006 Data Retention Directive, in order to pacify the latter's protests. Additionally, the European Commission had felt its need when it introduced the Proposal for a Council Framework Decision on the exchange of information under the principle of availability of October 2005, a document with far-reaching data protection implications.[24] Motivated expressly by the bombings in London in 2005 and within a short (six-month) notice by the Council, the European Commission presented its first Proposal for a DPFD in October 2005.[25]

3.2. A closer look at the 2005 Proposal for a Council Framework Decision

The 2005 proposal was drafted by the Commission along the lines of the Data Protection Directive.[26] In the 2005 DPFD draft, 'data subjects' (individuals) were afforded more or less the same rights as in the Directive (subject access, information, rectification); the data processing principles were similar to those of the Directive (even including the purpose specification principle); and there existed provisions dealing with the control of personal data exports to third countries. Control was exercised by a Supervisory Authority that could be the same as the already existing national Data Protection Commissions so as to spare expenses, to be assisted by a Register. A Working Party was also established (resembling

[21] The Second (2007) PNR Agreement (Council Decision 2007/551/CFSP/JHA of 23 July 2007 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement)), which was actually a third PNR EU–US Agreement, as a Second, interim, Agreement, was also adopted in the meantime (see Papakonstantinou V. & De Hert P, *The PNR Agreement and Transatlantic Antiterrorism Cooperation: No Firm Human Rights Framework on either side of the Atlantic*, Common Market Law Review, Vol. 46 issue 3, pp. 885–919).

[22] Directive 2006/24/EC (see above).

[23] The Council of the European Union (then, 15 Member States) had set up an internal working party on data protection in the "third pillar" in May 1998. The "Action Plan of the Council and the Commission on how best to implement the provisions of Amsterdam establishing an area of freedom, security and justice" (13844/98) said that data protection issues in the "third pillar" should be: "developed within a two year period" (IV.47(a)). Not until August 2000 was a draft Resolution drawn up by the Working Party, this was revised five times, the last being on 12 April 2001 under the Swedish Presidency of the EU (6316/2/01) when agreement appeared to have been reached and the Article 36 Committee was asked to address outstanding reservations. From that point on there had been silence – and the Working Party was abolished in 2001 when the Council was restructured to "streamline" decision-making.

[24] See Proposal for a Council Framework Decision of 12 October 2005 on the exchange of information under the principle of availability, http://europa.eu/scadplus/leg/en/lvb/l33257.htm The principle of availability was defined in the Hague Programme.

[25] Commission, *Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters*, (COM(2005) 475 final), 4 October 2005 (still available at the Commission's data protection website, under "Commission proposals", http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm#proposals).

[26] See the 2005 Proposal, p.4. The Commission, regardless of the fact that a different Directorate General had drafted Directive 95/46, felt that the Framework Decision "*should not hamper consistency with the general policy of the Union in the area of privacy and data protection on the basis of the EU Charter for Fundamental Rights and of Directive 95/46/EC. The fundamental principles of data protection apply to data processing in the first and in the third pillar*".

the Article 29 Working Party of the Directive). Perhaps more importantly, the original proposal wanted to regulate security personal data processing both at a national and at an EU, inter-Member States level. We will see that this idea was abandoned in the DPFD it its final version.

Not everything was unproblematic with the 2005 DPFD draft. Its legal basis was obscure; although it aimed at being enforceable at a national level as well, it was not clear whether the domestic processing of Member States could indeed be governed by it. As seen in the preceding paragraph, the proposed draft intended to apply both to internal or domestic processing of data and to cross border exchange of data. However, several Member States objected to this uniform application, suggesting that the provisions should only be implemented for inter-Member States data transfers.[27]

The 2005 DPFD draft also attempted to strike an admittedly difficult to find balance with the instruments already in effect (Schengen, Europol, Eurojust, Customs Information System)[28] and their provisions. Additionally, it attempted to strike an equally difficult balance between its scope of application (criminal matters) and the matters that would be excluded altogether from application of its provisions (i.e. State security). It is exactly these difficulties that attracted the Member States' criticism while the 2005 draft of the DPFD was being processed; naturally, these objections were expressed, if not formulated by the MDG.

3.3. *The drafting process after 2005 led by the Multidisciplinary Group on Organised Crime*

After the 2005 proposal was submitted, the EDPS issued an Opinion (in December 2005), and the European Parliament agreed on 60 amendments in its report in May 2006 and adopted it in September 2006.[29]

However, precisely during this time, between November 2005 and November 2006, the Council's Multidisciplinary *Group on Organised Crime* took over the drafting activities from the Commission and produced 29 working documents substantially changing the Commission proposal, although not reaching any agreement on the text after all. During that time amended texts were put to the table for discussion, almost on a monthly basis.[30]

The *Multidisciplinary Group on Organised Crime* (the MDG), a group comprising police officers and Ministry of Justice officials that, by definition, showed very little interest in data protection,[31] refused all involvement of any data protection experts (either of the Article 29 Working Party or of the EDPS) in the process of redrafting.

