Data protection in the area of freedom, security and justice. A short introduction and many questions left unanswered

Paul de Hert · Cornelia Riehle

Published online: 13 July 2010 © ERA 2010

1 General background

Data protection is one of the main issues raised in the development of the European area of freedom, security and justice (AFSJ). The introduction of measures touching upon data protection is coinciding with growing dilemmas as to how best to ensure individuals’ fundamental rights. Is current legislation on data protection adequate to the challenges posed by specific technologies and specific policies? Do the main actors have adequate powers to shape legislation and enforce controls? Do the Data Protection Framework Decision and the Lisbon Treaty offer satisfactory means to cope with present loopholes? These are some of the questions that are at the heart of the contributions in this issue.

1 Most contributions in this issue are based on presentations held in the following conferences which were organised by the Academy of European Law Trier and which were held in the first half of 2010:

- Data Protection in the Field of Justice and Home Affairs, Third International CPDP Conference, Brussel, 30 January 2010, 31O06;

P. de Hert (✉)
Faculties of Law of the University of Tilburg and Vrije Universiteit, Pleinlaan 2 Building B, 1050 Brussels, Belgium
E-mail: paul.de.hert@uvt.nl

C. Riehle
European Public and Criminal Law Section, Academy of European Law, Metzer Allee 4, 54295 Trier, Germany
E-mail: criehle@era.int
Let us briefly recall the bare essentials of European Union data protection law in the past. Protection of individual privacy and of personal data in Europe is based on several instruments both of international and of European Community law. Privacy protection relies in the main on Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and on Articles 7 and 82 of the Charter of Fundamental Rights of the European Union. More concrete legal norms are spelled out in the following documents.

1. Directive 95/46/EC—the so-called Data Protection Directive3—is the main piece of legislation concerning data protection in Community law. The objective of the Data Protection Directive is twofold: it aims both at protecting "the fundamental rights and freedom of natural persons, and in particular their right to privacy with respect to the processing of personal data" (Art. 1(1)), as well as ensuring the free flow of personal data (Art. 1(2)). However, it does not apply to the processing of data "in the course of an activity which falls outside the scope of Community law, such as those provided for by Title V and VI of the Treaty of the European Union and in any case to processing operations concerning public security, defence, State security (…) and the activities of the State in areas of criminal law" (Art. 3(2) 1st para.). The judgement of the European Court of Justice on the Passenger Name Record (PNR) cases has further curtailed the reach of the Data Protection Directive by establishing the criterion of the primacy of the final purpose of processing over the very nature of data collection.4 Notwithstanding such limitations, the Data Protection Directive remains a relevant reference for the development of data protection in the area of Freedom, Security and Justice for at least three reasons: it covers first pillar AESJ policies, such as those related to illegal immigration, visa and asylum;5 it created two of the main actors in data protection: the national data protection authorities and the Art. 29 Working Party6 and, finally, the definitions and principles of the Directive remain the main reference for the data protection provisions of other instruments.

2. Council of Europe Convention No. 108—the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data—provides a legally binding enumeration of data protection principles7 concerning: data quality, including a range of principles ranging from fair and lawful collection to purpose limitation

---

2 Article 8 which concerns “protection of personal data” states: “(1) Everyone has the right to the protection of personal data concerning him or her. (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. (3) Compliance with these rules shall be subject to control by an independent authority”.


4 Cf. Paragraphs 55–59 of joined cases C-317/04 and C-318/04.

5 The Data Protection Directive thus covers the EURODAC database and will partially cover the Schengen Information System II (SISII) and Visa Information System (VIS) databases.


 Springer
to adequate, relevant and not excessive collection (Art. 5); special categories of data (Art. 6); data security (Art. 7) and data subjects’ rights (Art. 8). Because of the limitations of the scope of Directive 95/46/EC, Convention 108 is the main reference point in the field of police and judicial cooperation. Several ‘third pillar’ instruments (instruments adopted in the framework of Title VI of the European Union Treaty) which provide for ad hoc data protection provisions use this Convention as a threshold. However, the Convention provides that its data protection guarantees can be submitted to legitimate derogations when these are provided for by the law of a Contracting Party and when they constitute “a necessary measure in a democratic society in the interest of: (a) protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences” (Art. 9). Furthermore, the Convention was drafted before new information technologies such as data mining and profiling were made available and deployed on their present massive scale, and also risks falling short insofar as concerns offering safeguards from new challenges.

