CHALLENGE
Liberty & Security

Research Paper No. 9
May 2008

The Changing Landscape of European Liberty and Security

Taking Stock:
Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice

Florian Geyer

Abstract

Exchange of information in the Area of Freedom, Security and Justice, using new technologies like biometric identifiers and creating large-scale centralised EU databases is a highly topical, yet equally controversial issue. A number of EU databases and systems of information exchange are already in place, others will soon become operational. In spite of this, proposals for new measures and mechanisms are frequently tabled; it appears as if the EU is only at the beginning of a 'new age of information exchange'. This working paper aims at taking stock of this development by providing a comparative picture of the existing EU JHA databases and EU rules on information exchange, as well as some of the main related proposals. The paper also looks at how some databases are used in practice and puts forward some suggestions as to how to alleviate concern about data protection.

An Integrated Project Financed by
the Sixth EU Framework Programme

ISBN-13: 978-92-9079-789-0

Available for free downloading from the CEPS website (http://www.ceps.eu)

Contents

TAKING STOCK:

DATABASES AND SYSTEMS OF INFORMATION EXCHANGE IN THE AREA OF FREEDOM, SECURITY AND JUSTICE

FLORIAN GEYER*

In the policy area that deals with security, counter-terrorism and 'unprecedented threats' new ideas and proposals intending to allow public authorities to gather, store, process and exchange an increasing amount of personal data are being brought forward in high numbers and with increasing frequency. Not even three months had passed, for instance, since Commissioner Frattini's EU Passenger Name Record (PNR) proposal of November 2007[1] when in February 2008 he tabled another two other proposals directed at tracking and monitoring travellers entering the EU: 1) an 'entry-exit system' based on biometric identifiers and 2) a system that would oblige travellers to register online before actually departing to Europe (both part of the EU Commissions' so called 'border package').[2] Questioning the added-value, effectiveness and proportionality of these and many other similar measures is often the immediate reaction by parliamentarians, human rights groups, concerned citizens and sometimes even member state ministers.[3] "Do we really need yet another intrusive measure before we know if the last one we enacted does its job?", could be a typical reaction; a reaction whose underlying concerns should not be easily dismissed, not least because judicial courts also seem to be increasingly opposed to some of the advances in granting authorities more and more powers and means of surveillance.

In this regard it might be a mere coincidence – yet with symbolical value – that in the same period that the EU Commission presented its 'border package', arguing for more and even bigger databases on foreign travellers, Advocate General Maduro of the Court of Justice of the European Communities (ECJ), for instance, considered a large-scale national database that contains only extensive data on Union citizens (and third-country nationals), but not on its own nationals, as discriminatory and in breach of community law.[4] Member state courts have also been active in that period, in particular the German Constitutional Court. That Court, the *Bundesverfassungsgericht*, issued a series of decisions in February and March 2008 that

---

* Florian Geyer is a Research Fellow in the Justice and Home Affairs Unit of CEPS. This paper falls within the framework of CHALLENGE – *the Changing Landscape of European Liberty and Security*, a research project funded by the Sixth EU Framework Programme of DG Research, European Commission, see www.libertysecurity.org. The author would like to thank Daniel Gros, Elspeth Guild and Sergio Carrera for their valuable comments.

[1] Copying the US PNR programme, that had led to many bitter reactions among policy makers and the public during the German EU presidency of 2007. See Commission Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, COM(2007) 654 final, 6.11.2007.

[2] Commission Communication, Preparing the next steps in border management in the European Union, COM(2008) 69 final, 13.2.2008. For an analysis see Guild, Carrera & Geyer, *The Commission's new Border Package: Does it take us one step closer to 'Cyber Fortress Europe'?*, CEPS Policy Brief No. 154, Centre for European Policy Studies: Brussels, March 2008.

[3] Cf. the statements gathered by EurActiv, 'EU to tighten border controls, critics fear 'Fortress Europe'', 14.2.2008 (http://www.euractiv.com/en/justice/eu-tighten-border-controls-critics-fear-fortress-europe/article-170292, last accessed 2.4.2008).

[4] ECJ, Opinion of Advocate General P. Maduro in case C-524/06 (Huber), 3.4.2008.

considerably limited or altogether discarded some new data-sensitive security laws in Germany:[5] questions of legal certainty and precision, purpose limitation and proportionality were among those addressed by the Court.

It is the sheer number of proposals and enacted measures in this field that could give rise to concern, however. In fact, even for professional observers, it is difficult to even glimpse the 'security web' that is currently being spun at national, supranational and transatlantic levels alike. What databases and channels of information actually exist? What data is stored and for how long? Which states participate and which authorities take part in each system? What are the data protection provisions? But above all: how do all the measures taken together interact and how can this kind of virtual security architecture transform societies that claim to be liberal and democratic?

The Hague Programme's vision

At EU level, improving the exchange of information is one of the main elements of the "The Hague Programme", the multi-annual programme adopted by the European Council in November 2004. This political programme constitutes the 'guiding star' for policy-making in the area of freedom, security and justice for the period 2004-2009.[6] Under the headline "Strengthening Security", EU leaders expressed their conviction that an "innovative approach to the cross-border exchange of law-enforcement information" was needed. They stipulated that with effect from 1 January 2008 the newly coined "principle of availability" should be the governing standard for information flows throughout the Union. This principle entails fast and (more or less) direct access for any law enforcement officer to necessary information held in any other member state. Full use of new technologies should be made, in order to establish reciprocal access to national databases, interoperability as well as direct (online) access to existing central EU databases. Under this scenario, the creation of new centralised EU databases would only be of secondary importance.[7] The European Council also requested strict observance of six key conditions for the development of this innovative approach to the exchange of law-enforcement information:

- the exchange may only take place in order that legal tasks may be performed,
- the integrity of the data to be exchanged must be guaranteed,
- the need to protect sources of information and to secure the confidentiality of the data at all stages of the exchange, and subsequently,
- common standards for access to the data and common technical standards must be applied,

---

[5] On 27.2.2008 the *Bundesverfassungsgericht* declared unconstitutional the new law of Nordrhein-Westfalen that would have allowed secret spying of personal computers and internet usage (1 BvR 370/07, 27.2.2008); on 11.3.2008 it quashed new provisions in the police laws of Hessen and Schleswig Holstein, that would have allowed the automatic identification and storage of vehicle registration plates of private cars by video cameras without suspicion in order to compare the data with existing police databases (1 BvR 2074/05, 11.3.2008); finally, on that very same day, the Court temporarily suspended some aspects of the new federal law that intends to implement the EU data retention directive (1 BvR 256/08, 11.3.2008).

[6] The Hague Programme: strengthening freedom, security and justice in the European Union, OJ C 53, 3.3.2005, p. 1.

[7] "New centralised European databases should only be created on the basis of the studies that have shown their added value", see OJ C 53, 3.3.2005, point 2.1, p. 8.

- supervision of respect for data protection, and appropriate control prior to and after the exchange must be ensured,
- individuals must be protected from abuse of data and have the right to seek correction of incorrect data.[8]

Furthermore, as regards border control and migration issues, the European Council embraced "biometrics and information systems" (point 1.7.2. of the Hague Programme) as *the* solutions for the future and requested the Schengen Information System II as well as the new Visa Information System to be operational in 2007.

A common EU Policy on Information Sharing?

Improving the exchange of information in the field of Justice and Home Affairs (JHA) is an important issue, also for the EU Counter-terrorism Coordinator, Gilles de Kerchove. In a discussion paper on the implementation of the EU counter-terrorism strategy, he criticised the fact that the current structures in the Council, with its multitude of different working parties dealing with related files, tended to produce incoherent and sometimes illogical results (Counter-terrorism Coordinator, 2007, p. 3). He calls for the adoption of a "Common EU Policy on Information Sharing" that will build on the results of an assessment of the practical use of EU instruments related to information exchange. Furthermore, in order to ensure consistency and efficiency of the work carried out in the Council, he suggests mandating only one single Council Working Party/Committee to reflect on, prepare, develop and monitor the implementation of this policy.

The aim of this paper

This working paper strives to contribute to these developments and ongoing discussions by providing a comparative picture of the existing EU JHA databases and EU rules on information exchange, as well as some of the main related proposals.[9] In this respect it aims at updating the 1999 report of the House of Lords EU Select Committee on "European Union databases"; by sketching also EU rules on data exchange directly between law enforcement authorities of member states, however, it goes beyond that parliamentary inquiry. This stocktaking exercise is provided in tables. The main objective of the paper is therefore informative in nature.[10] Further studies are invited to build on the empirical material provided in the annexes. However, the paper also presents some findings that emerged in the preparation of the tables, in particular when taking account of the Hague Programme's plans of 2004 as compared to the situation as of April 2008.

The systems under scrutiny – 'first' and 'third pillar' issues

In the comparative tables in Annex 1, the Schengen Information Systems I and II (SIS I and SIS II), EURODAC, the Customs Information System (CIS), the Europol Computer System, the Eurojust files as well as the Visa Information System (VIS) are displayed in the first set of tables. These can be regarded as centralised EU systems. As regards mechanisms of direct

[8] Ibid.