The work of the Commission and the interventions of the MDG met with little enthusiasm. The EDPS and the European Parliament both felt that their views were being ignored,[32] and later focused part of their critique on their lack of voice during the drafting procedure. A comparative analysis between the original Commission proposal and the status of the Framework Decision as of November 2006 demonstrates that the MDG was able to significantly worsen the protection of individuals to the benefit of law enforcement interests. The November 2006 Draft Framework Decision resembled only in form to the initial proposal; in fact, each and every fundamental data protection principle had been tied to exceptions that made their application in practice uncontrollable.[33]

[27] Information from a Communication of the Council to the Article 36 Committee (Coreper) on "*Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters – Questions on scope*", 13918/13.10.2006. Available at: http://www.statewatch.org/eu-dp.htm. Also, '*Data protection proposal in a muddle – member states divided – three Council working parties discussing the draft measure*', Statewatch, 2006 (available at: http://www.statewatch.org/news/2006/nov/02eu-dp-muddle.htm).

[28] The Commission proposal did not attempt to abolish the provisions of those legislative instruments that were affected by it (Schengen, Europol, Eurojust, Customs Information System), but contained general provisions for similar processing; at the same time, said instruments would continue to apply as sector-specific legislation, governing their particular subject matter. Although the 2005 DPFD draft did not take into consideration conflicts of law, the understanding of the drafters was that should the proposed Framework Decision be adopted, those provisions of said instruments that directly contradicted the provisions of the proposed Framework Decision should become null and void (not necessarily by means of direct mention in the text of the DPFD, but rather by adequate application of the *lex specialis* criterion upon them).

[29] See the documents referred to in http://www.statewatch.org/eu-dp.htm.

[30] Council of the European Union, Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, 13246/13.11.2006 (available at http://www.statewatch.org/eu-dp.htm).

[31] One commentator has observed that their "*primary interest is to make life difficult for criminals, not to have regard to the interests of data subjects*". See Lord Avebury, Speech to the Joint Parliamentary Meeting on EU developments in the area of freedom, security and justice at the European Parliament on October 3 (available at: http://www.statewatch.org/eu-dp.htm). Suggestions by Member States for the establishment of an *ad hoc* group for the processing of the Framework Decision, where data protection authorities (either national or the EDPS) would also participate, were rejected ('*Monitoring the state and civil liberties in the UK and Europe, EU policy "putsch": Data protection handed to the DG for "law, order and security*', *Statewatch*, March–April 2005, vol. 15 no 2). The only institutional data protection participation in the law-making process included one single presentation by the EDPS of his office's respective opinion in the MDG.

[32] In November 2006 the EDPS issued a second critical Opinion and in December 2006 the European Parliament adopted a report saying that it intended to re-examine the issue as the Council had ignored its views. See European Data Protection Supervisor Second Opinion and respective Press Release of 29.11.2006 ("*EDPS warns Council not to lower EU citizen's rights in third pillar data protection*"), as well as the European Parliament's Recommendation to the Council on the progress of the negotiations on the framework decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (2006/2286(INI)). See also Bunyan T, *EU data protection in police and judicial cooperation matters: Rights of suspects and defendants under attack by law enforcement demands*, Statewatch, 2006, p.2 (available at: http://www.statewatch.org/news/2006/oct/eu-dp.pdf).

[33] See De Hert P/Papakonstantinou V/Riehle C, *Data Protection in the Third Pillar: cautious pessimism*, in *Crime, Rights and the EU*, (ed. Martin M), JUSTICE, 2008.

A further point of substantial importance refers to the fact that, while the DPFD was being drafted, data protection changed Directorates within the EC bureaucracy – from DG Internal Market it moved to DG Justice and Home Affairs.[34] This change gravely affected the 'quality' of the Commission's proposals and approach during the subsequent negotiations rounds.

Finally, one must not forget that Third Pillar law-making requires unanimous and not majority decisions. A compromise had to be reached any time any Member State's agenda, political, legal or other, objected to a provision of the DPFD under discussion.

Towards the end of 2006, after the Finnish Presidency concluded its work on the DPFD and handed over to the German Presidency, both the EDPS and the European Parliament chose to intervene to alert the Council as to the clear compromise of individual rights created by the wording of the text, at least as it was being discussed at that time.[35] The EDPS expressly declared himself "*worried about indications that current negotiations in Council are leading to a fragmented and lowered level of protection for the citizens*" and thus "*strongly urge*[d] *the delegations to reconsider. The EDPS is concerned that legislation aiming at facilitating police and judicial cooperation might be adopted while the legal data protection framework is delayed and diluted*".[36] The Committee on Civil Liberties, Justice and Home Affairs of the European Parliament expressly felt "*extremely concerned at the direction being taken by the debate in the Council, with Member States appearing to be moving towards a data protection agreement based on the lowest common denominator; fearing, moreover, that the level of data protection will be lower than that provided by Directive 95/46/EC and Council of Europe Convention No. 108 and that implementation of such an agreement might have a negative impact on the general principle of data protection in each Member State without establishing a satisfactory level of protection at European level*".[37] It therefore called for maximum participation during the law-making process, with representations from national data protection authorities, the Article 29 Working Party and the European Parliament itself, as well as national parliaments.

