SCL The IT Law Community
SCL Forum
www.scl.org

The Police and Criminal Justice Data Protection Directive: Comment and Analysis

Paul De Hert and **Vagelis Papakonstantinou** offer a first comment on the proposed draft Directive. This article is a much updated reflection of a contribution to the SCL's 6th Annual Policy Forum held in September 2011

What is the current legal data protection framework for the Area of Freedom, Security and Justice (AFSJ)[1] personal data processing and what framework *could* be created in the near future? These two questions are constantly recurring in the EU data protection field, particularly after the ratification of the Lisbon Treaty. The amendment of the EU data protection regulatory framework currently under way offers a unique opportunity to re-evaluate past regulatory options and plan for the future.

Today, a regulatory patchwork is witnessed in AFSJ personal data processing (see **1. Does the proposed Directive simplify the current regulatory patchwork?** below). The complexity of this system was probably to be expected, given the Pillar system in the pre-Treaty of Lisbon environment. Commercial and general-purpose processing was separated from security-related processing. While the former benefited from a standard-setting Directive in effect since 1995,[2] the latter attracted the legislators' interest only after 9/11 turned the focus to personal data processing for security purposes; the Framework Decision[3] introduced only in 2008 largely failed to meet expectations, at least from a data protection point of view.[4]

Nevertheless, it ought to be acknowledged that security-related personal data processing presents a series of unique characteristics that make specialized data protection regulations necessary (see **2. Why a separate Directive is needed?** below).

A long consultation period led to the, simultaneous, release by the Commission of two draft instruments: the General Data Protection Regulation,[5] intended to replace the 1995 Directive, and the Police and Criminal Justice Data Protection Directive, intended to replace the 2008 Framework Decision. In this way, the Commission made a choice among the law-making options at hand, and introduced again two sector-specific instruments rather than one of general application, broadly following the older Pillar distinction (see **3. Main provisions of the Directive** below).

The amendment of the EU data protection framework is an ambitious task. From the 1995 Directive point of view, it needs to update the regulatory framework into the new Internet reality and also to address harmonisation difficulties among Member States. More substantial work is expected, however, for the AFSJ regulatory framework. The new instrument, supposedly replacing the 2008 Framework Decision, needs to address the shortcomings of the past as well as newly emerged challenges relating to the profiling and networking society (see **4. Profiling** and **5. Networked law enforcement and transparency** respectively), in order to at last provide individuals with effective means to exercise their right to data protection in the AFSJ context.

1. Does the proposed Directive simplify the current regulatory patchwork?

Police and judicial cooperation matters occupy a specific position in the field of data protection. The first data protection acts were introduced in view of the growing reliance of state administrations on computer systems that enabled the massive and automated processing of personal dataLater, the main preoccupation shifted towards the processing of personal data by private bodies for commercial purposes. The 1995 Directive, adopted after the entry into force of the Maastricht Treaty,

reflected both these concerns and the specific institutional set-up of the EU. It dealt accordingly with 'First Pillar' commercial and general-purpose processing, while processing performed by judicial, police and security services (so-called 'Third Pillar') was explicitly omitted.

While the 1995 Directive set the standards within its field of application, no similar standard-setting text existed in the field of police and judicial cooperation until 2008. Until that time, standards were rather set by the Council of Europe's Convention 108. Further elements of data protection derived from the sector specific measures adopted in the legal instruments on the Schengen Information System, Europol, Eurojust and the Prüm Decision among others. Data protection regulations for security-related processing were thus not introduced in the anticipated order: rather than first introducing a standards-setting instrument to be followed by sector-specific regulations, quite the opposite took place.

Personal data processing for security purposes gained exponentially in importance after 9/11. The terrorist attacks in several EU capitals further strengthened the request by security agencies, both in and out of the EU, to be provided with more extensive and efficient means to massively process the personal information of individuals in order to facilitate their work . Due to the favorable political and social environment, such means were granted.