[9] In order to limit the scope and to make this task feasible the paper restricts itself to those databases and rules that are intended to exchange personal, individualised data. Exchange of statistical data and similar general data is therefore not covered.

[10] In this regard it also intends to contribute to the research undertaken by the French team of the CHALLENGE research project, see e.g. Bonditti, 2007.

information exchange between law enforcement authorities (decentralised), fourteen texts had been examined, covering fields like DNA analysis results, football matches, terrorism, passport data, criminal records, money laundering, to name a few. Additionally, in this section the competing proposals on implementing the principle of availability are analysed. In the third set of tables, EU acts that provide common rules on the extraction of genuinely 'private' data are compared, i.e. data gathered by private parties for private purposes like telecommunication companies or airlines.

Although all these systems can be attributed to the area of freedom, security and justice (see Article 2 Treaty on European Union – TEU), they address substantially different issues: migration, asylum, free movement on the one hand and police and judicial cooperation in criminal matters, including counter-terrorism on the other. Making a distinction between these issues is not only mandatory in terms of content (e.g. the movement of persons across borders is *per se* neither a threat nor a crime), but also as regards the institutional EU order. While migration, asylum and free movement is located in the so called 'first pillar' of the European Union and subject (in principle) to the community method, police and judicial cooperation in criminal matters is part of the 'third', i.e. the intergovernmental pillar.[11] In contrast to the first, this third pillar does not entail proper involvement of EU institutions, but is regarded as an exclusive matter of member states. While this pillar duality would eventually be changed by the Lisbon Treaty[12], for the time being, it still governs the current setting of EU Justice and Home Affairs - with all its negative externalities (see Guild & Carrera, 2005).

Observations

Some observations are formulated in the following section that emanate from the work on the tables provided in the annexes.

Uneven participation of EU and non-EU member states: a new 'democratic deficit'?

Although the systems under scrutiny are essentially 'EU systems' not all EU member states participate, at the same time some non-EU states do take part. This is most obvious in the case of the current Schengen Information System (SIS). Iceland and Norway as non-EU states participate fully, while the EU states Cyprus, Romania and Bulgaria are not yet allowed to take part. On the other hand, the UK and Ireland, which do not participate in the Schengen free travel area, have received permission to be part of the police and criminal law contents of SIS. Practical issues, however, have so far prevented these states from actually getting connected to the SIS system (House of Lords, 2007, p. 11 and 14). Then there is Switzerland, and most recently Liechtenstein, that will soon be joining the system, again two non-EU states.

Were 'Schengen' a purely intergovernmental undertaking one would not necessarily be concerned by this situation: whoever is part of the Schengen free travel zone is also part of the Schengen Information System, as simple as that. Therefore Iceland, Norway and soon Switzerland and Liechtenstein are 'in' and the UK and Ireland are partially 'out'. However, since the incorporation of the Schengen *acquis* into the EU legal order (first and third pillar) with the Amsterdam Treaty, Schengen has eventually and undoubtedly become supranational in

[11] Furthermore, EU counter-terrorism efforts are sometimes located within the 'second pillar' as part of the EU's common foreign and security policy.

[12] For an assessment of the changes brought about by the Lisbon Treaty in the area of freedom, security and justice, see Carrera & Geyer, "The Reform Treaty and Justice and Home Affairs – Implications for the *common* Area of Freedom, Security and Justice", in Guild & Geyer (eds), *Security versus Justice? Police and Judicial Cooperation in the European Union*, Ashgate: Aldershot, 2008, pp. 289-307.

nature. Yet supranationality was the driving force for developing EU fundamental rights and for constantly adding more democratic elements into the constitutional setting of the Union. And here comes the problem: the Schengen framework is part of this setting but not all Schengen states are part of it. This entails for instance, that the Charter of EU Fundamental Rights – once binding with the Lisbon Treaty – will not govern the usage of the Schengen Information System by these four non-EU states.

Furthermore, there is the question of democratic accountability. The Schengen System is evolving and each substantive change to it needs a legislative act. The necessary legislation is already – at least as regards the first pillar – co-decided by the European Parliament (EP) and the Council (and with the Lisbon Treaty in force, co-decision issues will increase considerably).While non-EU Schengen states are involved in the Council proceedings via so called 'Mixed Committees', there are no Icelandic, Norwegian, Swiss or Liechtenstein parliamentarians involved when the EP decides on the acts. On the other side of this coin, attention must be given to the fact that the EU *non*-Schengen states the UK and Ireland do have 'their' Members of the European Parliament voting on Schengen immigration and border control matters although their governments are excluded from the Council vote, due to their non-participation.

These examples show that an uneven participation of EU states in supranational matters, leads to a whole series of contentious and complicated questions that can have negative effects on the institutional balance and the situation of the individual. In the area of freedom, security and justice, this fragmented participation is an even greater concern, not only due to the direct impact the policies have on each and every person, but also because the participation or non-participation of states is not even consistent. The databases and information systems in this area are a particularly good illustration of this: while the UK and Ireland are not participating in the migration and border control issues of SIS, they are part of the asylum database EURODAC, but not of the visa database VIS. In all of them, however, Iceland, Norway as well as Switzerland and Liechtenstein are participating, or will do so. As regards decentralised mechanisms of information exchange between law enforcement authorities, the latter participate only when the legislative act provides that "it constitutes a development of the provisions of the Schengen acquis". This has been established to be the case, e.g. in the third pillar framework decision on simplifying the exchange of information between law enforcement authorities, but not in almost all of the other mechanisms, however.

To establish which states are participating in which systems and mechanisms is consequently a rather unpredictable business. This unpredictability, however, might in itself lead to conflicts with yet another issue: that of data protection, since to know where personal data are stored and processed, by which authority and for what purposes is an essential part of data protection standards.[13]

Actual usage of the systems: under- and over-achievers?

Statistics showing the actual usage of the systems provide a mixed picture. While the SIS contains a total of around 22 million valid entries as of 1.1.2008, including objects and persons (Council, 2008, p. 1), the Customs Information System (CIS) as of 26.10.2006 featured only around 490 active cases with some member states having never entered any data and five member states being responsible for 95% of the entries (Council, 2007b, p. 4). As with SIS, CIS is also a cross-pillar database that contains entries on persons and objects alike: "CIS was created to store information on commodities, means of transport, persons and companies in order to assist in preventing, investigating and prosecuting actions which are in breach of

[13] See the recent Bundesverfassungsgericht judgement for instance, 1 BvR 2388/03, 10.3.2008.

customs and agricultural legislation (1st Pillar) or serious contraventions of national laws in the application of which the customs administrations have total or partial competence (3rd Pillar)" (Council, 2007b, p. 2).

Although one does expect that CIS is in fact 'smaller' as its focus is more limited than SIS, the huge discrepancy between entries in the two databases and the fact that only a handful of member states seem to be actually interested in the contents of CIS is nevertheless surprising. Even more so when considering that in an official leaflet on CIS it is stated that "each year throughout the EU, thousands of Customs officers are carrying out thousands of investigations on persons or companies suspected of being in breach of Customs, Agricultural or national legislations".[14] If this is the case, then it seems as if these "thousands of customs officers" are not too interested in sharing and receiving information from their counterparts in other EU member states.

Involved authorities: blurring boundaries and questions of control and 'value' of data

As stated above, the policies subsumed under the label 'area of freedom, security and justice' comprise a wide-ranging set of issues that need to be discerned. However, when looking at the authorities that have complete or partial access to the databases and systems of information exchange, it becomes obvious that the boundaries between these issues become increasingly blurred. In the case of SIS, this blurring is part of the system as it contains genuine law enforcement information (e.g. persons wanted for arrest) as well as genuine border control and immigration law information (e.g. banned third country nationals). Nevertheless, in an effort to uphold the boundary each member state has to declare which of its authorities has access to which set of SIS data.[15] Yet, in SIS and similarly in other databases and systems, these efforts might prove fruitless as member states are essentially free to designate their "competent authorities". They have to inform the Council Secretariat or the Commission about these competent authorities, but it does not appear as if any of the EU bodies has the power to reject a designation communicated by a member state.

In the case of Eurodac, for instance, data should only be entered and accessed by national authorities in charge of handling asylum requests. However, as the first coordinated inspection by data protection authorities has shown, in some member states Eurodac is operated partly or entirely by national police services (EDPS, 2007, p. 12). Although that report did not establish that Eurodac data had been actually searched for 'police purposes', it seems as if this is merely a matter of trust, not of possibilities. One might therefore wonder whether the intended proposal of granting law enforcement officers access to Eurodac would only formally allow what already takes place by the so-called 'normative power of the factual'. Furthermore, the VIS, the soon-to-be operational database on visa applicants, will not only be accessible by visa and immigration authorities, but also by 'competent authorities' of member states as well as Europol for the purpose of prevention, detection or investigation of terrorist offences and other serious crime.