Lack of consensus within the group explained why, in January 2007, the German Presidency, admitting that the Council was in a mess, asked the European Commission to go back to the drawing board and prepare a 'revised' proposal.[38] Although some commentators interpreted this measure as a promising step for data protection,[39] it is not clear that it was motivated by genuine data protection concerns after all. The German Presidency arguably intended to change the DPFD draft drastically in two ways. First, it was of the opinion that a compromise could be reached in order to resolve the dead-end that until that time was reached with regard to the DPFD's scope (a dead-end that threatened the release of the DPFD itself). Secondly, it wanted to merge the existing Third Pillar Joint Supervising Authorities already in place (Schengen, Europol, Eurojust).

It took two more years and a lot of compromise in-between, for that second proposal to finally become the DPFD.

4. The DPFD of 27 November 2008

The Data Protection Framework Decision "*on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters*"[40] was finally adopted in November 2008. Work by the MDG was concluded almost a year earlier, but the draft, due also to some linguistic processing, had to wait patiently for its formal adoption for quite some time; the delay being mostly attributed to the political agenda of 2008.

4.1. *General considerations*

The DPFD admittedly had to face a series of difficulties and to tackle difficult legal issues in a heated political environment.

First, an important difficulty referred to the particularities of its subject matter. The Data Protection Directive is mainly concerned with the processing of data by the private sector; hence it could afford to be strict on such issues as the purpose specification principle. Police information is something completely different. The police have a broader task, ranging from criminal investigation, crowd control or political policing, a series of functions often exercised without transparency, making control and data protection more vital. Moreover, police data is sometimes based on uncertain facts or on assumptions and hearsay ('soft data'). All these particular needs of the police are hard to match with the basic data protection principles, at least as included in the Data Protection Directive.

Second, the point of view has also changed. When the Data Protection Directive was being negotiated, in the early nineties, the private sector was, arguably, the data protection main "risk source"; in other words, what needed to be

[34] See "*Monitoring the state and civil liberties in the UK and Europe, EU policy "putsch": Data protection handed to the DG for "law, order and security"*, Statewatch, March–April 2005, vol. 15 no 2.

[35] In order to properly set the time scene, it should be noted that the Finnish Presidency, just one month before these EDPS' and Parliament's interventions on the Framework Decision, had also concluded the interim PNR Agreement (see above, Papakonstantinou V/De Hert P, *The PNR Agreement*), that also raised heated disputes with regard to its level of data protection (which disputes the Parliament expressly adopted, see for instance the respective debate at the Parliament's site, http://europarl.europa.eu, Ref. 20060901IPR10254).

[36] See EDPS' Press Release of November 29, 2006 (available at: http://www.edps.eu.int).

[37] European Parliament, Session Document, A6-0456/2006 FINAL, December 11, 2006.

[38] See page 4, point 7 in Presidency Note for discussion at the Article 36 Committee on 25–26 January: EU doc no: 5435/07.

[39] "*It has to be hoped that the Commission when revising the proposal takes into account the views of the European Data Protection Supervisor and the European Parliament and not just those of the Council. When it does return to the table the Council must give it to the Working Party on Data Protection and not to the working party comprised of law enforcement officials who have proved quite incapable of balancing their demands with the rights of citizens to meaningful data protection*" (Bunyan T, *EU: Data protection: German Presidency to ask for "revised" proposal*, Statewatch News Online, 26 January 2007 (03/07), sub 2 (http://www.statewatch.org).

[40] Council Framework Decision 2008/977/JHA, OJ L 350/60, 30.12.2008.

restricted was processing for profit. At the opposite side stood individuals, and their right to informational self-determination. Sides were clear and compromises were made in order both to protect individuals and not to suffocate the market. On the other hand, when the DPFD was being processed, interested parties and their motivations were more difficult to distinguish. On the one side stood security agencies around Europe, who asked for increasing processing powers. The other pole, however, was less clearly identified. Individuals, as represented by their national governments, were neither uniform nor adamant about their motivations. Security matters; it weighs much heavier upon the public conscience than business profit. After the terrorist attacks in several EU capitals, individuals were allegedly more willing to sacrifice some of their rights (for instance, the right to data protection) for an increased level of State security. Adamant voices in favour of data protection mostly came from the data protection community (national Data Protection Commissioners, the EDPS, NGOs), but they lacked wide public support. Hence, all compromises were practically made from that part of the negotiations.

Third, legal technicalities posed substantial difficulties. For instance, several Member States have specialised criminal investigation police bodies, while others do not; in some Member States only the police can enforce penalties, while in most this is done by the prosecutor. The lack of harmonisation at European level of the criminal process is general, beginning with the identification and investigation of a crime until its discussion in court.

In the same context, practically all Member States had, by the time the negotiations for the adoption of the DPFD were initiated, set up their own 'politics' within the crime prosecution sector, entering two-side agreements for the exchange of information (police cooperation) with third countries. As will be later demonstrated, for many Member States these already established bilateral agreements seemed too valuable to be abandoned.

4.2. *Basic provisions*

The structure of the DPFD broadly follows what has by now become the data protection standard (particularly after the Data Protection Directive): a set of definitions is followed by a basic set of processing principles, sensitive data are dealt with, rights are conferred to individuals, and a supervisory authority is established. However, two fundamental policy decisions that shape the whole DPFD have led to a less easy-to-follow text (for instance, no chapter division may be found in the DPFD): limitations in its scope and its undoubted pro-security perspective. Both factors will be discussed later in detail.