Originating from an agreement between the Council and the Parliament following the concerns voiced by the latter during the adoption of the 2006 Data Retention Directive, the 2008 Framework Decision was adopted on 30 December 2008 after a long and protracted negotiation. It gives priority to the concerns of judicial, police and security services; commentators note in particular that the scope of the 2008 Framework Decision is limited to cross-border processing, leaving aside the questions of domestic processing and its streamlining with the instruments already in place (Schengen, Europol etc). More importantly, it provides for exemptions from almost every data protection principle. In addition, since no supervisory body (mirroring, for instance, the 1995 Directive's Article 29 Working Party) has been set up in the 2008 Framework Decision, the data-protection principles featured in the instrument have not been incorporated into EU policy-making.

The Commission took notice of the 2008 Framework Decision shortcomings during the consultation period for the amendment of the EU data protection regulatory framework. In its Communication, it highlighted the lack of regulations for AFSJ domestic personal data processing, the wide space for exemptions to fundamental data protection principles, as well as the fact that the 2008 Framework Decision does not replace the multitude of sector-specific legislative instruments in effect or even clarify the relationship among them.

In response to these concerns, the Commission released the draft Police and Criminal Justice Data Protection Directive. With regard to the regulatory patchwork, the draft Directive is not aimed at introducing a hierarchy – on the contrary, it expressly leaves '*unaffected*' previously adopted acts within its subject-matter (in its Article 59). On the other hand, it does ask Member States to amend their bilateral agreements as per its provisions (in its Article 60). From this point of view, the draft Directive takes a, bold, first step in order to create a processing environment whereby differentiations from its principles and regulations will be increasingly hard to justify.

2. Why a separate Directive is needed

The last decade witnessed the release of AFSJ personal data processing instruments at an unprecedented rate. The experience gained from their implementation is too valuable to be overlooked. In particular, two important lessons stand out. The first relates to the fact that law enforcement personal data processing presents a series of unique characteristics that make specialized treatment necessary.

As far as law enforcement personal data processing is concerned, a number of special conditions need to be somehow acknowledged and accommodated in any relevant regulations. For instance, law enforcement agencies thrive on 'hearsay', and thus not in data quality-certified personal information. Moreover, they may need to keep data for very long periods, if possible for ever, and correlate them incessantly in relation to crimes which appeared irrelevant when the data first appeared. Also suspects need not have complete access to their files or even be informed that they are under police scrutiny until they are charged with a crime. Profiling, although a risky enterprise (see **4. Profiling** below), may at times provide important results.

These characteristics require special, accommodating data protection provisions. The 2008 Framework Decision was perhaps exceedingly accommodating towards them. The draft Police and Criminal Justice Data Protection Directive seems to be adopting a more balanced approach: although specialized conditions of processing are acknowledged (for instance, in Articles 5 and 6), the general rules and principles of data protection – rather than exceptions to them – continue to apply in the field.

The second lesson learned pertains to the fact that the distinction between commercial and security personal data processing was proven to be schematic and artificial. In other words, distinguishing in practice between commercial and security personal data processing is extremely difficult, if not impossible; hence, a system of two legal instruments based on exactly this distinction will not help. Apart from clear-cut cases whereby, for instance, data is collected by the police and kept in its systems, it is very likely that data collected by commercial data controllers in the course of their duties are used by law enforcement agencies; even the opposite is not inconceivable. Case law provides very little assistance to this end: although PNR processing was ultimately considered security-related, electronic communications processing was considered commercial processing.

Consequently, the criterion here ought be data and not controller-centric: once a dataset is created it may be put to any use at all, from marketing and credit scoring to terrorist combat and parking ticket collecting. Choosing which regulations to apply based on the data's users rather than its uses is misguided

in the contemporary processing environment.

3. Main provisions of the Directive

The Commission, while preparing the amended EU data protection framework, had two realistic options at hand: (1) to release a single, comprehensive, standard-setting text that would set the general rules for all personal data processing within the EU, or (2) to continue distinguishing between commercial and security-related processing through the continued existence of the 1995 Directive and the 2008 Framework Decision, appropriately amended, respectively. Apparently, the Commission chose to replace both documents simultaneously, broadly following the model already in effect.

The Police and Criminal Justice Data Protection Directive is divided into 11 chapters, each regulating a specific data protection aspect. Chapter I contains its scope of application, that now extends to domestic processing too, as well as the definitions used in its text – important additions refer to the terms of 'personal data breach', 'genetic' and 'biometric' data.