Furthermore it is necessary to mention that some databases and mechanisms also allow (normally under certain restrictive conditions) the exchange of information with authorities of non-EU states and international organisations. This is the case for CIS and VIS, for the EU-US and EU-Canada PNR agreements, the EU-PNR proposal and as regards Europol and Eurojust.

Yet, extending access to databases and information systems to more and more authorities gives rise to another set of questions, concerning among others, those of effective control and 'value' of the data.

---

[14] http://www.ec.europa.eu/anti_fraud/fide/leaflet.pdf (last accessed 4.4.2008).

[15] See Council doc. 6073/2/07 REV 2, 25.6.2007.

As regards control, in a judgement of 10.3.2008 the *Bundesverfassungsgericht* reiterated the importance for the individual of being able to oversee with sufficient reliability what personal information is known to which authorities.[16] Dangers exist, the Court stated, in particular, when personal information is used and interlinked in a way that is impossible to monitor or control by the individual. Considering this statement in the light of the material gathered in Annex 1, one wonders whether the individual whose data has been entered into EU databases or is subject to EU systems of information exchange has in fact any chance of finding out about this, let alone to controlling it. Although there are provisions that intend to ensure that the individual is duly informed and that grant access rights to personal data held, these instruments might be insufficient to establish how the personal information has been actually used, interlinked, and especially, with which authorities it has been exchanged, and how these authorities have further used and exchanged it.

In this respect it is interesting to note, for instance, that data processed in SIS II shall, in principle, *not* be transferred to third states or international organisations (article 54 SIS II-decision). At the same time, however, Europol and Eurojust do have partial access to SIS II data and these two bodies are in fact allowed to communicate the information obtained to third countries and third bodies, only provided that the member state that entered the data has given its consent (article 41(3) SIS II-decision). Whether or not the concerned individual must give his consent or be at least informed about his member state's consenting decision is not regulated by the SIS II-decision.

Finally, as regards the 'value' of data, it is worth examining whether the efforts to involve many more authorities might actually lead to a decrease in value of the data. As was seen in many incidents, authorities compete against each other and information is an important element in this struggle (for sociological research on this struggle, see Bigo, 2007). This competition could also have been one of the underlying motives of a recent 'exchange of views' between authorities in Germany. After security authorities successfully foiled a likely terrorist attack in Germany in September 2007, police officials complained that, in spite of what was perceived as a formidable operation, they were not given sufficient information by the German secret services. The latter denied these allegations and stated, that "policemen don't understand that they don't need to know everything".[17] If sharing information appears to be a contentious field even within one member state, how much more difficult must it be at EU and international level? With member states' authorities knowing that everything they feed into an EU-wide system is accessible to potentially all other authorities in the EU and beyond, they might decide to keep the really important and valuable information for themselves and share it, perhaps, only on a bilateral basis of trust, if at all.

"Competent authorities": is there a common understanding among member states?

The designation of 'competent authorities' by member states for the purpose of participating in EU databases and systems of information exchange is also interesting from another perspective: Is there a common or at least comparable practice among member states?

When looking at the material provided in Annex 2, the answer must be 'no'. In that annex, information is compiled on how member states responded to the request of designating a "competent law enforcement authority" according to article 2a of the *Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and*

---

[16] Bundesverfassungsgericht, 1 BvR 2388/03, 10.3.2008, para. 59-61.

[17] Taken from an article entitled: "Polizisten müssen nicht immer alles wissen", *Süddeutsche Zeitung*, 14.12.2007, p. 6; see also "Lebensgefährliches Schweigen", *Süddeutsche Zeitung*, 12.12.2007, p. 2.

intelligence between law enforcement authorities of the Member States of the European Union.[18] This article defines the concept of law enforcement authority as:

> a national police, customs or other authority that is authorised by national law to detect, prevent and investigate offences or criminal activities and to exercise authority and take coercive measures in the context of such activities. Agencies or units dealing especially with national security issues are not covered by the concept of competent law enforcement authority.

Member states had to communicate 'their' authorities to the Council Secretariat by 18.12.2007 and were reminded about this by the Secretariat in October 2007.[19]

When looking at the table in Annex 2, the following aspects are worth mentioning:

- Only three member states were able to respond on time to their statutory requirement of informing the Council Secretariat about the designation.
- A majority of 'big' member states and in total some 40% of member states had not informed the Council within three months following the deadline.
- The practice of designating authorities varies considerably. In the extreme, there is Spain, which appears to have designated only a contact point for international police cooperation, contrasted with Latvia which has even designated – perfectly in line with the definition – captains of seagoing vessels of ships under the Latvian flag. Most interesting is the case of Austria, which designated a department of its Ministry of Interior as well as district administrations.
- The position of prosecutors and judges seems to be entirely unsettled. From all member states that have submitted their information so far, only the Czech Republic and Latvia consider public prosecutors as being competent law enforcement authorities in the sense of the framework decision.

Lack of common data protection standards

Moving on the to the data protection elements in the EU databases and systems of information exchange, it is possible to observe that at least the vast majority of them take account of the need to ensure the rights of the data subject; some go further and provide specific and detailed requirements. An exception to this is, however, provided by the newly adopted Council resolution on the exchange of information related to the expulsion of third country nationals in the context of counter-terrorism. This resolution lacks even the faintest reference to the data protection rights of concerned individuals.

Yet although data protection requirements are mainly taken into account, the comparative analysis of the databases and systems reveals a considerable lack of common standards. It appears, furthermore, as if this lack of common standards is only partially due to the fact that while there is a data protection directive governing the 'first pillar' Justice and Home Affairs issues, there is – until the present day – no comparable horizontal EU 'third pillar' data protection law (the 2005 Commission's proposal to remedy this gap[20] is making no progress in the Council).

---

[18] OJ L 386, 29.12.2006, p. 89.

[19] Council doc. 14258/07, 24.10.2007.

[20] Commission, Proposal for a Council framework decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, COM(2005) 475 final, 4.10.2005.

This shall be highlighted by the following, non-exhaustive, examples.

- Different time limits for storing data are foreseen within the same subject area. The EU-Canada PNR agreement provides for a regular storage time of 3.5 years and exceptionally a maximum of 6 years. In the EU-US PNR agreement the regular storage time has already doubled to 7 years plus a further storage of 8 years in a 'dormant' database. The EU's own PNR proposal, finally, considers 5 years as appropriate but also intends to rely on a 'dormant phase' of 8 years.
- In most of the legal texts, reference is made to a data protection convention drafted in the framework of the Council of Europe in Strasbourg: the "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data"[21] with subsequent amendments and certain recommendations. In some cases, it is stipulated that these Council of Europe standards must be 'taken into account' or reference is made in the preambles. For SIS, SIS II, CIS and VIS it is additionally provided that participating contracting states must adopt national rules in order to achieve a level of data protection that is at least equal to this Council of Europe standard. Then, in the context of Europol, these national rules must not only be adopted, but furthermore that they must be in force before any data can be exchanged. However, only in one of the latest proposals, the 'Prüm Initative' of 2007,[22] it is foreseen that the Council must unanimously decide whether this level of data protection and the other data protection requirements established by the proposed Council decision itself are satisfied by the participating states.
- The European Data Protection Supervisor has not been assigned the competence to monitor consistently all EU databases and systems of information exchange in addition to the national supervisory authorities. In some databases he is involved (Eurodac, SIS II, VIS), in others not.
- For many data protection aspects, EU rules provide that national laws are decisive, e.g. as regards the requirement to inform the concerned data subject. These national rules, however, might differ substantially.
- Only in a small minority of legal texts, the idea that data protection requirements could be ensured by the technical design of the database or the system of information exchange is reflected ('data protection by design'). An automatic deletion of data once the allowed storage period is over, for instance, is foreseen in the FIDE database of CIS. Furthermore, in the 'Prüm Initiative' it is stated that implementing rules must guarantee that "state-of-the-art technical measures are taken to ensure data protection and data security (…)" [article 29 (2)(a) Prüm Initiative].

The Hague Programme implemented?

Finally, has the Hague Programme's vision on information systems come true? Well, only partially, it seems.

Most obviously, none of the crucial timelines have been met. Neither are SIS II and VIS operational at the time of writing (scheduled for 2007), nor is the exchange of information governed by the principle of availability (scheduled for 1 January 2008). The Commission's proposal as regards the latter was tabled in 2005 but appears not to be followed further by the

---

[21] European Treaty Series No. 108, signed 28.1.1981.

[22] Initiative of the Kingdom of Belgium, […] with a view to adopting a Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ C 71, 28.3.2007, p. 35.

Council. The member states' counter-proposal of 2007 ('Prüm Initiative') is still under discussion. Even if negotiations are finalised soon, the system would still need months - if not years - to be up and running as the technical requirements are considerable. In addition, one might wonder whether the Prüm Initiative is in fact a realisation of the principle of availability as envisaged by the Hague Programme. Europol, for instance, is not mentioned once in the member states' proposal while it seems as if the Hague Programme wanted Europol to profit from the principle of availability and is accordingly involved in the Commission's proposal.