3. There are also many ad hoc instruments contributing to data protection in the area of Freedom, Security and Justice, especially in the field of security, such as: ad hoc data protection rules in AFSJ instruments; the ad hoc data protection rules of European agencies such as Europol and Eurojust; ad hoc data protection rules in international agreements on data exchange between the European Union and third countries; ad hoc data protection rules in international agreements on data exchange between Europol and third countries, and, finally, national laws.

4. The foregoing shows that prior to 2008, data protection in the area of Freedom, Security and Justice was scattered not merely because of the European pillar structure, but also because third pillar data protection itself was a real jigsaw puzzle of ad hoc data provisions and national laws. The Data Protection Framework Decision which was finally adopted on 27 November 2008, after three years of debates and discussions, was introduced to offer a comprehensive framework of data protection in the field of police and judicial cooperation.

---


10 Prüm Council Decision and the Visa Information System.


12 EU-US PNR, EU-Australia PNR, SWIFT.

13 Europol has the possibility of applying two kinds of international agreement with third countries or international bodies and institutions: strategic and operational agreements. Only the latter implies exchange of personal data. Europol has concluded this kind of agreements with, among others, United States, Canada, Iceland, Switzerland and Eurojust. A full and updated list of international agreements is available at: http://www.europol.europa.eu/index.asp?page=agreements.

The Framework Decision created a general regime for data protection in the ‘third pillar’. It confirmed the applicability of general data protection principles (such as legality, proportionality, right to access, erasure and rectification, judicial remedies) to the sector of police and judicial cooperation in criminal matters.

The question of integration also forms part of the subject of an article by Jeannine Dennewald in this issue, however, in the much broader context of the entire European judicial area. In her article, Dennewald explains the diverse mechanisms and reasons which have led to what is often referred to a ‘variable-geometry’ Europe and analyses its future development under the Treaty of Lisbon.

2 Problems with the Framework Decision on Data Protection

It is important to present and discuss at least four central issues concerning the Framework Decision on Data Protection; (i) scope; (ii) automated individual decisions and special categories of data; (iii) National Data Protection Authorities and (iv) transfer to third countries.

1. The scope of the Framework Decision has been confined to data which is exchanged among member states, as well as among member states and authorities or information systems which have been established on the basis of the Treaties (Art. 1(2)(a), (b) and (c)). Hence it is limited to the processing of data in cross-border cases.

Apart from the exclusion of domestic data, two other sets of data are excluded from scope of the Data Protection Framework Decision. The Framework Decision does not affect (a) the more specific regime provided, for example in relation to Eurojust, Europol, the Schengen Information System or the Customs Information System; (b) data exchanged in the frame of “existing obligations and commitments incumbent upon Member States or upon the Union by virtue of bilateral agreements with third States” (recital 38) or (c) acts adopted on the basis of Title VI TEU that contain ad hoc data protection provisions (recital 39). Among the last category are, Europol, Eurojust, Schengen Information System and Customs Information Systems acts, as well as the Prüm Decision. Such a limited scope has been, and is still, one of the main focuses of criticism from both the European Parliament and the European Data Protection Supervisor. Such a limited scope risks undermining the level of protection of personal data, fostering divergences in the national standards and adding complexity to the field. In his article in this issue, Hilke Hijmans argues in favour of one comprehensive legal data protection framework covering the entire area of Freedom, Security and Justice which he considers the only means to achieve legal certainty. However, as can be seen from the articles by Diana Alonso Blas and Michael Niemeier in this issue, there are also strong arguments in favour of tailor-made legal data protection framework. In her article, Alonso Blas underlines the specific nature of personal data in the field of police and judicial cooperation in criminal matters where the data of crime suspects, victims and witnesses alike are processed—inevitably requiring, according to Alonso Blas, for differentiated regulations (e.g., regarding the right to information or to object).

The question of legal certainty is also at the heart of the article by Catherine Kessedjian in this issue in which she analyses the case-law of the European Court
of Justice and finds a growing tendency by the Court to create exceptions to the rules on res judicata so as to enforce the effectiveness of European Union law.

