Working Paper
Research Unit EU Integration
Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

Marie McGinley and Roderick Parkes

Data Protection at the EU Level: A Stocktaking of the Current State of Affairs

Ludwigkirchplatz 3–4
10719 Berlin
Phone +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

Working Paper FG 1, 2007/ 03, May 2007
SWP Berlin

Overview

Under the German EU-Presidency (first semester of 2007), the EU's agenda on safeguarding individuals' rights as regards the collection and exchange of their personal data has appeared somewhat contradictory and even self-defeating. On the one hand, the Presidency has taken forward, albeit without much elan, efforts to introduce a framework decision on protection standards for data collated and exchanged for reasons of combating criminality and terrorism under the Third Pillar of the EU – a move predicated by many upon the need to bring a degree of uniformity to this area. On the other, it has sought to upload to the EU-level the so-called Pruem Convention along with its attendant data-protection standards. The Pruem Convention is an initative concluded by a small number of EU member states with the aim of facilitating the transnational exchange of data for reaons of combating criminality and terrorism. Its transplantation to the EU-level would further fracture the data-protection landscape, militating against a key rationale behind the Framework Decision. Further, recent analysis shows that both these measures bear serious lacunae in terms of the data-protection standards they propose.

Against this background, the present paper maps out the current state of data protection at the EU-level. It argues that the uneven and patchy protection offered by the EU is unsatisfactory for two reasons: Firstly, and most obviously, this state of affairs spawns dangers for individuals' liberties and right to privacy. Secondly, far from standing in a zero-sum relationship to the EU's commercial and internal security aims, the imposition of robust, common data-protection standards can actually facilitate them; these benefits are scarcely harnessed in the current data-protection regime.

This second point is frequently overlooked and even misrepresented in the political debate about data protection. In particular, data-protection rights are often perceived as a hindrance to the effective provision of internal security, with concerns that security agencies have to jump through additional hoops before being able to act. Yet, the harmonisation of EU standards might facilitate data exchange between national and European security agencies currently undermined by the diverse data-protection regimes to which these agencies are bound. Similarly, by strictly regulating the circumstances under which data can be exchanged with other EU and extra-EU agencies, as well as the use that can be made of them by these other actors, security agencies lose their power to decide *ad hoc* whether to hand over data – a power which they may interpret 'over cautiously'. Meanwhile, by giving 'data subjects' the right to inquire and check the veracity of the information held on them, security agencies can introduce a means of ensuring the accuracy of data exchanged.

This paper looks at the current state of data protection from this perspective, examining: the degree of uniformity of protection standards between and within the First and Third Pillars; the standards under which data can be transferred between EU and extra-EU agencies; the use that can be made of data transferred between EU agencies; the data-subject's power to check the accuracy of the information held by EU agencies; the robustness of the independent supervision of these standards. It argues that by maintaining its uneven, and faulty, protection standards, the EU is failing to take advantage of these potential benefits for the liberties of individuals and the effectiveness of internal-security measures.

1. Data Protection in the First Pillar: The Data Protection Directive

1.1 Early Data Protection in the EC and the adoption of the Data Protection Directive

Today's efforts to regulate data protection under the Third Pillar of the EU can in no little part be traced to earlier attempts to manage data collection for commercial rather than security purposes, and thus to developments in the now First Pillar. The progress of these early efforts to boost data protection was, however, anything but smooth. Even before 1975, and the EP's first Resolution on the subject, the Commission had dealt with the issue of commercial data collection and exchange; yet, it failed to address the risks to the individual posed by exchanging and processing data. It focused instead on the economic potential contained in collecting and processing data, with a view to completing the internal market. Data protection standards were viewed by some at the national and European levels as imposing unnecessary restrictions on economic imperatives.

In 1979, the EP again passed a resolution, with specific recommendations to the Commission and a renewed call for legislation aimed at protecting the individual. At a time when many member states had already adopted data-protection laws in a purely domestic context, the EP was also aiming at the creation of a system of harmonised rules so that legislation in different member states would not conflict.[1] This did not receive much support, with the Commission pointing out that the Council of Europe was at the time drafting a convention on data protection. The Commission did however advise member states to ratify the Convention.[2]

The Commission finally recognised data protection as a Community responsibility in 1990, when it presented a proposal for a directive on data protection.[3] In this, the Commission did indeed recognise the potential commercial benefits of harmonising data protection: the Commission thus sought to harmonise individual state regulations on data protection in order to overcome barriers to creating the internal market in accordance with Article 100a of the Treaty establishing the European Communities (TEC). Yet, even then, there was an apparent concern that harmonising data protection standards in line with the privacy and human rights concerns advocated by the Parliament could prove obstructive to the realisation of commercial priorities.