Here it is enough to note that the DPFD expressly aims at ensuring "*a high level of protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data in the framework of police and judicial cooperation in criminal matters, provided for by Title VI of the Treaty on European Union, while guaranteeing a high level of public safety*" (Art. 1.1).

The scope of the DPFD shall be elaborated in detail later in this paper. Here only its limitations will be briefly noted: the DPFD is not intended to cover national, intra-Member State data processing. On the contrary, the DPFD applies only on sets of personal data that "*are or have been transmitted or made available between Member States*" (Art. 1.2(a)). In other words, only inter-Member States transfers are regulated by the DPFD. Member States are free to do as they please in their interior; some may even choose to provide "*for the protection of personal data collected or processed at national level, higher safeguards than those established in this Framework Decision*" (Art. 1.5). At any event, however, "*this Framework Decision is without prejudice to essential national security interests and specific intelligence activities in the field of national security*" (Art. 1.4).

The basic data protection principles, established since the 1960s in European data protection, are to be found in the DPFD too, albeit burdened by a series of exemptions. At any event, in principle at least, "*personal data may be collected by the competent authorities only for specified, explicit and legitimate purposes in the framework of their tasks and may be processed only for the same purpose for which data were collected. Processing of the data shall be lawful and adequate, relevant and not excessive in relation to the purposes for which they are collected*" (Art. 3.1). In addition, "*personal data shall be rectified if inaccurate and, where this is possible and necessary, completed or updated*" (Art. 4.1). Readers of the DPFD, however, should pay special attention to a series of exemptions, most notably those benefiting "*further processing*" i.e. non-deletion of personal data that is allegedly essential to police processing.

The processing of sensitive data only occupies six lines in the text of the DPFD (Art. 6). The scope limitation (the DPFD applies only to sets of data that are transmitted among Member States) has made necessary the introduction of a series of Articles on such "international" cooperation, regulating issues, for instance, of "logging and documentation", verification of quality, compliance with national processing restrictions, or even transmission to private parties (Art. 9–15).

The rights of individuals are covered in Art. 16 ("*information for the data subject*"), Art. 17 ("*right of access*") and Art. 18 ("*right to rectification, erasure or blocking*"), plus a welcome addition of a "*right to compensation*" (Art. 19).

The independent supervising authority entrusted with monitoring compliance with the DPFD in favour of individuals is established in Art. 25: "*Each Member State shall provide that one or more public authorities are responsible for advising and monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Framework Decision. These authorities shall act with complete independence in exercising the functions entrusted to them*" (par. 1). An important tool to their, otherwise limited, powers may prove to be the right to "*prior consultation*" (Art. 23). Luckily for Member States' strained national budgets, nothing in the DPFD precludes the possibility that this "supervisory authority" may be the same as the national Data Protection Commissions or Commissioners already established and operating since the time of the Data Protection Directive (Preamble, par. 34).

The DPFD does not go as far as establishing an "Article 29 Working Party", as the Directive did. Neither, as will be seen later, is any form of central guidance or control introduced ("comitology"); not even in order to assist national supervisory authorities. The same applies to the German Presidency's

aim to consolidate all separate data protection supervising bodies already operating under the different instruments in effect in the EU (Schengen, Eurojust, Europol); an objective that was evidently abandoned.

5. A few points to be noted (from a data protection perspective)

This paper is not intended to provide an exhaustive analysis of the DPFD provisions; not even a comprehensive analysis of all data protection concerns expressed by data protection proponents. Rather than that, four points will be highlighted, not just because they lie at the center of the debate but also because the policy options behind them establish the tone for the whole DPFD.

5.1. *Scope*

The DPFD applies only to ''*personal data that are or have been transmitted or made available between Member States*'' (Art. 1.2(a)). This is a fundamental limitation, because it evidently leaves out all domestic, intra-EU Member State national processing. In other words, law enforcement agencies in Member States shall abide by the DPFD principles only for these sets of personal data that they transmit to another Member State or that have been transmitted to them by another Member State; as far as processing data under their own jurisdictions is concerned, they are free to do as they please.

This policy choice has resolved a debate that plagued negotiations for the DPFD ever since its 2005 draft. Member States, as represented in the MDG, were split into two parties, those who asked for the DPFD to have national effect as well and those, eight altogether, who refused any such thought (the United Kingdom, Switzerland, the Czech Republic, Denmark, Ireland, Iceland, Malta and Sweden).[41] Presumably the debate had nothing to do with the DPFD itself, but could probably be related to national agendas. Application of the DPFD at domestic level would mean indirect recognition that Third Pillar (security) regulations carry direct effect into national law, a step that several Member States are not willing to take (see, after all, the process for ratifying the Lisbon Treaty, but also Member State participation in the Schengen Agreement[42]).

While negotiating the DPFD the legality of its potential domestic application was put to the test; a legal opinion by the Legal Service was asked on this matter. The Legal Service replied positively, but this was not enough to reverse Member State objections.