2. Given the increased relevance of profiling techniques, the issues of “automated individual decisions” (Art. 7) and “processing of special categories of data” are very sensitive ones. On these topics, the Framework Decision has a “yes, but…” approach. Processing of sensitive data is allowed subject to a requirement of strict necessity and on the condition that adequate safeguards are provided by national law (Art. 6). “Automated individual decisions” are permitted if authorised by law—which also lay down safeguards for the legitimate interests of the subjects of data (Art. 7). In both cases, the 1995 Data Protection Directive adopted the opposite form of wording, establishing a general prohibition and permitting processing as an exception (Art. 15 on “automated individual provisions” and Art. 8 on “the processing of special categories of data” of the 1995 Directive), as did the Council of Europe Convention 108 on “special categories of data” (Art. 6). That the rights of the data subject can be easily infringed by national law is shown in Hilde Hijmans’ article in this issue giving the example of German Constitutional Court’s judgment on the German law implementing the Data Retention Directive. In its judgment, the Court declared some of the German provisions unconstitutional in their present form and called for very strict provisions concerning access and use.

The growing importance of countering crime with technologies, on the other hand, is illustrated in the article by Laviero Buono in this issue illustrating the growing danger caused by “cybercrime”, which encompasses a wide range of crimes starting from familiar kinds of criminal behaviour which happen to be conducted by using a computer (such as computer-related fraud) to new forms of crime such as ‘phishing’ or ‘skimming’. In his article, Buono outlines the main legislative and non-legislative initiatives at European Union and Council of Europe level and calls for systematic training for European Union judges and prosecutors in order to successfully combat cybercrime.

3. The Data Protection Framework Decision states that 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 [the] Framework Decision” (Art. 25). The Framework Decision also specifies certain powers for those data protection authorities: investigative powers (Art. 25(2)(a)); effective powers of intervention (Art. 25(2)(b)); and the power to engage in legal proceedings (Art. 25(2)(c)). As is stated in recital 33, these data protection authorities should be independent. How topical and complex the question of independence of data protection authorities can be was just recently illustrated when the European Court of Justice decided that data protection authorities in the German Länder were not completely independent and further defined the notion ‘completely’. A detailed analysis of the judgment is offered in the article by Hilde Hijmans in this issue. It is important to emphasise that even if the Data Protection Framework Decision follows the example of the Data Protection Directive, it nonetheless does not set up any working party parallel to that under Art. 29 of the Directive—notwithstanding the fact that the European Parliament proposed an amendment to contrary effect. However, recital 34 does leave open the possibility of entrusting data protection authorities, which have already been established, with new responsibilities. As is discussed below, in that case, a certain degree of coordination and harmonisation could
be assured through existing channels of cooperation. In her article in this issue, however, Diana Alonso Blas looks very favourably on the existing system of specialised supervision for Europol, Eurojust, and the Schengen Information System. Taking the example of Eurojust, she sees the main reason that its joint supervisory body functions so well is due to its specialised nature.

4. Finally, among the main shortcomings of the Framework Decision, there are the rules on the “transfer to competent authorities in third States or to international bodies” (Art. 13). The Framework Decision defines four criteria for transmission, linked to the principle of purpose limitation; quality of the recipient; prior consent of the originally transmitting Member State and an adequate level of protection (Art. 13(1)). However, the latter criteria is weakened by three major derogations: “legitimate specific interests of the data subjects”; “legitimate prevailing interests, especially important public interests” and “the third State or receiving international body [providing] safeguards which are deemed adequate by the Member States concerned according to its national laws” (Art. 13(3)). All of these criteria leave a huge margin of appreciation to governments, in particular because the criteria according to which the adequacy of safeguards will be assessed remain quite vague (Art. 13(4)).

3 The Lisbon change

With the Lisbon Treaty, which was signed on 13 December 2007, and entered into force in December 2009, a stronger basis was created for the development of a clearer and more effective data protection system. Two sets of reforms may have a major impact on data protection in the area of freedom, security and justice: (i) the strengthened recognition of the right to data protection, and (ii) the different distribution of decision-making powers.