It was at this time, though, that events conspired to add weight to the Parliament's agenda: The process of European integration had shifted increasingly towards areas of 'high politics'.[4] This raised the issue of what protection the EU was offering its citizens at a time when the EU was dealing with policies of core importance to individuals' human rights. The EU's growing propensity to comment on the human rights standards in place in third countries also opened its own provisions up to scrutiny.

This dual pressure – the human rights agenda put forward by the European Parliament and the commercial agenda advocated by the Commission – in favour of common standards for the protection of commercial data culminated in the 1995 Directive EC 95/46 of the EP 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" within the European Communities. The Directive applies to activities in the EU member states regulated by Community legislation, as well as the institutions and organisations of the European Communities.

The Directive may be seen as relatively successful in combining these twin agendas. In the Preamble, the intention is clearly stated that any harmonisation of laws related to data processing must not lead to a lessening of the protection currently afforded. Furthermore, member states are obliged to seek to ensure a high level of protection in the Community.[5] While the Preamble does not constitute a legally binding part of the Directive, the body of

[1] EP Resolution of 8 May 1979 OJ 1 EC Nr. C 140 of 5.6.1979, 34.
[2] Commission Recommendation, of 29 July 1981 on a Council of Europe convention for the protection of individuals in relation to automatic processing of personal data, OJ EC Nr. L 246 of 29.8.1981.
[3] Commission Communication on the protection of Individuals in relation to the processing of personal data in the community and information security of 13 September 1990, COM (90) 314 final.
[4] Kübler, p. 24.
[5] Preamble, point 10

the text also contains detailed provisions on the rights of the data subject. The text and its daily implementation provide proof that, at the very least, human rights protection does not necessarily undermine measures aiming at practical and operational effectiveness.

All the same, the text could have gone even further towards satisfying the twin pressures that drove its development. The Directive is understandably wrought with the evidence of the compromises and political battles that characterised its adoption. Implementation of the Directive is, for example, complex as the measure does not completely harmonise data protection in the First Pillar, but leaves some little scope for member states to apply specific standards. It also contains a number of vague definitions.

The defining characteristics of the Directive are set out in more detail below; however, it is worth pointing out at this stage that an evaluation of these characteristics remains difficult: Several member states were slow to transpose the provisions of the Directive into national legislation and did not adhere to the deadline specified (end of 1998). As a result, the Commission launched infringement proceedings before the ECJ against France, Germany, Ireland, Luxemburg and the Netherlands in December 1999. These cases have since been resolved; however the fact that member states only began to notify the Commission of legislative measures taken to transpose the Directive into national law in 2001 and 2002 (and in some cases even later) means that experience in implementing the Directive's provisions is limited, making it difficult to assess its value.[6]

1.2 Data use

The principles contained in the Directive reflect and expand upon the Council of Europe's 1981 "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data" – the so-called 108 Convention. However, one of the main differences between the Data Protection Directive and the 108 Convention is that the collection of data is required to have a "specified, explicit and legitimate" purpose.[7] Like the 108 Convention, the Directive stipulates that personal data must be processed fairly and lawfully. The principle of proportionality of data usage is enshrined in Article 6 (1c) and taken almost word for word from the 108 Convention, which states that data may only be collected and further processed if they are "adequate, relevant and not excessive". In addition, Article 8 sets out rules governing the legitimacy of processing data and Article 9 deals with the processing of sensitive data.[8]

1.3 The Rights of the Data Subject

Article 12 guarantees every data subject the right of access to his personal data, including the right to know whether or not data relating to him is currently being processed, as well as the purpose for which it is being processed. This encompasses the right to have data rectified, blocked or deleted if it is found to be inaccurate or contrary to the provisions of the Directive. Under Article 14, the data subject has the right to object to the use of his data "on compelling legitimate grounds relating to his particular situation"[9] unless there are other provisions in national legislation. The data subject can also object to the use of this data if it is to be processed for the purpose of direct marketing. Member states are obliged to make sure that data subjects are aware of the existence of this right.[10]