Furthermore, by embracing the principle of availability in the Hague Programme, it appeared as if European leaders wanted the EU to slowly abandon the idea of creating more large-scale centralised databases in the area of freedom, security and justice. In spite of this, a number of proposals have been tabled, with some of them 'thinking even bigger' than many of the existing databases. The 'entry-exist system' is one of them. Other proposals in this direction are the Electronic System of Travel Authorisation (ESTA), the Automated Fingerprint Identification System (AFIS) and in part the EU register for travel documents and identity cards. In this respect too it seems as if the path of the Hague Programme has been somewhat abandoned.

The picture is different, however, when looking at the issue of biometrics. Here, the Hague Programme called on the other actors to continue their efforts to integrate biometric identifiers in travel documents, visas, residence permits, EU citizens' passports and information systems "without delay". This call has in fact been heard and biometric identifiers are incorporated in all the newer systems, like Eurodac, SIS II and VIS. Biometrics are also heavily relied upon in the new Commission's border package proposals and are a recurrent theme in most of the recent communications and documents. The official enchantment with this technology, however, has met criticism by observers who have warned against considering technology as the "ultra-solution to the permanent state of fear", without duly considering that it may end up creating more insecurity, for instance in terms of data protection (cf. Bigo & Carrera, 2004; see also CHALLENGE Mid-term Report, 2007, pp. 7-14).

Conclusions and Recommendations

The main purpose of this paper is to provide detailed comparative information on the growing number of EU databases and systems of information exchange in the area of freedom, security and justice. This should facilitate the understanding of the developing, technology-based security architecture in the EU, its interrelations and possible implications. The following observations constitute a selection of the many others that can be drawn from this overview:

- Uneven participation of EU member states and non-EU member states in EU systems of information exchange not only poses problems as regards complexity and comprehensibility of the systems but also as regards democratic control and the coherent protection of fundamental rights.
- Actual usage of the systems of information exchange varies considerably, with some hardly being used at all.
- Boundaries between migration and asylum issues, border control, criminal law and counter-terrorism are becoming blurred. This contains the risk that the movement of people across borders is conceived and treated more and more as a security issue and a potential criminal activity. In addition, the majority of data in EU systems to which law enforcement authorities have access, relates to third-country nationals. This however entails, that third-

country nationals are more likely to be put under criminal investigation, simply because there is no comparable centralised EU-database for EU nationals.[23]

- Control of data flows becomes increasingly difficult as more and more authorities are lined up to the systems. This development also entails the danger that important information is held back by national authorities and shared only on a bilateral basis of trust.
- Member states' practice of designating 'competent authorities' shows huge discrepancies. This adds to the complexity of the systems and hampers the control of data flows. In addition, this discrepancy might create uneasiness and distrust among the authorities involved. Not every police officer or prosecutor, for instance, might feel comfortable with exchanging information with political bodies of other member states.
- Data protection standards differ between the various systems, due not only to the disparities of the current institutional setting of the EU (pillar division).
- The Hague Programme's plans for the exchange of information remain largely unfulfilled.

Based on these observations, the following recommendations – which are by no means exclusive – are put forward:

- Allowing more non-EU member states to participate in EU databases and systems of information exchange or – on the other hand – granting more EU member states to choose their involvement 'à la carte' should be critically assessed.
- A stronger, supranational control on member states' diverging practice of designating "competent authorities" should be exerted.
- No new EU large-scale IT systems of the dimensions of SIS II and VIS should be agreed upon and established before SIS II and VIS are actually operational and have proven to be proportional, safe and reliable. This requires an assessment of these systems not only as regards their 'efficiency' but also as regards their legal and ethical implications.
- The EU Counter-terrorism Coordinator's idea of a "Common EU Policy on Information Sharing" should be seriously considered and accompanied by a coherent and reinforced "Common EU Policy on data protection". This policy would not only need to address the existing discrepancies within the pillars but also propose solutions for the time after the entry-into-force of the Lisbon Treaty (which will put an end to the 'era of pillars'). In view of this, it might be advisable to suspend any further – fruitless[24] – negotiations on the

[23] Cf. on the discriminatory effect in this regard - but concerning Union citizens on the one hand and nationals of a member state on the other - also the Opinion of Advocate General Maduro in case C-524/06 (Huber), 3.4.2008, para. 21: "(…). Indeed, law enforcement and the combating of crime could, in principle, be a legitimate public policy reason qualifying rights granted by Community law. What member states cannot do, though, is to invoke it selectively, that is, against EU nationals living their territory, but not against their own citizens. If a central register is so important for effective general policing, it should obviously include everyone living within a particular country regardless of his/her nationality. It is not open to national authorities to say that fighting crime requires the systematic processing of personal data of EU citizens but not of that relating to nationals. This would be tantamount to saying that EU nationals pose a greater security threat and are more likely to commit crimes than citizens, which, as the Commission points out, "is completely unacceptable".

[24] Cf. EDPS, Data Protection Framework Decision: EDPS concerned about the dilution of Data Protection standards, Press Release, 30.9.2007.

proposed third pillar framework decision on data protection[25] and start with a completely new proposal once the new Lisbon Treaty is in force. This would also ensure proper involvement of the European Parliament and judicial control by the ECJ. Furthermore, this new approach on data protection could consider the following elements:

  - The European Data Protection Supervisor should be systematically involved in the supervision of all EU databases and systems of information exchange in order to allow at least one body to perceive the interrelations of these mechanisms and their impact on data subjects.
  - 'Data protection by design', allowing for automated solutions to data protection requirements should be made an obligatory element in the implementation of new and existing databases and systems.

- Overambitious political timetables, as contained in the Hague Programme should be avoided in the future. They create expectations and thereby exert artificial pressure on the legislative processes. This is particularly true for a policy area as important and as sensitive as Justice and Home Affairs.

[25] Commission, Proposal for a Council framework decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, COM(2005) 475 final, 4.10.2005.

Annex 1

The following tables provide a comparative overview of some of the major EU databases and EU mechanisms for information exchange, involving personalised data, in the field of Justice and Home Affairs. This overview is broken down into three main sections:

1. EU databases and information networks managed by EU institutions or bodies/agencies, featuring inter alia the centralised large-scale databases, like the Schengen Information System or EURODAC.
2. Common rules on exchange of information genuinely gathered by public authorities. This section comprises mainly EU legal acts in the field of police and judicial cooperation that aim to enhance decentralised information exchange directly between law enforcement authorities.
3. Common rules on exchange of information genuinely gathered by private parties. In contrast to section 2, the last section concentrates on EU legislation that establishes common rules for the public exploitation of information that is genuinely gathered by private parties. Commonly known examples of such legislation are the data retention directive or the Passenger Name Record PNR) agreements with the USA and Canada.

In all three sections, this overview intends not only to give information on the status quo but also highlight some new proposals and possible future steps.

Note on the methodology: The information provided in these tables is taken mainly from the legislative texts that are cited in the footnotes. In some cases the information is taken directly from the original texts, in other cases, it has been reformulated or clarifying elements have been added. In order to allow readability, the respective articles of the legal texts are not specifically cited. Where additional data is provided (e.g. statistical material), the source is given. In the section “data protection elements” the legislative texts were searched for references/statements on data protection, privacy or fundamental rights; additionally for any specific rules regulating these issues. No judgement is made however, on the quality of these data protection elements.

I. EU databases and information networks managed by EU institutions or bodies/agencies

I.1. Active systems as of 31.3.2008

I.1.1. Schengen Information System[26]