1. The new Treaty on the Functioning of the European Union (TFEU) provides for a general provision on data protection: Art. 16 TFEU. In fact, this article goes far beyond the simple rewording of Art. 286 TEC, it also states that “everyone has the right to the protection of personal data concerning them” (Art. 16(1) TFEU). Furthermore, it indicates the use of the “ordinary legislative procedure” in laying down rules on the protection of personal data processed, among others, by member states “when carrying out activities which fall within the scope of Union law, and the rules relating the free movement of such data” (Art. 16(2) TFEU). That Art. 16 TFEU is a new and still ambiguous component of the European Union data protection regime is well illustrated by looking at the two articles by Hilde Hjelm and Diana Alonso Blas in this issue. While Hjelm sees room for interpretation that Art. 16 TFEU could envisage one comprehensive legal data protection instrument for the area of freedom, security and justice, Alonso Blas outlines elements of the Lisbon Treaty that point to a tailor-made legal framework in the former third pillar sector.

Finally the ‘constitutional’ need for rules on data protection and for their independent supervision is enshrined in primary law not only in relation to personal data processed by European Union institutions, but also such data processed by member states. Such a strengthening of the recognition of the right of data protection is fostered also by Article 6 of the new Treaty of the European Union (TEU-L). It recognises the rights and freedoms set out in the Charter of Fundamental Rights of the

Springer
European Union (Art. 6 TEU-L) and provides for accession of the Union to the European Convention for the Protection of Human Rights and Fundamental Freedoms (Art. 6 TEU-L).

2. The second set of reforms provides for a different distribution of decision-making powers. Given the trans-pillar nature of the area of freedom, security and justice and its policies, the collapse of the pillar structure, with the inclusion of Title V on the area of freedom, security and justice in the TFEU (Arts. 67–89 TFEU), is a major development in the field. Title V incorporates also third-pillar policies such as a police cooperation (Arts. 87–89 TFEU) and judicial cooperation in criminal matters (Arts. 82–86 TFEU) where data exchange is a main issue.\(^{15}\) Furthermore, as is the case in Art. 16(2) TEU-L, the “ordinary legislative procedure” generally applies.\(^{16}\) Its impact on data protection in the area of freedom, security and justice is considerable: on the one side, it gives the European Parliament more powers than mere consultation on third pillar policies, and on the other, it may limit the “race to the lowest common denominator” by introducing qualified majority voting in the Council. Given the increasing “internationalisation” of data access and flows, and the relevance of international agreements on anti-terrorism and police cooperation, the introduction of the “ordinary legislative procedure” will have a major impact on the area of freedom, security and justice data protection because it guarantees, on the basis of Art. 218(5)(v), the need for the European Parliament’s consent in the conclusion of international agreements.

Beyond the foregoing, the above-mentioned changes brought by the Lisbon Treaty are decisive not only for the field of data protection but for the whole area of police and judicial cooperation in criminal matters as is illustrated with respect to the area of police cooperation in Michael Niemeier’s article in this issue. Further novelties for police cooperation in the European Union outlined in his article include the introduction of the COSI (“Comité de sécurité intérieur”), Europol’s new legal basis, ideas regarding the architecture of information exchange, and strategic considerations concerning the external dimension of the European Union’s internal security.

4 After Lisbon, some open questions

We saw earlier that the Data Protection Framework Decision can hardly be said to be completely satisfactory: the presence of too many flaws risks prejudicing its purpose of providing a “high level of protection of the fundamental rights and freedoms of natural persons” (Art. 1(1)DPFD). Instead of bringing simplicity, it appears to foster complexity in the AFJS data protection puzzle. Moreover, it neither adequately addresses new technologies, nor offers solid ground to ensure data protection in data

---

\(^{15}\) Chapter 5 Police cooperation of the Title V TFEU explicitly indicates the “collection, storage, processing analysis and exchange of relevant information” among the main measures of police cooperation between Member States’ competent authorities (Art. 87(2)(a)) and the main tasks of Europol (Art. 88(2)(a)).