One must also keep in mind that in Third Pillar (security) decision-making a consensus is necessary. Member States that objected to the extended scope of the DPFD, although perhaps a minority, could not be simply disregarded by the majority that wished for the contrary. Their objections had to be accommodated, and a compromise had to be reached in some form. It was this situation that the German Presidency faced; after more than a year of intense negotiations within the MDG a consensus on such a central matter as the scope of the DPFD appeared no way near. The second and final draft resolved the issue in the way depicted in the DPFD's ultimate wording. Thus, the battle between those who wished for more European integration and those who wished for less ended, arguably, with a defeat for the first. The actual loser, however, was data protection.

The distinction in each Member State between two sets of personal data when police processing is concerned is problematic both from a practical and from a theoretical perspective. From a theoretical point of view, it appears that the police and the justice systems of each Member State should maintain two databases. One would be for strictly internal uses, where personal data from their respective jurisdiction will be stored and processed according to national law that can differ from the DPFD. The other database shall include personal data received by another Member State, by virtue of the DPFD. To this set of data the DPFD rules shall apply. The two databases may never be mixed.

In practice, the DPFD could allow for the following situation: police within a Member State applying a national law, less pro-data protection than the DPFD, collects data within its jurisdiction and then transmits them to another Member State. The DPFD applies to these data as far as the recipient is concerned, but this is by now irrelevant, because the DPFD provisions have already been 'breached', hence the recipient already has increased processing powers than the DPFD generally allows for.

Harmonisation is hardly also an issue, as per the DPFD's ultimate wording. The cause of harmonisation of national laws, apart from an aim of EC institutions in general,[43] was a declared aim ever since the first DPFD drafts. The multitude of national laws, increasing after 9/11 and attacks in European capitals as well as regulatory initiatives such as the Data Retention Directive or the ever-present 'principle of availability', made the need for harmonisation imminent. The 'two-set' of personal data solution, however, hardly relates to this objective. Each Member State is left free to continue applying its national laws within its jurisdiction; the DPFD has no power over them. Additionally, those Member States who 'lost' in the above debate secured an exemption in Art. 1.5, allowing them to apply more strict rules to national law ('higher safeguards') compared to those of the DPFD. Europe therefore divides into three after the DPFD release: those Member States applying nationally less strict rules than the DPFD, those choosing to follow the DPFD provisions, inserting them ''as is'' into their national law, and those choosing to go over that level. All these compromises, easy to trace back but hard to understand, amount to a hardly successful outcome, regardless of the point of view adopted.

[41] See *Data protection proposal in a muddle – member states divided – three Council working parties discussing the draft measure*, Statewatch, 2006 (available at: http://www.statewatch.org/news/2006/nov/02eu-dp-muddle.htm).

[42] See also Preamble (7) of the DPFD, whereby ''*No conclusions should be inferred from this limitation regarding the competence of the Union to adopt acts relating to the collection and processing of personal data at national level or the expediency for the Union to do so in the future*''.

[43] When lack of harmonisation can have a detrimental effect on the Internal Market.

5.2. *Security versus privacy and its consequence for the data protection principles*

The DPFD, as already noted, had to reconcile the right to data protection with the increased need (after 9/11) for State security. Given the political agenda at the time of its drafting it undoubtedly leans towards State security. This reflected not only the balance within the institutions responsible for its drafting (Council, DG Justice, MDG, no data protection formal representation whatsoever, no Parliament participation at all), but also the state of mind of Europeans. At a time when European capitals were being bombed or threatened and European soldiers were fighting in Iraq and Afghanistan civil liberties unavoidably retreated in public opinion agendas.

In addition to the political conditions, one must not overlook the fundamental difference between the subject matters of the DPFD and the Data Protection Directive that unavoidably, by now, constitutes the European data protection standard against which the DPFD is judged. As already noted, the Data Protection Directive is intended to regulate commercial processing, whereby personal data are used for profit. The DPFD on the other hand (even more if it had national scope) is intended to regulate the use of personal data by the police. The two situations differ gravely. While businesses may be expected to use their clients' or potential clients' data in certain limiting ways, while seeking to maximize profit, the police work differently. They keep track of criminals for most of their lives, correlate data from different sources, work on suspicion and hearsay, and store current data for no obvious reason other than it may prove extremely useful in the future.

As a result of the above, data protection principles were compromised in the final text of the DPFD. Almost each and every one of them comes with an exemption that opens the door to the police to do otherwise than the principle prescribes, if they see fit.

Before illustrating this through a couple of examples, a clarification is needed as to what exactly constitute those ''data protection principles''. As everybody knows by now, the ''data protection principles'' are a set of principles that regulate the collection and processing of personal data. They include the 'fair and lawful' collection and use of data principle; the data quality (subset of) principle(s); the principle of proportional (to their cause) collection and processing of personal data; the principle of data security, as well as, notoriously, the purpose specification principle. The 'data protection principles' come from way back – their first draft may be found in the first Data Protection Acts ever to see the light of day. Subsequently, they were included in all national European Data Protection Acts, in the Council of Europe Convention of 1981, and eventually in the text of the Data Protection Directive, constituting by now one of the four data protection pillars (the other three being the rights of data subjects, the establishment of independent supervisory authorities and the notification/registration system respectively). It should also be noted that, although the Directive is mainly concerned with commercial processing, several Member States in their national Data Protection Acts used the same principles to regulate State processing as well (notwithstanding of course the Convention itself).