	Information on	Handling of biometric identifiers?	Actual Size	Feeding authority	Access	Data protection elements	Time limits for storage	Costs	Participating States
C-SIS (Central system)	Persons: a) Persons wanted for arrest/ extradition purposes. b) Third country nationals to be refused entry into the Schengen territory. c) Missing persons (minors and adults) or persons that for their own protection need temporarily to be placed under police protection. d) Witnesses and persons required to appear before judicial authorities. e) Persons to be put under discreet surveillance or subjected to specific checks. **Data elements include among others:** names including aliases, specific physical characteristics, place and date of birth, sex, nationality, whether the person is armed, violent or has escaped, action to be taken.	No	Number of valid records as of 1.1.2008 (see Council 2008, p. 2): Persons: a) 19,119 persons wanted for arrest/extradition. b) 696,419 third country nationals to be refused entry. c) 24,594 adult and 22.907 minor missing persons. d) 64,684 persons who have to appear before judicial authorities. e) 31,577 persons to be put under surveillance or specific checks.	Information is supplied by contracting states via national sections (N-SIS). All of these are connected to the central technical function (C-SIS).	Authorities responsible for border checks, other police and customs checks carried out within the country and judicial authorities as designated by the contracting states. Partial access can be granted to visa and immigration authorities. Europol and Eurojust have partial access. In practice a wide ranging set of national authorities have access to SIS: from police, state security services, public prosecutors and judges, customs authorities, ministerial departments, immigration offices and vehicle registration authorities.	Special set of rules on protection of personal data and data security. Contracting states must adopt national rules in order to achieve a level of protection of personal data at least equal to that resulting from the principles laid down in the Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data of 28 January 1981 and in accordance with Recommendation No. R (87) 15 of 17 September 1987 of the Committee of Minister of the Council of Europe regulating the use of personal data in the police sector. Rules on purpose limitation. Rules on the right to have inaccurate or unlawfully stored data corrected or deleted.	a) Data entered for the purposes of tracing persons are kept for the time required to meet the purposes for which they were entered. After a maximum of 3 years an obligatory review of the necessity to keep the data must take place (After 1 year in case of entry for discreet surveillance or specific checks). However, under certain circumstances, even after deletion of data in the C-SIS, contracting states are allowed to store C-SIS data for a longer period in their national files. b) 10 years maximum storage time for other data than that mentioned under a). c) 5 years maximum storage time for vehicles, boats, aircrafts, containers entered for the purposes of discreet surveillance and specific checks.	Year 2006 2,07 million Euros for C-SIS. (Commission 2007c, p. 11). Costs for the central system are borne jointly by contracting states.	EU member states except Cyprus, Romania, Bulgaria plus non-EU states Iceland and Norway. UK and Ireland are in principle allowed to access the police and judicial cooperation-parts of SIS (not the ones relating to borders), but have not yet realized their practical connection to the system (House of Lords 2007, p. 11 and 14). Switzerland and Liechtenstein to join soon. (Council 2007a, p. 4)

[26] Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders, OJ L 239, 22.9.2000, p. 19 as amended by Council Regulation (EC)No. 871/2004 of 29 April 2004 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism, OJ L 162, 30.4.2004, p. 29 and Council Decision 2005/211/JHA of 24 February 2005 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism, OJ L 68, 15.3.2005, p. 44. See also Council Decision 2006/228/JHA of 9 March 2006 fixing the date of application of certain provisions of Decision 2005/211/JHA concerning the introduction of some new functions for the Schengen Information System, including the fight against terrorism, OJ L 81, 18.3.2006, p. 45 and Council Decision 2006/229/JHA of 9 March 2006 fixing the date of application of certain provisions of Decision 2005/211/JHA concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism, OJ L 81, 18.3.2006, p. 46.

	Information on	Handling of biometric identifiers?	Actual Size	Feeding authority	Access	Data protection elements	Time limits for storage	Costs	Participating States
	Data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexuality shall not be registered. Note that additional information to an entry in C-SIS can be exchanged between national authorities. This additional information is held in the so called SIRENE databases of each contracting state. Objects: a) Vehicles, boats, aircrafts, containers for the purpose of discreet surveillance or specific checks. b) Objects sought for the purposes of seizure or use as evidence in criminal proceedings (e.g.. stolen identity cards, vehicles, firearms, bank notes).		On top 299,473 aliases of wanted persons. Objects: a) 3,012,856 vehicles. b) 17,876,227 identity cards. c) 314,897 firearms. d) 390,306 blank documents. e) 177,327 banknotes.		A list of all authorities for all participating states having access to SIS is provided in Council doc. 6073/2/07 REV 2, 25.6.2007.	Access to stored data by data subject governed by national laws. Liability governed by national law. National supervisory body in each contracting state responsible for the national sections of SIS. Joint supervisory authority composed of national supervisory authorities responsible for C-SIS. Contracting states may refuse to act on the basis of an SIS alert, if they consider it to be incompatible with their national laws, international obligations or essential national interests.			

I.1.2. Eurodac[27]

	Information on	Handling of biometric identifiers?	Actual Size	Feeding authority	Access	Data protection elements	Time limits for storage	Costs	Participating States
Eurodac – Central database	Full 10 fingerprints and 4 control images of persons aged at least 14 years who are: a) Applicants for asylum **Data elements include among others:** fingerprints and control images, member state of origin, place and date of application for asylum, sex, reference number used by member state of origin, date on which fingerprints were taken. b) Persons apprehended in connection with the irregular crossing of borders coming from a third country **Data elements include among others:** fingerprints and control images, member state of origin, place and date apprehension, sex, reference number used by member state of origin, date on which fingerprints were taken. The system also allows checking fingerprints of **persons found illegally** present in a member state with the existing fingerprints stored in Eurodac. However, the data of these persons are not stored.	Yes	Period 2003-2005 a) 657,753 sets of data of asylum applicants; b) 48,657 sets of data of persons apprehended at borders; (Commission 2007a, p. 5).	Participating states – Eurodac national access points. In theory this should only be national authorities in charge of handling asylum request. In some member states, however, Eurodac is operated partly or entirely by national police services (EDPS 2007, p. 12).	National authorities. See also: Feeding authority.	Special rules on data use, protection and liability are provided in the regulation. Data protection directive 95/46/EC is additionally applicable. EDPS is competent data protection authority to monitor activities of the Eurodac central unit National data protection authorities supervise collection and use of data at member states level.	a) 10 years for asylum applicants (obligatory erasure of data as soon as the person has acquired citizenship of a member state; obligatory blockage of data as soon as the person is recognised and admitted as refugee in a member state), b) 2 years for persons apprehended at borders (data shall be erased if person acquires citizenship, obtains residence permit or leaves the EU territory).	Year 2006 244,240.73 Euro expenditure for maintaining and operating the Central Unit. Period 2003-2006 7.8 million Euro of Community expenditure for all externalised activities specific to Eurodac. (Commission 2007b, p. 5)	EU 27 plus Norway and Iceland. Switzerland and Liechtenstein soon.

[27] Cf. Council Regulation (EC) No. 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention, OJ L 316, 15.12.2000, p. 1.

I.1.3. Customs Information System[28]

	Information on	Handling of biometric identifiers?	Actual Size	Feeding authority	Access	Data protection elements	Time limits for storage	Costs	Participating States
CIS – 3rd pillar	1) "Traditional" CIS: Information, inter alia, on: a) Commodities, b) means of transport, c) businesses, d) persons, for the purposes of sighting and reporting, discreet surveillance or specific checks and only if there are real indications to suggest that the person concerned has committed, is in the act of committing or will commit serious contraventions of national laws. **Data elements include among others:** names (maiden name, aliases), date and place of birth, nationality, sex, particular objective and permanent objectives, reason for inclusion of data, suggested action, warning code indicating and history of being armed, violent or escaping. Data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life shall not be registered.	No	Period 2003-2006 and covering 1st and 3rd pillar entries a) 490 active cases (i.e. all cases which have not been deleted by users or automatically). b) 1370 users. 95% of all cases have been entered by only 5 member states (all figures Council 2007b, p. 4).	Inclusion of data is governed by national laws of member states.	Customs administrations as designated by member states. Other authorities competent to act in order to prevent, investigate and prosecute serious contraventions of national laws, as designated by member states. Access can be granted to international and regional organisations. Data retrieved from the system may also be used by other national authorities than those who have direct access, by non-member states and by international or regional organisations.	Special set of rules on protection of personal data and data security. Contracting states must adopt national rules in order to achieve a level of protection of personal data at least equal to that resulting from the principles laid down in the Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data of 28 January 1981. Rules on purpose limitations. Rules on the right to have inaccurate or unlawfully stored data corrected or deleted. Access to stored data by data subject, governed by national laws. Liability governed by national law. National supervisory body in each member state responsible for the lawfulness of the entry, processing and use of CIS data in that member state. Joint supervisory authority composed of national supervisory authorities responsible for the supervision of the operations of CIS.	As long as necessary to achieve the purpose for which the data was included. After 1 year an obligatory review of the necessity to keep the data must take place.	n/a	EU 27

[28] Cf. Convention drawn up on the basis of Article K.3 of the Treaty on European Union, on the use of information technology for customs purposes, OJ C 316, 27.11.1995, p. 34; Council Act of 12 March 1999 drawing up, on the basis of Article K.3 of the Treaty on European Union, the Protocol on the scope of the laundering of proceeds in the Convention on the use of information technology for customs purposes and the inclusion of the registration number of the means of transport in the Convention, OJ C 91, 31.3.1999, p. 91. Note that apart from this third pillar legal base, there is also a first pillar regulation. Council Regulation (EC) No. 515/97 of 13 March 1997 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters, OJ L 82, 22.3.1997, p. 1. See also: Proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No. 515/97 of 13 March 1997 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters, COM(2006) 866 final, 22.12.2006.

	Information on	Handling of biometric identifiers?	Actual Size	Feeding authority	Access	Data protection elements	Time limits for storage	Costs	Participating States
	2.) Customs Files Identification Database (FIDE): [29] Information on ongoing or completed investigations for serious infringements of national laws against persons or businesses in member states. "Serious infringements" are defined as those punishable by deprivation of liberty or a detention order for at least 12 months, or by a fine of at least 15 000 EUR.	No		National authorities responsible for carrying out customs investigations designated by member states.	National authorities responsible for carrying out customs investigations designated by member states.		Governed by laws of member states. However, the following maximum periods of data retention are foreseen (automatic deletion): a) 3 years if data refers to current investigations and it has not been established that an infringement has taken place; the data must be deleted earlier, if 1 year has passed since the last investigative act. b) 6 years if data refers to investigation files that have established that an infringement has taken place but which have not yet led to a conviction or a fine. c) 10 years if data refers to investigation files that have led to a conviction or a fine Additionally: as soon as a person or business is eliminated from an investigation, all CIS data must be deleted immediately.		