\(^{16}\) Concerning the extension of the “ordinary legislative procedure” under Title V TFEU, cf. Chap. 2 Policies on Border Checks, Asylum, and Immigration: Art. 77(2), 78(2) and 79(2); Chap. 3 Judicial Cooperation in Civil Matters: Art. 83(2); Chap. 4 Judicial Cooperation in Criminal Matters: Art. 82(2), 83(1) and 84; Chap. 5 Police Cooperation Arts. 87(2) and 88(2).
flows towards third countries. Finally, the inclusion of Art. 1(4) on "essential national security interests and specific intelligence activities" poses a question mark over its utility.\textsuperscript{17}

On the contrary, the Lisbon Treaty offers very positive, and needed, inputs and stimuli for the AFSJ data protection system. However, its main impact is "derivative", and its simple entry into force does not modify the entire picture in one swoop as there will still be the need to amend or modify the Data Protection Directive and to repeal the Data Protection Framework Decision.

The 'transatlantic' question also remains. Can Europe define its own policy regarding data protection without a dialogue with the United States? Doubts are raised by Franziska Boehm in her article in this issue where she considers the European Union-PNR proposal\textsuperscript{18} to be strongly influenced by American and Canadian security policy instruments, to violate European data protection standards such as Art. 8 of the European Convention on Human Rights. However, on a more positive note, she also welcomes the European Parliament's new powers of co-decision under the Lisbon Treaty as an opportunity to further assure the right to data protection in the European Union.

A High Level Contact Group was set up to develop a common ground between the two parties. The Contact Group's work finished formally last November, with its final report and some amendments published later being the main outcomes. Given that the High Level Contact Group was not a formal diplomatic forum, but rather an informal working group, its conclusions are not binding, and moreover, official work is still needed to formulate a real draft agreement. (Its work has mainly amounted to the creation of a sort of dictionary between privacy in United States terms and privacy in the European Union, and vice versa). The question is whether a more formal US-EU Agreement will ever see the light of day and, if so, whether it will be legally binding. Doubt is expressed by Hilke Hijmans in his article in this issue in which he wonders how the controversial issue of guaranteeing redress in United States data protection laws can be solved.

A second, twofold set of issues is the interlinking of an eventual EU-US data protection agreement with the already extant EU-US agreements (concerning PNR, SWIFT, EUROPOL and EUROJUST) and with other international agreements. In fact, similar security measures are proliferating around the world (cf. the PNR agreements with Canada and Australia, the Electronic System of Travel Authorisation in United States and Australia; the widespread of biometrics included in identity cards and so on) and these measures are also transnational in nature.\textsuperscript{19}

---

\textsuperscript{17}Art. 1(4) of the Data Protection Framework Decision states: "[t]his Framework Decision is without prejudice to essential national security interests and specific intelligence activities in the field of national security".

\textsuperscript{18}Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, COM (2007) 654, 6 November 2007.

\textsuperscript{19}These issues will be dealt with in the Academy of European Law Trier seminar Data Protection in the Age of SWIFT, PNR, PRÜM and E-Justice, to be held in Trier on 31 May—1 June 2010, 310D62.
5 The Stockholm Programme and Action Plan

Finally, the newly adopted Stockholm Programme, the five year roadmap for the area of freedom, security and justice for the period 2010–2014, as well as its implementing Action Plan will put the first flesh on the bones of the Lisbon Treaty.

The Stockholm Programme calls for a comprehensive strategy to protect citizens’ data within the European Union and in its relations with other countries and asks the Commission, amongst others, to

- evaluate the functioning of the various instruments which form the basis for the data protection regime in the European Union (first pillar and third pillar) and present, where necessary, further legislative and non-legislative initiatives to maintain the effective application of the above principles,
- propose a Recommendation for the negotiation of a data protection and data sharing agreement with the United States of America, based on the work carried out by the EU-US High Level Contact Group on data protection and data sharing,
- consider a legal instrument laying down the data protection principles regarding the transfer of privately held data to third states for law enforcement purposes,
- improve compliance with the principles of data protection through the development of appropriate new technologies, based on greater public/private sector cooperation, particularly in the field of research,
- examine the introduction of a European certification scheme for “privacy-aware” technologies, products and services,
- conduct information campaigns, in particular to raise awareness among the public.”

Finally, in the Annex to the recently published Action Plan implementing the Stockholm Programme, the Commission is asked to issue a comprehensive new legal framework for data protection by 2010.

---