What has become by now known as the 'basic data protection principles' has been greatly compromised in the text of the DPFD. This has been done either by exempting clauses or by use of the broad notion of '*further processing*'. As far as the latter is concerned, Art. 3.2 amends in practice the purpose specification principle as declared in Art. 3.1: ''*further processing for another purpose shall be permitted in so far as:*''*(a) it is not incompatible with the purposes for which the data were collected; (b) the competent authorities are authorised to process such data for such other purpose in accordance with the applicable legal provisions; and (c) processing is necessary and proportionate to that other purpose. The competent authorities may also further process the transmitted personal data for historical, statistical or scientific purposes, provided that Member States provide appropriate safeguards, such as making the data anonymous*''.

Given that the whole DPFD is about police and judicial processing, the purpose specification principle may in practice always be by-passed, because personal data shall always be collected for police processing purposes and processing under the DPFD shall thus never be '*incompatible with the purposes for which the data were collected*'.

Other data protection principles have more subtle exemptions. For instance, as per Art. 4.1 of the DPFD. ''*Personal data shall be rectified if inaccurate and, where this is possible and necessary, completed or updated*'', introducing thus the possibility for the police formally to keep inaccurate records on its suspects. Or, as per Art. 4.2 of the DPFD, ''*personal data shall be erased or made anonymous when they are no longer required for the purposes for which they were lawfully collected or are lawfully further processed. Archiving of those data in a separate data set for an appropriate period in accordance with national law shall not be affected by this provision*''; in practice, personal data shall thus never be deleted, they will simply change databases.

The above exempting methodology has been meticulously applied on each and every one of the basic data protection principles, most of the times thus emptying them of their content for the protection of individuals.

5.3. *Limitations to the principle of availability within and outside the EU*

One of the motivations explicitly acknowledged for releasing the DPFD is warranting that ''*the exchange of personal data within the framework of police and judicial cooperation in criminal matters, notably under the principle of availability of information as laid down in the Hague Programme, should be supported by clear rules enhancing mutual trust between the competent authorities and ensuring that the relevant information is protected in a way that excludes any discrimination in respect of such cooperation between the Member States while fully respecting fundamental rights of individuals. Existing instruments at the European level do not suffice*'' (Preamble, par. 5). The implementation of the principle of availability, particularly after the limitation in its scope, is one of the fundamental premises of the DPFD.

In the Hague Programme of October 2004, the European Commission proposed to substitute the principle that data belong to State authorities and can only be transmitted to another Member State on the conditions established by the State that holds the information with the 'principle of availability'. Under the latter principle, the authorities of any

Member State would have the same right of access to information held by any other authority in the EU as applies to equivalent public authorities within the State where the data are held.[44] (The principle of availability is thus a newcomer in the data protection field, an after-9/11 addition that reflects the political climate since. In practice, the principle of availability invites Member States to do away with all national limitations to the work of their judiciary: by virtue of the principle, any police or justice official of one Member State may automatically access data held by its colleagues in another Member State).

The principle of availability evidently held a central role since the 2005 DPFD that had the explicit aim to open the way to ''*interoperability of national databases or direct (on-line) access*''.[45] The final DPFD, however, goes one step further, granting availability-related rights not only among State authorities of Member States but also to third countries, or even to private parties.

The basic function of the principle of availability obviously refers to state (law enforcement) authorities of Member States. These are called in the DPFD '*competent authorities*' (see Definitions in Art. 2). After all, the whole DPFD, as per its scope, applies to ''*personal data that are or have been transmitted or made available between Member States*'' (Art. 1). The DPFD does not include any technical measures, requesting the actual interoperability among police databases of Member States, nor does it introduce a formal procedure for data requests among security agencies in the EU. The ''*transmission*'' and ''*making available*'' of data is taken for granted and not further elaborated. Instead, the conditions for the respective processing are set in Articles 11 and 12 of the DPFD: competent authorities of a Member State may naturally process personal data as per the purposes for which they were transmitted or made available. Under a series of exemptions, however, such competent authorities are allowed to ''*further process*'' the above transmitted or made available data – the list of exemptions is so far-reaching that in practically every case data may be used for purposes totally unrelated to those for which they were originally transmitted or made available. The only possible way out for those Member States that do not wish for their data to be processed for whichever purposes other Member States deem '*relevant*', is to establish nationally stricter processing restrictions; these, if notified accordingly at the time of the respective data transmissions ought to be respected by the recipient Member State.

International data transfers obviously pose a much greater threat. As already noted, even before discussions on the DPFD began, practically all Member States maintained bilateral relationships with third countries, exchanging police information; any one of the Member States would be quite unwilling to forgo, or to re-examine these relationships, under the light of the DPFD. International data flows thus had to be accommodated.

The DPFD expressly caters for international data transfers in its Art. 13: a Member State who has received data from another Member State may transmit such data outside Europe if such transfer is necessary as per the DPFD's purposes (crime prevention, etc.); the receiving party is a State security agency (but not always, as international data transfers may be guided towards private parties too, see below); the original Member State from where the data comes from has consented to such transfer unless it is an emergency; and, more importantly, if ''*the third State or international body concerned ensures an adequate level of protection for the intended data processing*''. The omnipresent 'adequacy criterion' that thus has followed data protection since its first steps, arguably being responsible for its survival over the years, has made it into the DPFD text (naturally, given the 1981 Convention and its Additional Protocol, little space is left for a complete exemption).