[29] Council Act of 8 May 2003 drawing up a Protocol amending, as regards the creation of a customs files identification database, the Convention on the use of information technology for customs purposes, OJ C 139, 13.6.2003, p. 1.

I.1.4.Europol[30]

	Information on	Handling of biometric identifiers?	Actual Size	Feeding authority	Access	Data protection elements	Time limits for storage	Costs	Participating States
Europol - The Europol Computer System (TECS) **TECS consists of three elements:** **1.) The Information System** **2.) Analytical Work Files** **3) The Index System**	1.) The Information System a) Suspects or convicted persons of a crime. b) Possible future offenders. **Data elements include among others:** surname, maiden name, given names, aliases or assumed names, date and place of birth, nationality, sex, specific physical characteristics. Additional data on the type of crime, used means, earlier convictions can be processed.	Yes, in particular as soon as SIS II is operational.	As of 18.12.2006 4311 offences. Inputs to the Information System by member states and Europol in 2006 amounted to more than 50.000. (Both figures: Europol 2007, p. 18).	Member states, represented by their national units and liaison officers in compliance with their national procedures. Europol itself shall input data supplied by third states and third bodies as well as analysis data.	National units, liaison officers, the Director, the Deputy Directors as well as duly empowered Europol officials. Indirect access by "competent authorities" designated by member states.	Special set of rules on protection of personal data and data security. Member states must adopt national rules in order to achieve a level of protection of personal data at least equal to that resulting from the principles laid down in the Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data of 28 January 1981 and in accordance with Recommendation No. R (87) 15 of 17 September 1987 of the Committee of Minister of the Council of Europe regulating the use of personal data in the police sector. No data exchange shall take place before these measures have not entered into force in the member states. Europol itself shall take account of the Council of Europe principles. Rules on purpose limitations. Rules on data protection requirements when data is transferred to third states or third bodies. Specific rules on access to information, correction and deletion of in correct data. Rules on liability. National supervisory body in each contracting state responsible for monitoring the input and use of Europol data by the member state's authorities. Joint supervisory authority composed of national supervisory authorities responsible for Europol.	As long as necessary for the performance of Europol's task. After a maximum of 3 years an obligatory review of the necessity to keep the data must take place. Personal data relating to specific offences shall be deleted if proceedings against the person are dropped or if that person is acquitted of the offence.	Year 2006 Total budget of Europol: 66.01 million Euros (Europol Annual Report, 2006, p. 23).	EU 27 With a number of third countries and international bodies, Europol has concluded agreements.
	2.) Analytical Work Files a) Suspects or convicted persons of a crime. b) Possible future offenders. c) Possible witnesses. d) Victims and possible victims. e) Contacts and associates. f) Persons who can provide information on the criminal offence under consideration.		28 Analytical Work Files in 2006. (Europol 2007, p. 15).	Analysts and other Europol official specifically designated for each analysis project. Experts from third states and third bodies may be "associated" with the activities of an analysis group.	Analysts and other Europol official specifically designated for each analysis project. The liaison officers and/or experts of the member states which are concerned by the analysis file. Experts from third states and third bodies may be "associated" with the activities of an analysis group.		As long as necessary for the performance of Europol's tasks. After a maximum of 1 year an obligatory review of the necessity to keep the data must take place.		

[30] Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention), OJ C 316, 27.11.1995, p. 2 as amended by subsequent protocols. A consolidated version of the Convention is available on Europol's website: http://www.europol.europa.eu/legal/Europol_Convention_Consolidated_version.pdf. Note: a legislative proposal is currently under discussion to provide Europol with a new legal base (Council decision). This proposal also affects the Europol Computer System and related issues, see Proposal for a Council Decision establishing the European Police Office (EUROPOL), COM(2006), 817 final, 20.12.2006.

	Information on	Handling of biometric identifiers?	Actual Size	Feeding authority	Access	Data protection elements	Time limits for storage	Costs	Participating States
	Data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexuality shall – in principle - not be registered. However, if it is "strictly necessary" also such data can be processed and stored.								
	3.) Index System		n/a	Created by Europol.	Director, Deputy Directors, duly empowered Europol officials, liaison officers.		n/a		

I.1.5.Eurojust[31]

	Information on	Handling of biometric identifiers?	Actual Size	Feeding authority	Access	Data protection elements	Time limits for storage	Costs	Participating States
Eurojust	a) Persons who are the subject of criminal investigation or prosecution. b) Witnesses or victims in a criminal investigation or prosecution. **Data elements include among others:** surname, maiden name, given names, aliases or assumed names, date and place of birth, nationality, sex, place of residence, profession. In exceptional cases: other personal data relating to the circumstances of an offence. Data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexuality may be processed only when such data are necessary for the national investigations concerned as well as for coordination within Eurojust.	Yes, in particular as soon as SIS II is operational.	Year 2006: 771 registered cases (Eurojust 2007, p. 19).	Eurojust national members, their assistants and authorised Eurojust staff.	Eurojust national members, their assistants and authorised Eurojust staff. Eurojust may exchange data with national competent authorities of member states, authorities of third countries which are competent for investigations and prosecutions as well as international organisations and bodies.	Special set of rules on protection of personal data and data security. Eurojust must take necessary measures to guarantee a level of protection for personal data at least equivalent to that resulting from the application of the principles of the Council of Europe 1981 Convention for the Protection of individuals with regard to Automatic Processing of Personal Data. Special rules on data use, data security and liability. Access by individuals and the possibility to claim correction and deletion of incorrect files exists. Own data protection officer as well as independent supervisory authority. Own extensive rules of procedure on the processing and protection of personal data at Eurojust were adopted (OJ C 68, 19.3.2005, p. 1).	Generally: as long as prosecution is ongoing, has not resulted in a final judicial decision and is still legally possible (e.g. not statute barred). Continuous observance is required. Obligatory review of necessity every 3 years.	Year 2006 Total budget of Eurojust: 14.7 million Euros (Eurojust 2007, p. 52).	EU 27 Europol has concluded agreements with a number of third countries.

[31] Council Decision of 28 February 2002 setting up Eurojust with a view of reinforcing the fight against serious crime, OJ L 63, 6.3.2002, p.1.

I.1.6. Joint Situation Centre - SitCen[32]

SitCen	The EU Joint Situation Centre (SitCen) is located within the Council Secretariat and composed of analysts from member states' external and internal intelligence services.[33] Based on assessed/evaluated intelligence provided by member states' services SitCen monitors and assesses events and situations worldwide on a 24-hour basis with a focus on potential crisis regions, terrorism and weapons of mass destruction-proliferation. SitCen is divided into three Units: the Civilian intelligence Cell (CIC), comprising civilian intelligence analysts working on political and counter-terrorism assessment; the General Operations Unit (GOO), providing 24-hour operational support, research and non- intelligence analysis; and the Communications Unit (handling communications security issues and running the Council's ComCen).[34] There is no legal document that governs the activities of SitCen, yet it seems quite likely that personal data is in fact handled and processed.

I.2. Future systems soon to be active

I.2.1. Schengen Information System II[35]

	Information on	**Handling of biometric identifiers?**	**Size**	**Feeding authority**	**Access**	**Data protection elements**	**Time limits for storage**	**Costs**	**Participating States**
Central SIS II (SIS II will replace the current SIS)	a) Persons wanted for arrest for surrender purposes on the basis of a European arrest warrant (EAW) or wanted for arrest for extradition purposes. In case of an EAW, supplementary information specific to the EAW procedure has to be communicated. b) Third country nationals to be refused entry into the Schengen territory. c) Missing persons. d) Witnesses and persons required to appear before judicial authorities. e) Persons to be put under discreet checks or subjected to specific checks. Supplementary information has to be provided in these cases.	Yes	Estimates provided in official documents refer to searches conducted in the system, not to total number of entries. As regards searches, the Commission expects a growth from 65 million to 95 million in the first two years of the system (Commission 2005a, p. 45).	Information is supplied by contracting states via national interfaces (NI-SIS).	Authorities responsible for the identification of third country nationals for the purposes of border control, other police and customs checks carried out within the country and judicial authorities as designated by the contracting states. Partial access can be granted to visa and immigration authorities. Partial access by vehicle registration authorities.	General reference to fundamental rights and the EU Charter. Reference to Directive 95/46/EC (i.e. "first pillar" data protection directive) for the first pillar aspects of SIS II. Reference to Regulation 45/2001 on the processing of personal data by the Community institutions and bodies and on the free movement of such data. Personal data shall be protected by the Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data of 28 January 1981 and subsequent amendments thereto. Special set of rules on protection of personal data and data security.	a) **Data on persons** are kept for the time required to meet the purposes for which they were entered. After a maximum of 3 years an obligatory review of the necessity to keep the data must take place (after 1 year in case of entry for discreet check or specific checks). However, under certain circumstances, even after deletion of data in the SIS II, contracting states are allowed to store data for a longer period in their national files.	Period 2007-2012 Estimation of 2005: 114 million Euros out of EU budget to get the system up and running (House of Lords 2007, p. 15.)	Situation as of March 2008: EU member states (UK and Ireland partially) except Cyprus, Romania, Bulgaria plus non-EU states Iceland and Norway. Switzerland and Liechtenstein soon.