Many of these rights are, however, subject to restriction on seven grounds listed in Article 13. These include reasons of: national security; defence; public security; preventing, investigating, detecting or prosecuting criminal offences.[11] In cases where Article 13 applies, the supervisory authority of the member state concerned is nevertheless obliged to hear claims for checks on the lawfulness of data processing lodged by any data subject.[12] The Article remains problematic though: Article 13 may, for example, be justly criticised for

---

[6] Report from the Commission, First Report on the implementation of the Data Protection Directive (95/46/EC, COM(2003) 265 final,) Brussels, 15.5.2003,
[7] Article 6 (b)
[8] i.e. data which would reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership or any data pertaining to health or sex life (Article 9 (1)).
[9] (Article 14 (a))
[10] Article 14 (b) second subparagraph
[11] Article 13 (1) points a – g
[12] Article 28 (4) para. 2

being vaguely worded. More fundamentally, with the exception of point e, which states that a restriction can be imposed to safeguard "an important economic or financial interest of a member state or of the European Union", the listed grounds for restriction relate to areas which have subsequently proved of high salience given the EU's growing competencies in areas of internal security.

1.4 Independent Supervision

National Supervisory Authorities

Article 28 of the Data Protection Directive provides for the establishment of independent, domestic public authorities, which are to be responsible for monitoring the Directive's application in their respective territories. They are to be consulted when measures of relevance to data protection are being drawn up. All of the EU member states now have such an authority, headed by a data-protection commissioner.[13]

Individuals who feel that their fundamental rights have been violated with regard to the processing of their personal data can lodge a complaint with their national supervisory authority. The supervisory authorities have investigative competence, as well as the power to intervene in legal proceedings. Decisions taken by them can be appealed against in the courts.

The Article 29 Data Protection Working Party

The 1995 Data Protection Directive also provides for an independent advisory body ("Working Party on the Protection of Individuals with Regard to the Processing of Personal Data"), which was duly established on the basis of Article 29 of the Directive.

The Working Party consists of a representative from the designated supervisory authority of each member state. It further includes a representative from the supervisory authority established for the Community institutions and bodies, as well as a representative from the Commission. The Working Party elects its own chairman for a period of office of two years, subject to renewal.

The Working Party's tasks consist of promoting a uniform application at the national level of the measures outlined in the Data Protection Directive as well as of informing the Commission of any discrepancies between data protection in the Community and the relevant laws and practices of member states. It gives the Commission an opinion on the level of protection both in the Community and in third countries and advises the Commission should an amendment of the Data Protection Directive be on the table. Similarly, it advises the Commission on any other measures aimed at safeguarding the rights and freedoms of individuals within the context of processing personal data.[14]

In addition, the Working Party is entitled to make recommendations on all matters relevant to data protection in the Community, which are then forwarded to the Commission and the Article 31 Committee, which is composed of representatives from the member states and a representative from the Commission.

The European Data Protection Supervisor and Data Protection Officers

Article 286 of the EC Treaty, adopted in 1997 as part of the Treaty of Amsterdam, provides for the establishment of an independent supervisory body responsible for monitoring the application of Community acts relating to the protection of personal data in the Community institutions and bodies.

These provisions were taken over in Regulation (EC) No. 45/2001 of the EP and Council on the protection of individuals with regard to the processing of personal data. The Regulation generally follows the substance of the Data Protection Directive with a separate chapter on protection of personal data and privacy in the framework of internal telecommunications networks.

[13] Similar authorities also exist in the EFTA countries, as well as candidate states for accession to the EU. A list of these authorities can be retrieved at: http://ec.europa.eu/justice_home/fsj/privacy/nationalcomm/index_en.htm
[14] Article 30

The Regulation specifically provides for an independent supervisory authority at Community level ("European Data Protection Supervisor" – EDPS) and sets out his tasks and powers. The EDPS and an assistant EDPS were appointed in January 2004 after the decision of the EP and Council of 22 December 2003.[15] Currently, the EDPS is Peter Hustinx, former President of the Dutch national data-protection authority and former Chairman of the Article 29 Working Party (1996 – 2000).