Chapter II of the Directive lays down the principles of the processing, expressly following those of the 1995 Directive and the Regulation intended to replace it. Explicit reference is made to the transparency and to the data minimisation principles. It is mostly in this Chapter that flexibility options for the processing of personal data are afforded in the AFSJ context, enabling data controllers to process personal information (including sensitive data) of varied quality, for purposes other than those they were collected, using profiling techniques, if needed.

The rights of individuals are set in Chapter III of the Directive: the rights to information, access to data and objection to the processing are to be found among these provisions, properly adapted in the AFSJ context.

Chapters IV, VI and VII refer to the enforcement mechanism: this is to be composed of supervisory authorities at Member State level and a European Data Protection Board. These are complemented by provisions on '*remedies, liability and sanctions*' set in Chapter VIII. Finally, international data transfers are regulated in Chapter V.

As expressly set in many instances in its '*detailed explanation'*, the Directive follows, whenever possible, the provisions of the General Data Protection Regulation and the 1995 Directive and also, at times, older suggestions by the Commission that were abandoned while introducing the 2008 Framework Decision. Differentiations in view of the special needs of AFSJ processing are of course to be expected, but even these are placed under close scrutiny. From this point of view, the Directive appears to be making a positive contribution to the individual right to data protection, finally affording data subjects the means to protect their rights effectively.

4. Profiling (Article 11 of the Directive)

Although a generally accepted definition is yet to be seen , profiling is broadly understood as the creation of individual profiles through processing-intensive methods and the undertaking of actions based on such findings. As such, it has gained in importance in the AFSJ context. Notwithstanding differentiations in terminology, profiling may be found to be the basis of several EU law enforcement processing activities (for instance, VIS or PNR), because it is intrinsically connected to the trend towards generalization of data processing in view of the development of 'a stronger focus on the prevention of criminal acts and terrorist attacks before they take place'. Nevertheless, in all the above cases, no mention is made of the data protection safeguards that need to be implemented for the protection of individuals. This may be illustrated, for instance, in the latest EU 'Proposal for a Directive on the use of PNR data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime', whereby although 'assessment of passengers' procedures form the basis of the relevant processing, its single article on data protection (Article 11) says nothing on the conditions under which such processing is to take place.

The 2008 Framework Decision and the 1995 Directive do not deal with profiling in concrete terms, but rather incidentally refer to it (in Articles 7 and 15 respectively) by way of automated-decisions on individuals.

Consequently, today profiling operations in the AFSJ context are gaining in importance without, however, this development being followed by effective and adequate data protection regulation.

The draft Directive expressly refers to profiling in Article 9. Its provisions, while adopting a realistic approach, make significant improvements over the regulatory framework in effect today. The Directive takes note of profiling and the potential impact it may have for AFSJ personal data processing. It therefore allows it to take place, but makes it subject to certain conditions. Perhaps the most important is that it cannot be based on sensitive data (data revealing ethnic origin, political opinions, religion, sexual preferences etc). Secondly, it requires a special law to be introduced to regulate such processing. The merits (and the lawfulness) of such law will be evaluated against the Directive's provisions, taking into consideration too that the individual right to data protection is by now acknowledged in the EU Treaty (Art. 16 TFEU), as well as the potential accession of the EU to the ECHR (so the ECtHR case law will also apply).

The fact that the Directive attempts to provide a definition for profiling should also not go unnoticed: '*automated processing of personal data intended to evaluate certain personal aspects relating to the data subject*'. The task of defining profiling is by no means easy or straightforward. The Commission seems to require '*automated*' processing that is aimed at making an '*evaluation*' of specific individuals' '*personal aspects*'. While the '*automated*' criterion seems reasonable, it appears that the Commission has in mind an *ad hoc* processing operation, setup and executed in order to single out certain individuals based on their specific characteristics. As such, it may be limiting, as it excludes, for instance, incidental profiling (applying 'profiling-type' search criteria within the search results of already executed, normal, processing)

or non-evaluatory profiling (not evaluating, but merely identifying data). In addition, the fact that '*personal data*' are required may also prove limiting: processing-intensive methods may use various datasets to reach the, necessarily vague, conclusions that are the aim of profiling operations. The Commission therefore could perhaps make the definition of profiling more general in the next versions of the Directive.