The ''*adequate*'' level of protection, however, is to be judged by each Member State by itself. In the 2005 DPFD proposal, a Directive-like system had been set up, allowing some central control on the third countries to which national law enforcement agencies would send data. However, the MDG and ultimately the DPFD itself have moved away from this idea (and any 'comitology' altogether for the same purposes), preferring to leave the task of taking '*adequacy*' decisions to Member States.[46] Given that as a basic DPFD principle bilateral agreements between Member States and third States are expressly not affected by its provisions (Art. 26), the situation in practice is awkward at the very least. Indeed, in the not-unlikely event that a Member State (for instance, Greece) considers that a third country with which it has a bilateral data transfer agreement (for instance, Saudi Arabia) ensures an 'adequate' level of protection and another Member State, that has not a similar bilateral agreement with the same third Member State (for instance, Belgium), does not think in the same way, the practice will, at the very least, prove chaotic. In the above example, under the DPFD Greece will be able to send data of Belgians, transmitted to it by Belgium, to Saudi Arabia, in emergencies without Belgium's consent, even though Saudi Arabia, had it applied directly to Belgium, would not get such access. Under the DPFD the web of international data transfers of EU criminal records is practically impossible to follow, even less to control.

Finally, a great deal of controversy has covered the application of the principle of availability with regard to private parties (in or out of the EU, as international transfers to private parties are allowed under the DPFD). Despite the strong opposition during the negotiations stage, an Article on making available personal information under the DPFD to private parties was ultimately adopted (Art. 14). Regardless of its numerous conditions that have to apply simultaneously upon which such transmission of data may occur, one cannot but wonder why a cooperation between private parties and the police was officially adopted in the text of the DPFD. It might appear that certain privileged organisations, within the private sector, may benefit from personal data collected and processed by the police for its own purposes; the DPFD does not foresee any particular controlling powers of any data

[44] See De Hert P/Gutwirth S, *Interoperability of Police Databases Within the EU: An Accountable Political Choice?* (April 2006), Tilburg University Legal Studies Working Paper No. 003/2006; TILT Law & Technology Working Paper Series No. 001/2006. Available at SSRN: http://ssrn.com/abstract=971855.

[45] See 2005 DPFD draft, p.3.

[46] See Art. 15 of Council's document 13246/13.11.2006 (available at: http://www.statewatch.org/eu-dp.htm).

protection authorities or even simple knowledge of individuals regarding the transfer of criminal records to private parties. In addition, its Preamble attempts to justify the DPFD's political choice on such trivial and petty crimes such as "vehicle crime", protecting "insurance companies" or "improving the conditions for the recovery of stolen motor vehicles from abroad" – hardly a serious justification for the transmission of criminal records by the police to private parties (even less by the principle of proportionality standards). The DPFD's comment that "*this is not tantamount to the transfer of police or judicial tasks to private parties*" only serves to aggravate the situation, sounding even more threatening to potential infringement of individual rights.

5.4. *Schengen JSA, Europol JSB, the Eurojust JSA and the CIS JSA*

The final point to be noted in this paper, with regard to data protection policy options behind the DPFD, refers to the data protection supervisory bodies.

As already underlined, the DPFD came in late, practically reversing the normal law-making order: usually, first a general text lays down the general rules and principles and then case-specific legislation follows, implementing these general rules and principles into specific sectors. Security-related data protection legislation in the EU did exactly the opposite: case specific provisions were released (and indeed have been implemented widely) and only after several years has the general, principle-laying text (the DPFD) followed.

Sector-specific legislation in security-related European data protection refers mostly to the Schengen Agreement(s), Eurojust and Europol. All these instruments include in their texts data protection provisions, have several years of implementation in practice and have established their own mechanisms and principles. In fact, all police and judicial cooperation instruments have established their own data protection controls and agencies (the Schengen Joint Supervisory Authority (JSA), the Europol Joint Supervisory Board (JSB), the Eurojust JSA and the CIS JSA). With the exception of the Eurojust JSA, all these agencies are actually composed of almost the same representatives,[47] who generally are, moreover, the very same people who participate in the Article 29 Working Party to discuss matters related to the First Pillar as representatives of their own national supervisory authorities. Those representatives, nevertheless, do not have an institutionally recognised forum allowing them to meet and discuss at EU level data protection in the Third Pillar in general.

The situation was thus problematic even before the release of the DPFD. Solutions were suggested from both poles of data protection. The European Data Protection Commissioners met on 14 September 2004 in Wroclaw, Poland and adopted a Resolution to set up a "*joint EU forum on data protection in police and judicial cooperation matters (data protection in the Third Pillar)*". The Resolution highlighted the contrast between the First Pillar, where the Article 29 Working Party is in place, and the Third Pillar, where there is no equivalent body; the three joint supervisory bodies covering Europol, Schengen and Eurojust have specific mandates and, according to the resolution, "*a broader approach is required to secure a uniform level of data protection safeguards for the whole area of police and judicial cooperation*".[48]

The Commission in its original 2005 DPFD draft aimed at affecting as little as possible other, already existing police cooperation instruments[49] and, indeed, the proposed text did not replace those specific regulations.[50] In the same spirit, there was also no question of merging the different Joint Supervisory Authorities. Instead, the Proposal (in its "comitology" part) chose to establish a sort of Working Party, in a way parallel to the Directive's Article 29 Working Party, allowing the representatives of the existing Joint Supervisory Authorities to meet and conduct together a consultancy role on matters related to the Third Pillar.