The EDPS and his Assistant are appointed for a period of office of five years, which can be renewed by common accord of the EP and Council on the basis of a list of candidates drawn up by the Commission.[16] According to Article 41 of this Regulation, the mandate of the EDPS is to ensure the respect of fundamental rights with regard to the processing of personal data within the context of Community institutions and bodies.

The duties of the EDPS are outlined in Article 46 of the Regulation and are essentially the same as those of the national supervisory authorities. Just as national authorities enjoy the power to intervene in domestic court proceedings, the EDPS enjoys an equivalent right to intervene before the ECJ when data-protection issues are involved. The EDPS made use of this right for the first time when he intervened in two cases in support of EP conclusions regarding the transfer of passenger name records (PNR) to the United States by providing written and oral statements.

In addition, the EDPS advises Community institutions on new legislation relevant to data protection. The Commission is obliged to cooperate with the EDSP by providing relevant information, consulting the Supervisor when adopting a relevant legislative proposal (including any measures which are intended to be implemented at the national level). The EDPS also monitors developments which could be relevant to data protection, including those occurring outside of the First Pillar.[17]

Like the national supervisory authorities, the EDPS is authorised to carry out prior checks on data-processing operations deemed to pose a risk to the rights of data subjects due to their scope or purposes. Such processing operations can, for example, involve data relating to health and to suspected offences, criminal convictions or security measures.[18] The EDPS cooperates with national supervisory authorities, including in matters related to the Third Pillar in order to improve the consistency in protecting personal data.[19]

Another important aspect of the regulation is the obligation for Community institutions and bodies to appoint at least one Data Protection Officer (DPO), who works independently and is responsible for ensuring the provisions of the regulation are applied within the respective institution or body. All institutions and some of the Community bodies have now appointed DPOs, some of whom took up their work even before the EDPS and his assistant were appointed. The rationale behind the appointment of the DPOs is that they should form a network internal to the Community institutions and bodies and linked by a common obligation to cooperate with the EDPS.

1.5 Protection of data communicated to third parties under the First Pillar

The Data Protection Directive contains strict rules governing the transmission of data to third countries.[20] The adequacy of data protection standards in third countries requesting data is assessed considering all the circumstances surrounding the transfer operation, including the rules of law in force in the third country and the professional rules and security measures which are complied with in that country.[21] Member states and the Commission are obliged to keep each other informed of cases of third countries which do not provide adequate standards of data protection.

---

[15] Decision 2004/55/EC of the European Parliament and of the Council of 22 December 2003 appointing the independent supervisory body provided for in Article 286 of the EC Treaty (European Data Protection Supervisor).
[16] Article 42 (1), regulation 45/2001
[17] Peter J. Hustinx, "The European Data Protection Supervisor after two years" in: *DANA – Datenschutz Nachrichten 1/2006*, p. 4 – 6.
[18] Article 27
[19] Hustinx [as in footnote 17], p. 3.
[20] Article 25 (1). See also Steve Peers, "Human Rights and the Third Pillar", in: Philip Alston (ed.), *The EU and Human Rights*, Oxford 1999, p. 182.
[21] Article 25 (2)

Article 26 does, however, allow for derogations from these principles in certain circumstances, the definition of the circumstances being rather vague. For example, if "the transfer is necessary or legally required on important public interest grounds ...".[22]

The transfer of data to third countries is an area in which the Commission has identified significant divergences in member states' implementation.[23] On the one hand, some member states tend to be very lax in transferring data to third parties, with insufficient assessments of the adequacy of data protection and only submitting it to very limited control by the state and national supervisory authorities, thus violating Article 25 (1) of the Directive. This state of affairs poses a risk to all of the member states, in that the free flow of personal data is guaranteed by the Directive and so third states will be more inclined to approach the member state with the most lax provisions on data transfer, thus weakening the standard of protection for the Union as a whole. In addition, the Commission found that the number of authorisations for transfers reported by national supervisory authorities (as required under Article 26 (2)) to be "derisory by comparison with what might reasonably be expected", suggesting the possibility that illegal (i.e. without adequate protection standards) transfers are taking place. On the other hand, other member states were found to be over stringent and unnecessarily hampering the flow of data, by submitting all transfers to administrative authorisation, even in cases where the adequacy of protection standards has been established (for example, through binding Commission decisions, or because the transfer qualifies as one of the exceptions listed in Article 26). These cases again show the effect of the member states' slow and divergent implementation of the Directive on data protection and the need for mechanisms to ensure their enforcement.