5. Networked law enforcement and transparency (Article 4 of the Directive)

Personal data processing for security-related purposes has become by now a network phenomenon. Data processors come in various forms and legal statuses, including EU organisations, national law enforcement agencies and private parties. The EU data protection framework in effect today has enabled a web of personal information exchanges whereby access is requested, and customarily granted, to a multitude of datasets, ranging from passenger to telecommunications records. At its base lie the provisions of the 2008 Framework Decision.

Explicit reference is therefore needed in the Directive's text to the principle of transparency**.** Its application would bring substantial changes to AFSJ processing as executed to date. Data controllers would need to execute their processing in an easily identifiable and controllable way. Processing would need to be open and accessible to the individuals concerned as well as to the data protection authorities and to any third party with an interest in inquiring into its operation and effectiveness. In addition, an efficient data protection enforcement mechanism would have to be established, both at Member State level and at EU level.

The Commission mostly succeeds in addressing the above challenges in its draft Directive. AFSJ processing at Member State level is placed under the controlling powers of a supervisory authority, which could be the same as the supervisory authority required by the General Data Protection Regulation. In addition, the European Data Protection Board established under the same Regulation is to oversee processing within the Directive. The Commission also establishes the principle of transparency as one of the draft Directive's guiding principles (in its Article 4). Finally, the Commission introduces into AFSJ personal data processing a series of new controlling instruments: the requirement for data controllers to engage in prior consultation with supervisory authorities, rules as to data breach notifications and the introduction of Data Protection Officers are all mechanisms that are expected to increase transparency and awareness. This is a useful contribution within the networking society context.

However, the draft Directive could perhaps do more to assist individuals while protecting their data protection rights in the AFSJ processing context. The acknowledgement of the special circumstances that necessitate a special legal treatment for AFSJ personal data processing ought to be compensated by an equal strengthening of the individual's position. To this end, the Commission ought to consider introducing a reversal of the burden of proof in favour of individuals – or even a right to notify individuals after AFSJ-related processing of their personal data is completed without any needs for further investigation).

Conclusion

The regulation of AFSJ-related personal data processing has been a much debated issue within the EU for the past few years. The exponential growth of the processing of personal data for security purposes witnessed within the context of the post-9/11 environment was not followed by equally effective regulations for the individual right to data protection. The (until recently) limited options for an EU regulatory intervention in the relevant fields only added to this discrepancy. It was under these circumstances that the 2008 Framework Decision was released, overall offering very little in practice to data subjects across the EU.

On the other hand, the fact that AFSJ personal data processing presents certain distinguishing characteristics that differentiate it from any other type of processing cannot be overlooked.

The Commission attempts to bridge the above differences in its draft Directive. It acknowledges the special needs of AFSJ processing, hence it grants it a specialized Directive rather than submitting it to the General Data Protection Regulation. It allows profiling. It also chooses not to take the extra step to protect individuals, through, for instance, a reversal of the burden of proof or the right to be notified once the investigation is over.

On the other hand, individual data protection is expected to benefit from the firm application of data protection rules over Member State AFSJ processing,. overseen by supervisory authorities and a European Board, in exactly the same way as with any other personal data processing in the EU. The grave risks for individual data protection created by the networking and profiling societies are acknowledged in the draft Directive text, and positive (regardless whether adequate or not) measures are taken to address them.

The draft Directive appears therefore to be a balanced text that caters to the needs of all its recipients, data controllers (security agencies) and data subjects alike. Although the Commission in this case apparently builds upon poor premises (the 2008 Framework Decision), it quickly distances itself from them and introduces a draft text that for most of its part resembles the General Data Protection Regulation. The law-making process is expected to be long, particularly in view of the many changes that the draft Directive intends to introduce in AFSJ processing in the EU. However, as long as the basic principles of the text at hand are preserved, individuals swill at last profit from strong data protection regulations in the AFSJ field – a long overdue, and mostly unjustified, omission that will finally be rectified. ●

Professor Paul De Hert is a Professor at the Vrije Universiteit Brussels (VUB –LSTS) and an associated-professor at Tilburg University (TILT).