[32] There is no public legal or policy document governing the work of SitCen; on its practical evolution see cf. W. Shapcott, Director of SitCen, Oral Evidence, House of Lords, EU Committee, 5th Report of Session 2004-05, "After Madrid: the EU's response to terrorism", pp. 53 - 62.

[33] G. de Vries, "The European Union's role in the fight against terrorism", *Irish Studies in International Affairs*, vol. 16 (2005), pp. 3-9.

[34] General Secretariat of the Council of the European Union, Notice of Vacancy Ref. A/015.

[35] Regulation (EC) No. 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation of the Schengen Information System (SIS II), OJ L 381, 28.12.2006, p. 4; Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ L 205, 7.8.2007, p 63. Regulation (EC) No. 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates, OJ L 381, 28.12.2006, p. 1.

	Information on	Handling of biometric identifiers?	Size	Feeding authority	Access	Data protection elements	Time limits for storage	Costs	Participating States
	Data elements include among others: names including, previous names, birth names, aliases, specific physical characteristics, place and date of birth, sex, photographs, fingerprints, nationalities, whether the person is armed, violent or has escaped, action to be taken, links to other alerts issued in SIS II. Data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexuality shall not be registered Note: supplementary information to an entry can be exchanged between national authorities ("Sirene"). Objects: a) Vehicles, boats, aircrafts, containers for the purpose of discreet checks or specific checks. Supplementary information has to be provided in these cases. b) Objects sought for the purposes of seizure or use as evidence in criminal proceedings (e.g. stolen identity cards, vehicles, firearms, bank notes).				Partial access by Europol and Eurojust. Personal data processed in SIS II shall not be transferred to third countries or international organisations. However: passport number, country of issuance and the document type of stolen, lost, misappropriated, lost or invalid passports entered in SIS II may be exchanged with Interpol.	Specific reference to principle of proportionality. Specific rules on purpose limitation. Rules on the right of information (but only as regards third country nationals who are refused entry the Schengen territory. In the police and criminal law entries of SIS II, information to the data subject is governed by national law). Rules on the right to have inaccurate or unlawfully stored data corrected or deleted. Access to stored data by data subject, governed by national laws. Liability governed by national law. National supervisory authorities in each contracting state shall monitor the lawfulness of the processing of SIS II data on their territory. European Data Protection Supervisor shall monitor the activities of the EU personnel managing SIS II. All supervisory bodies shall meet at least twice a year. Contracting states may refuse to act on the basis of a SIS II alert, if they consider it to be incompatible with their national laws, international obligations or essential national interests (this, however, is not possible for alerts on third country nationals which are banned from EU territory).	On acquisition of citizenship of any state whose nationals are beneficiaries of the right of free movement within the Community, the entry must be deleted if it refers to an entry-ban for third country nationals). b) 10 years maximum storage time for **alerts on objects** for seizure or use as evidence in criminal proceedings. c) 5 years maximum storage time for **vehicles, boats, aircrafts, containers** entered for the purposes of discreet checks and specific checks.		

I.2.2. Visa Information System[36]

	Information on	Handling of biometric identifiers?	Size	Feeding authority	Access	Data protection elements	Time limits for storage	Costs	Participating States
Central-VIS	**Visa applicants**, the application procedure and the "visa history" of the applicant. This includes fingerprints and photographs as well as among others: a) surname, surname at birth, first names, sex, date, place and country of birth, b) current nationality and nationality at birth, c) type and number of travel documents, issuing authority, date of issue and expiry, d) place and date of application e) type of visa requested f) details of the person issuing an invitation and/or liable to pay the applicant's subsistence costs during the stay, g) main destination and duration of intended stay, h) purpose of travel, i) intended date of arrival and departure, j) intended border of first entry or transit route, k) residence, l) current occupation and employer; for students: name of school, m) in the case of minors, names of father and mother.	Yes	Foreseen capacity: 70 million applicants (Commission 2004, p. 45).	Visa authorities of the participating states.	Visa, immigration and asylum authorities as designated by participating states. Competent authorities responsible for carrying out checks at external border crossing points in accordance with Schengen Border Code. On request in specific cases also designated authorities for the purpose of prevention, detection or investigation of terrorist offences and other serious criminal offences as well as Europol within the limits of its mandate and when necessary to perform its tasks. Under specific circumstances VIS data can be transferred to third countries or to an international organisation. VIS data obtained for the purpose of counter-terrorism and crime should in principle not be transferred to third countries or international organisations, but it is allowed in exceptional cases of urgency.	General reference to fundamental rights and the EU Charter. Reference to principle of proportionality, human dignity and anti-discrimination in the use of the database. Reference to Directive 95/46/EC (i.e. 'first pillar' data protection directive). Reference to Regulation 45/2001 on the processing of personal data by the Community institutions and bodies and on the free movement of such data. As far as access by law enforcement authorities is concerned, participating states must ensure that their national data protection laws correspond to the level provided by the Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data of 28 January 1981 and subsequent amendments thereto. As regards access to Europol, the Europol Convention and its data protection requirements must be respected. Special set of rules on protection of personal data and data security Specific rules on purpose limitation. Rules on the right of information (as far as law enforcement authorities using VIS data are concerned, this aspect is governed by national law). Rules on the right to have inaccurate or unlawfully stored data corrected or deleted. Access to stored data by data subject governed by national laws. Liability governed by national law.	5 years maximum. On expiry of the period the system itself shall automatically delete the data. If applicant acquires nationality of a participating state, his file and the links to it shall be deleted without delay.	Period 2004-2009 (development phase): Circa 70 million Euro estimated costs. This excludes the costs incurred at member state level as well as maintenance costs (Commission 2008, p. 20)	Situation as of March 2008: EU member states except UK and Ireland, Cyprus, Romania, Bulgaria. Denmark can choose to join. Non-EU states Norway and Iceland will participate. Switzerland and Liechtenstein soon.

[36] Council Decision of 8 June 2004 establishing the Visa Information System (VIS), OJ L 213, 15.6.2004, p. 5; Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short stay visas (VIS Regulation), 2004/0287 (COD), PE-CONS 3630/1/07 REV 1, 1.10.2007; Council Decision concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection, investigation of terrorist offences and of other serious criminal offences, Council doc. 11077/1/07 REV 1, 11.10.2007; Proposal for a Regulation of the European Parliament and of the Council amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics including provisions on the organisation of the reception and processing of visa applications, COM(2006) 269 final, 31.5.2006; Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 562/2006 as regards the use of the Visa Information System (VIS) under the Schengen Borders Code, COM(2008) 101 final, 22.2.2008.

	Information on	Handling of biometric identifiers?	Size	Feeding authority	Access	Data protection elements	Time limits for storage	Costs	Participating States
	Links to previous applications and between applicants travelling together.					National supervisory authorities in each contracting state shall monitor the lawfulness of the processing of VIS data by the participating states. European Data Protection Supervisor shall monitor the activities of the EU personnel managing VIS. All supervisory bodies shall meet at least twice a year.			