[22] Article 26(1d)
[23] As described in its implementation report.

2. Data Protection in the Third Pillar

2.1 Exploiting the benefits of robust common standards?

It was argued above that, just as the imposition of robust, common data-protection standards can be beneficial to the commercial aims of the EU, so too it can facilitate the provision of internal security. Such standards can facilitate data exchange for purposes of combating crime and terrorism, as well as creating mechanisms to ensure the accuracy of these data. A generous analysis of the data-protection standards in place would come to the conclusion that their architects were unaware of these benefits; a less generous one would identify the marks of security officials' desire to retain the operational autonomy that robust standards would restrict, even at the cost of the effectiveness of their work.

The above data-protection standards apply to the EC-, or 'First', Pillar of the EU only. EU cooperation for the purposes of combating crime and terrorism has developed largely outside the formal Community framework and was only later drawn into the mainstream process of European integration, through the framework of the Third Pillar. This Third Pillar cooperation is subject to data-protection standards different from those of the First Pillar. Yet, the fight against terrorism is a 'cross-cutting' aim, requiring coordination between different policy areas and actors; thus many policies relevant for counterterrorism cooperation are dealt with under the First Pillar. Moreover, some of the areas of cooperation – notably immigration and asylum policy – formerly dealt with under the Third Pillar have indeed been transferred into the First Pillar (although they remain subject to anomalous rules regarding judicial and/or parliamentary oversight).

Moreover, several different data-protection regimes actually exist alongside each other in the Third Pillar. Standards differ between the central units established between the member states to enhance cooperation between law enforcement agencies investigating and prosecuting organised and cross-border crime (Europol, Eurojust). Different standards apply to databases to identify asylum applicants and illegal immigrants through a system for comparing fingerprints (Eurodac), maintain and distribute information related to border control and law enforcement (Schengen Information System - SIS), exchange visa data (Visa Information System – VIS) and customs related information to enhance cooperation between member state authorities in order to combat cross-border crime (Customs Information System – CIS).

That all of these bodies and systems have their own provisions regarding data protection raises the question of how transparency and the respect of these varying standards can be guaranteed. It also means that a data subject may be treated differently (in terms of access to data, right of redress etc) depending on the body that happens to have collected and stored his data and perhaps transferred them to another body or authority.[24]

2.2 Data use

Eurojust[25], the SIS and Europol have no explicit provisions for data quality. The text establishing Eurojust[26] and the Schengen Agreement[27] specify what kind of data may be processed. The Schengen Agreement also contains a list of the types of personal data which may be stored[28] Eurojust permits the processing of sensitive data when such data are necessary for the national investigations concerned as well as for coordination within Eurojust. However, in this case the DPO must be informed.[29]

The Schengen agreement stipulates that the SIS may only contain data for the purposes outlined in Articles 95 – 100. The decision on "whether the importance of the case warrants

[24] For example, the Council adopted a recommendation on hooliganism which aims to ensure that stadium exclusions imposed in one member state are mutually recognised by other member states. There are, however, no provisions for challenging this mutual recognition. See Peers [as in footnote 20], pp. 177.
[25] Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (2002/187/JHA) Hereafter: Eurojust decision.
[26] Article 15, Eurojust decision.
[27] Title 4 Chapter 2, Article 94, Schengen agreement
[28] Article 94 (3)
[29] Article 15 (4) Eurojust decision

the inclusion of the report in the Schengen Information System", however, rests with the contracting party.[30]

The Europol Convention merely states that data can be used "in order to prevent and combat crimes falling within the competence of Europol and to combat other serious forms of crime"[31]. The data may be used by Europol only when it is completing its tasks as outlined in Article 3.

2.3 Rights of the data subject

Article 19 of the Eurojust Decision lays down the data subject's right of access to personal data and states that an individual wishing to exercise this right may do so in a member state of the data subject's choice.[32] The member state authority must then refer the matter to Eurojust. Although the decision to grant or deny access rests initially with the member states concerned, should they be unable to reach agreement, the matter is referred to the Eurojust College, which reaches a decision on the basis of a two thirds majority. The College consists of the national members, who each have one vote.