The other data protection pole obviously rejected any thought of granting central control, and thus power to regulate national matters, to any EU instrument in the Third Pillar. These national agendas were expressed mostly through the MDG that had been since the beginning not very favourable towards this aspect of the original 2005 Draft Proposal.[51] On the other hand, one of the priorities of the German Presidency, whose policy decisions ultimately shaped the DPFD, was to merge the different Third Pillar data protection bodies – an initiative strongly opposed mostly by the Eurojust JSA. This initiative was obviously abandoned while in the negotiations' stage within the MDG for the drafting of the DPFD (see Art. 28).

The text of the DPFD ultimately adopted takes none of the above into consideration. The co-ordination and cooperation difficulties that were presumably to be addressed by the DPFD continue to be relevant at least for the foreseeable future.

Article 28 of the DPFD ('Relationship to previously adopted acts of the Union') states that existing laws on the exchange of personal data will take precedence over the provisions of the DPFD when they contain specific conditions as to the use of such data by the receiving Member State. Paragraph 39 of the Preamble of the DPFD on legal texts that contain "a complete and coherent set of rules covering all relevant aspects of data protection" suggests no effect or impact of the DPFD on these texts: "The relevant set of data protection provisions of those

[47] "*Indeed it is common for the same person to sit on all three JSAs under a different hat (applying different rules)*" (The European Union Committee, "European Union – Fifth Report", Ordered by the House of Lords to be printed 22 February 2005, http://www.publications.parliament.uk/pa/ld200405/ldselect/ldeucom/53/5302.htm).

[48] Resolution to set up a "*joint EU forum on data protection in police and judicial cooperation matters" (data protection in the third pillar)*" adopted on 14 September 2004 by the European Data Protection Commissioners meeting in Wroclaw, Poland. According to this network of representatives of national data protection supervisory authorities, "*There is no alternative to creating a high and harmonized data protection standard in the EU Third Pillar*" (see, *Declaration adopted by the European Data Protection Authorities*, London, 2 November 2006).

[49] See Preamble (20) and Chapter VIII of the 2005 DPFD Proposal, where only specific provisions seem to be affected by it, rather than all of its principles expressly superseding any other provisions of the same subject matter.

[50] It even let them explicitly untouched, see recital 39 of the 2005 DPFD draft.

[51] See the 2005 DPFD drafts during the 2006 processing stage, as provided at Statewatch (http://www.statewatch.org/eu-dp.htm).

acts, in particular those governing the functioning of Europol, Eurojust, the Schengen Information System (SIS) and the Customs Information System (CIS), as well as those introducing direct access for the authorities of Member States to certain data systems of other Member States, should not be affected by this Framework Decision''. However when existing laws have a more limited scope; the rules set out in the DPFP should be applied (paragraph 40 of the Preamble of the DPFD).

There is some wisdom in this approach to leave legal texts with a solid complete scheme of data protection unaffected. Nevertheless it is, so we believe, not to be excluded that even in cases where a complete scheme of data protection provisions is present, one could call upon some of the provisions in the DPFD. The silence of the DPFD on this matter, only partly remedied for in the Preamble, could then be used to the advantage of the protection of the rights of the individual.

6. Conclusion

The DPFD is a much-needed and long-overdue text, which however is more about police and judicial cooperation than about data protection. It is a readable text allowing law enforcement authorities to check on their data protection duties when transferring data outside their national borders. However, it is far from perfect and all-encompassing. It's drafting circumstances (DG Justice and the MDG, no data protection proponents, no Parliament or EDPS representation) and the international politics (war against terrorism) reversed hopes and expectations. Rather than a text that would resolve data protection matters, it apparently became a text that created more problems for the protection of individual privacy. This privacy 'doom scenario' did not realise itself, but the final text does contain some shortcomings. Most importantly there is the problem of the limited scope of the DPFD, leaving national processing of data by police and judicial authorities untouched. However, it may be that this very scope limitation actually represents a narrow escape for data protection altogether. Because the DPFD, due to its scope, is not the data protection text everybody expected, it may be that it is just the preliminary text for the one to follow, after all the practical shortcomings of this one become visible. Hopefully, by that time, the international agenda will have again switched from the war against terrorism to protecting individual rights once more.

Acknowledgement

The authors wish to thank Herke Kranenborg for careful review of drafts.

Paul De Hert (*paul.de.hert@uvt.nl*) *is Professor at the Vrije Universiteit Brussels (LSTS) and associate professor at Tilburg University (TilT).*

Vagelis Papakonstantinou (*vpapakonstantinou@pkpartners.gr*) *is lecturer at the University of Patras and Partner in PKpartners Law Firm in Athens, Greece.*