Vagelis Papakonstantinou is a member of the Vrije Universiteit Brussels (VUB –LSTS) and a scientific assistant at the International Hellenic University.

Endnotes

1. This article will use expressions such as 'data processing in the field of police and judicial cooperation' and 'AFSJ personal data processing' without making any distinction.
2. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281 , 23/11/1995 pp.0031–0050 (the '1995 Directive').
3. 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 (the '2008 Framework Decision')
4. See, for instance, Paul de Hert and Vagelis 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,' *Computer Law & Security Review* 25 (2009): 403–414.
5. European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 Final, 25.01.2012.
6. See European Commission, Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final, 25.01.2012.
7. Art.3.2. excludes activities falling outside of Community law as well as 'processing operations concerning public security, defence, State security […] and the activities of the State in the area of criminal law'.
8. The implementation of these rules are supervised by distinct bodies, including the Schengen joint supervisory authority (under Art.115 of the Schengen Convention), the Europol JSB (under Art.24 of the Europol Convention), the Eurojust JSB (under Art.23 of the Eurojust Decision).
9. See, for instance, the Data Retention Directive, Preamble, 10.
10. See the Economist series on Terrorism and Civil Liberty back in 2007, in particular, Civil liberties: Surveillance and Privacy, 27.09.2007.
11. The limitation of the scope of the 2008 Framework Decision to cross-border exchanges was introduced at the behest of a number of Member States and associate countries, including the Czech Republic, Denmark, Ireland, Malta, Sweden and the United Kingdom, as well as Iceland and Switzerland. See de Hert and Papakonstantinou (2009), for a more detailed analysis of the drafting process of the 2008 Framework Decision and of its contents from a data-protection perspective as well as de Hert and Bellanova's (2009) briefing note on behalf of the LIBE Committee.
12. Very briefly, these core principles – initially promoted by the first data protection legislations adopted in the 1960s and 1970s by European countries – include the principle of fair and lawful collection and use of data and data quality principles such as the principal of proportional collection and processing of personal data, the principle of data security, and the purpose specification principle.
13. It was considered in the Commission's initial proposal, but was edited out in subsequent rewritings of the instrument.
14. See, European Commission, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union, COM(2010) 609 final, 4.11.2010 (the 'Commission Communication').
15. See Commission Communication, pp.13–14.
16. Apart from the 2008 Framework Decision see also the PNR Agreements between the EU and third countries (the USA, Canada and Australia), the efforts to introduce an intra-EU PNR instrument, the Data Retention Directive etc.
17. After all, the 'specific nature' of the judicial cooperation in criminal matters and police cooperation fields has been acknowledged in the Lisbon Treaty Declarations (21).
18. See Article 60 of the draft Police and Criminal Justice Data Protection Directive.
19. On PNR-related processing, that was found security-related despite the fact that data are collected by airline carriers for commercial purposes, see, for instance, Vagelis Papakonstantinou and Paul de Hert, 'The PNR Agreement and Transatlantic anti-Terrorism co-Operation: no Firm Human Rights Framework on either Side of the Atlantic,' *Common Market Law Review* 46 (2009): 885–919.). On the other hand, the retention of telecommunications data, equally collected by telecommunications providers for commercial purposes, has been judged as commercial processing (as established by the ECJ in its Case C-301/06, Ireland v. Parliament and Council).
20. To-date, the EU documents on profiling from a data protection point of view only consist of a recommendation of the European Parliament (European Parliament recommendation to the Council of 24 April 2009 on the problem of profiling, notably on the basis of ethnicity and race, in counter-terrorism, law enforcement, immigration, customs and border control (2008/2020(INI)), and a Council of Europe Recommendation (Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, 23 November 2010)
21. COM(2011) 32 final.
22. Data Protection Impact Assessments have, however, been taken out from the formal Commission draft Directive, in comparison to its version leaked in November 2011.
23. Such a reversal would after all be in line with fundamental case law by the ECtHR, see ECtHR, K.U. vs Finland, judgment of 2 December 2008.
24. See also De Hert P/Boehm F, The rights of notification after surveillance is over: ready for recognition? available at http://digitalrights.leeds.ac.uk/papers/right-of-notification-after-surveillance/.