The Eurojust decision also sets out specific grounds upon which access to personal data shall be denied: if such access may jeopardise one of Eurojust's activities, any national investigation which Eurojust is assisting, or the rights and freedoms of third parties. [33]

Article 109 of the Schengen Agreement lays down that the data subject's right of access is governed by the law of the contracting state in which he invokes this prerogative. Article 114 (2) grants data subjects the right to request a check on their data and on the purpose for its being held. The decision on whether or not information is subsequently provided, as well as the procedures followed, can be determined by the national supervisory authority of the contracting party in question, if this is in line with national legislation. The information can be refused if this would undermine the performance of the legal task specified in the relevant report, or in order to protect the rights and freedoms of other individuals. Communication of information is also refused during the period of reporting "for the purposes of discreet surveillance".[34]

The Europol Convention affirms the data subject's right to access personal data in Article 19. This right may be exercised in a member state of the data subject's choice and is in accordance with the law of the member state where the right is claimed. Reasons for denying access are similar to those outlined in the Eurojust decision. Under the Europol Convention access can also be denied in order to "protect security and public order in the Member States" or "to prevent crime".[35]

Eurojust[36], Europol[37] and the Schengen Agreement[38] all have provisions for correcting, deleting or blocking data which is found to be inaccurate or where storage is contrary to the provisions in the respective agreements. This includes the right of a data subject to request such action. In addition, Article 116 of the Schengen Agreement details the member states' responsibilities with regard to any injuries caused to an individual through the use of their national data file in the SIS. This is also the case if the contracting party included legally or factually inaccurate information. Article 118 sets out safeguards which the contracting pasrties are obliged to provide.

Eurojust and Europol are obliged to amend data that is found to be inaccurate in collaboration with the affected member state. The above-mentioned agreements also provide

---

[30] Article 94 (1)
[31] Article 17, Europol Convention
[32] In addition, to these provisions, the College of Eurojust has adopted Rules of Procedure on the processing and protection of personal data at Eurojust. Article 4 of the rules of procedure clearly expresses Eurojust's commitment to act in respect of fundamental rights with particular regard to the right to privacy and data protection. Furthermore, it underlines the principle of purpose limitation (Article 15), the rights of data subjects (Articles 8 and 9) and stipulates that data processing must take place with respect to the principles of lawfulness and fairness, proportionality and necessity of processing (Article 5).
[33] Article 19 (4)
[34] Article 109 (2)
[35] Article 19 (3.2)
[36] Article 20
[37] Article 20
[38] Articles 110 and 111

for time limits in the storage of data. Both the Eurojust decision and Europol Convention contain provisions that personal data processed by these bodies may be stored only as long as is necessary to perform the tasks for which they were transmitted. They also stipulate that a review of the need to store data is carried out every three years.

Data stored in the SIS for the purposes of locating persons may be retained only for as long as is necessary to achieve the purpose for which they were supplied. Their need to be retained is reviewed at least every three years.[39] However, this review is carried out by the contracting party and not by an independent authority. Contracting parties can extend the period of data retention within the review period if this is necessary for the reason for which the data was originally stored. Any extension must be communicated to the technical support function.[40]

In the case of data held for the purposes outlined in Article 99, in other words, data stored for the purposes of prosecuting criminal offences and for the prevention of threats to public safety, a review is carried out every year. Contracting parties can also set shorter review periods, if this is in accordance with their national legislation.[41] Any other data may be retained for a maximum period of ten years.

In addition, data which are 'deleted' are still retained for one year in the technical support function. However this data may be consulted only for the purposes of subsequently checking their accuracy. Afterwards they must be destroyed.[42]

2.4 Independent supervision

Eurojust is subject both to internal supervision, through the provision of a DPO,[43] and external supervision through the joint supervisory body.[44] An individual can appeal a Eurojust decision before a joint supervisory body[45] regarding for example the correction, blocking and deletion of personal data.[46]

The Europol Convention also has a common supervisory body, with representatives from the national supervisory authorities.[47] Individuals can appeal Europol decisions to this body; however no provisions are made for internal supervision. Similarly, Article 115 of the Schengen agreement provides for a joint supervisory authority, which consists of two representatives from each of the national supervisory authorities from the contracting parties. It also has access to the technical support function in order to check that the provisions of the agreement are being implemented.[48]

2.5 Protection of data communicated to third parties under the third pillar

Provisions in the Europol Convention, and in particular those in the Council Act of 12 March 1999 adopting the rules governing the transmission of personal data by Europol to third States and third bodies, have been criticised for being too vague and thus not providing sufficient safeguards for the data subject.[49] Although there are provisions for a clear purpose limitation[50], an obligation to correct and erase false data[51] and even a prohibition of

---

[39] Article 112 (1). There is an additional review mechanism in Article 103 that each contracting party shall ensure that, on average, every tenth transmission of personal data is recorded in the national section of the SIS by the data file managing authority for the purposes of checking the admissibility of searching. The recording may be used only for this purpose and must be deleted after six months.
[40] Article 112 (4)
[41] Article 112 (2)
[42] Article 113 (4)
[43] Article 17
[44] Article 19 (8)
[45] In order to create the Joint Supervisory Body, member states each appointed a judge from their country, who was not already a member of Eurojust for inclusion on a list of potential candidates to sit on the Joint Supervisory Body for a period of at least eighteen months. The Joint Supervisory Body consists of three permanent members and one or two *ad hoc* judges during the examination of an appeal. A judge appointed by a member state becomes a permanent member one year before his member state assumes the Presidency of the Council and remains a permanent member for eighteen months. The chairman of the body is the judge appointed by the member state holding the Presidency of the Council (Article 23, 2002/187/JHA).
[46] Article 20
[47] Article 23
[48] Article 115 (2)
[49] Simitis, p. 18.
[50] Article 6 (2)
[51] Article 7

communicating data to third parties,[52] there are at the same time facilities for the Director of Europol to decide to transfer data to third parties, if he feels this is "absolutely necessary".[53] This can occur under the condition that it is in the "fundamental interests" of member states or on the grounds of imminent "criminal danger". The decision on whether or not these abstract conditions have been fulfilled rests with internal decision-making within Europol.[54]

According to the Eurojust decision, communication of data to third parties is subject to the consent of the member state of origin, as well as an adequate level of data protection by the receiving state, if it is not party to the 108 convention.[55]

Any contracting state can, however, derogate from this provision if its aim in exchanging the data is "taking urgent measures to counter imminent serious danger threatening a person or public security".[56] In this case, for the data exchange to be authorised, the recipient must "give an undertaking that the data will be used only for the purpose for which it was communicated."

Access to the SIS is generally only granted to authorities responsible for border, police and customs checks, as well as those agencies coordinating these checks. The conditions under which this access is granted are governed by the national legislation in the contracting party. The contracting parties are obliged to submit a list of the competent authorities that are authorised to search the data contained in the SIS directly. The list must also state for which purposes the authorities may search the SIS. The conditions for granting access are outlined in Article 101.

[52] Article 5 (5)
[53] Article 2 (1b)
[54] Cited in Simitis, p. 19.
[55] Article 27 (4), Eurojust decision
[56] Article 27 (6), Eurojust decision

3. The data-protection challenge for the EU

Against the background of this bewildering array of procedures, mechanisms and standards in place in the Third Pillar – some of which show serious lacunae –, the efforts of the member states to reconfigure the data-protection standards for data used in combating crime and terrorism must be judged against the following criteria:

1. the compatibility of the Third Pillar standards they introduce with the standards already in place in the First Pillar. The recent ructions concerning the transfer to the US of 'passenger names records' (PNR) stored in the EU highlighted the difficulties arising from the existence of different standards for the First and Third Pillars: passenger data collected for commercial purposes under the scope of the Data Protection Directive were refused the protection it afforded because they were to be subsequently transferred as part of efforts dealt with under the Third Pillar.

2. the degree to which they introduce a harmonised framework for all the agencies and data systems housed within the framework of the Third Pillar, as well as for the relevant national bodies. The creation of a common data-protection framework can facilitate data-exchange between these agencies just as it played an important part in the development of the internal market; it also fosters transparency and a degree of certainty for data subjects.

3. the robustness of the standards introduced. Both the freedoms of individuals and the effectiveness of internal security measures can be strengthened by robust standards governing: the conditions under which data can be transferred; the subsequent use that can be made of that data; the data subject's power to check the veracity of the data transferred; the independent supervision of these standards.