I.3. Legislative Proposals and possible further steps

	Aim and content of the proposals/possible further steps
European Register of Convicted Persons (ERCP)[37]	This idea is part of the efforts to facilitate the exchange of information extracted from criminal registers of the member states. However, concrete legislative proposals and measures in this field have so far concentrated only on EU citizens (see below II.1. and II.2.). So far, a de-centralised solution where the convicting member state informs the member state of nationality of the EU citizen convicted, has been chosen. As regards third-country nationals, however, the Commission is proposing to consider establishing a centralised index of convicted third-country nationals. Only those elements enabling the identification of the convicted person (possibly including biometrics) would be communicated to the index. The additional data on the convictions would not be in the index but would need to be requested by the convicting member states.
EU register for travel documents and identity cards?[38]	In its Communication of 24.11.2005 the Commission assumes that member states will create national databases of issued travel documents and identity cards, including biometric identifiers enrolled at application. In order to enhance the effectiveness of these databases, the Commission suggests establishing a register of indexes at European level or, alternatively, to interlink all these national databases. This would allow a check on the authenticity of every travel or ID document issued in a member state and to determine, using biometrics, the identity of any person to whom a travel or ID document was issued, according to the Commission.
European criminal "Automated Fingerprint Identification System (AFIS)"[39]	In its Communication of 24.11.2005 the Commission suggest establishing a European AFIS for police investigation purposes, combining all fingerprint data currently available in national criminal AFIS systems. In its Annual Policy Strategy for 2008 (21.2.2007) the Commission had scheduled "Implementing a centralised database of fingerprints" (p. 12). However, in the Legislative and Work Programme for 2008 (23.10.2007) this idea has not been taken up again.
Entry-exit system?[40]	In its Communication of 13.2.2008, the Commission proposes a new system to register the entry/exit of third country nationals. This new system could include the recording of information (including biometric data) on the time and place of entry of third country nationals, the length of stay authorised, and the transmission of automated alerts directly to the competent authorities, in case the person 'overstays'. The technical solution for its implementation is not decided yet. It could become part of the Visa Information System (VIS) or be realized in a new system (database).
Electronic System of Travel Authorisation (ESTA)[41]	In its Communication of 13.2.2008 the Commission proposes to analyse the feasibility of a system that would require travellers to the EU to make an electronic application supplying, in advance of travelling, data identifying the traveller and specifying the passport and travel details. This information could then be used for verifying whether the traveller fulfils the conditions for entering EU territory.
Granting law enforcement authorities access to Eurodac[42]	This envisaged proposal aims at allowing member states' police and law enforcement authorities to conduct searches in Eurodac for the purposes of preventing, detecting or investigating criminal offences, in particular terrorist offences. Until now, the purpose of Eurodac is to assist in determining which member state is responsible for the examination of an application for asylum lodged in a member state. A detailed legislative proposal has not been tabled yet.

[37] Commission Working Document on the feasibility of an index of third-country nationals convicted in the European Union, COM(2006) 359 final, 4.7.2006: see also White Paper on exchanges of information on convictions and the effect of such convictions in the European Union, COM(2005) 10 final, 25.1.2005.

[38] Commission Communication, on improved effectiveness, enhanced interoperability, and synergies among European databases in the area of Justice and Home Affairs, COM(2005) 597 final, 24.11.2005, p. 9.

[39] Commission Communication, on improved effectiveness, enhanced interoperability, and synergies among European databases in the area of Justice and Home Affairs, COM(2005) 597 final, 24.11.2005, p. 8. Note that the abbreviation AFIS as used in the cited Commission's document, is also the abbreviation of an already existing EU information system, titled "Anti-Fraud Information System", see e.g. OLAF Annual Report 2006, 27.3.2007, p. 19.

[40] Commission Communication, Preparing the next steps in border management in the European Union, COM(2008) 69 final, 13.2.2008, p. 7-9.

[41] Commission Communication, Preparing the next steps in border management in the European Union, COM(2008) 69 final, 13.2.2008, p. 9.

II. Common rules on exchange of information genuinely gathered by public authorities

II.1. Enacted legislation/adopted resolution as of 31.3.2008

	Cited Legal base	Instrument	Stated Purpose	Exchange of information on	Involved authorities	Data protection elements	Participating States
DNA Analysis results (1997 and 2001)[43]	None provided	Council Resolution	To make a significant contribution to the investigation of crime.	Data from the non-coding part of the DNA molecule for the purpose of investigating crime. However: exchange of this data is not a legally binding obligation. The resolution just contains suggestions to member states. Among these suggestions are: a) to consider establishing national DNA databases, b) to consider establishing a network of compatible national DNA databases at EU level, c) as a second step to consider the need to establish a European DNA database.	One contact point per member state.	Reference to the Council of Europe 1981 Convention for the Protection of individuals with regard to Automatic Processing of Personal Data is made in the preamble. National rules must comply with the Council of Europe standards. General reference to "sufficient safeguards concerning the security and protection of personal data".	EU 27
Mutual assistance in criminal matters (2000)[44]	Arts. 31(a) and 34(2)(d) TEU	Convention	To improve judicial cooperation in criminal matters between member states without prejudice to the rules protecting individual freedom.	Any relevant information linked to the investigation or prosecution of crime with or without a specific request by one member state. Special provision foreseen for requests for interception of telecommunications and transmission. Additional protocol to the Convention stipulates conditions of obtaining information on bank accounts and banking transactions.[45]	Different authorities depending on the precise request for mutual assistance.	Rules on purpose limitation are laid down as well as the possibility to refuse assistance under certain circumstances. Reference to national law and the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) in preamble.	EU 27 and for certain aspects also Norway and Iceland.[46]

[42] Legislative proposal not yet tabled but requested by JHA Council of 12 – 13 June 2007. See also Commission 2007a, p. 11; Commission 2005b, p. 8; Council of the European Union, Access to Eurodac by Member States' police and law enforcement authorities, Council doc. 5452/07, 19.1.2007.

[43] Council Resolution of 9 June 1997 on the exchange of DNA analysis results, OJ C 193, 24.6.1997, p. 2; Council Resolution of 25 June 2001 on the exchange of DNA analysis results, OJ C 187, 3.7.2001, p. 1.

[44] Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C 197, 12.7.2000, p. 3.

[45] Protocol established by the Council in accordance with Article 34 of the Treaty on European Union to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C 326, 21.11.2001, p. 2.

[46] See Agreement between the European Union and the Republic of Iceland and the Kingdom of Norway on the application of certain provisions of the Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union and the 2001 Protocol thereto, OJ L 26, 29.1.2004, p. 3.

	Cited Legal base	Instrument	Stated Purpose	Exchange of information on	Involved authorities	Data protection elements	Participating States
Money laundering (2000)[47]	Art. 34(2) (c) TEU	Council Decision	To improve the mechanisms for exchanging information on suspicious financial transactions and underlying criminal activity.	Any available information that may be relevant to the processing or analysis of information or to investigation by the Financial Intelligence Unit regarding financial transactions related to money laundering and the natural or legal persons involved.	Financial Intelligence Units (FIUs) in member states as set up in accordance with Directive 91/308/EC and further defined as "A central, national unit which, in order to combat money laundering, is responsible for receiving (and to the extent permitted, requesting), analysing and disseminating to the competent authorities, disclosures of financial information which concern suspected proceeds of crime or are required by national legislation or regulation."	Clear legal commitment to data protection standards as stipulated in Council of Europe 1981 Convention for the Protection of individuals with regard to Automatic Processing of Personal Data and to national legislation. Rules on purpose limitation and data security. Possibility to refuse exchange of information if this would be "clearly disproportionate to the legitimate interests of a natural or legal person or the Member State"; also, if it would be in breach of "fundamental principles of national law".	EU 27
Football matches (2002)[48]	Arts. 30(1) (a) and (b), 34 (2)(c) TEU	Council Decision	High level of safety within an area of freedom, security and justice by developing common action among member states in the field of police cooperation. Preventing and combating football-related violence.	Personal data of "high-risk supporters". Exchange of information, including personal data, shall take place before, during and after a football event with an international dimension.	National football information points of a "police nature". These contact points shall communicate the information to all police services concerned.	Reference to "domestic and international rules applicable" to data exchange. Council of Europe 1981 Convention for the Protection of individuals with regard to Automatic Processing of Personal Data shall be taken into account.	EU 27
Genocide and crimes against humanity (2002)[49]	Arts. 30 and 34 (2)(c) TEU	Council Decision	Closer cooperation of authorities involved in investigating crimes of genocide, crimes against humanity and war crimes.	Any available information that may be relevant in the context of investigations into genocide, crimes against humanity and war crimes such as those defined in the Rome Statute of the International Criminal Court of 17 July 1998.	Authorities involved in investigating crimes of genocide, crimes against humanity and war crimes. Designated contact points in member states.	Not specified. General reference to "limits of the applicable national law."	EU 27

[47] Council Decision of 17 October 2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information, OJ L 271, 24.10.2000, p. 4.

[48] Council Decision of 25 April 2002 concerning security in connection with football matches with an international dimension, OJ L 121, 8.5.2002, p. 1 as amended by Council Decision 2007/412/JHA of 12 June 2007, OJ L 155, 15.6.2007, p. 76.

[49] Council Decision of 13 June 2002 setting up a European network of contact points in respect of persons responsible for genocide, crimes against humanity and war crimes, OJ L 167, 26.6.2002, p. 1.

	Cited Legal base	Instrument	Stated Purpose	Exchange of information on	Involved authorities	Data protection elements	Participating States
EU-US Agreement on mutual legal assistance (2003)[50]	Arts. 24 and 38 TEU	International Agreement/ Council Decision	To combat crime in a more effective way as a means of protecting the EU's and the US's democratic societies and common values.	Any relevant information linked to the investigation or prosecution of crime under certain conditions. Special provision foreseen as regards bank information of natural or legal persons suspected of or charged with a criminal offence.	Designated national authorities of member states and the US responsible for investigation or prosecution of criminal offences. Also administrative authorities can profit from the Agreement provided they are competent to investigate criminal offences according to national law	Rules on purpose limitation are laid down as well as the possibility to refuse assistance under certain circumstances. General reference to the "rights of individuals and the rule of law" in preamble.	EU 27 and USA
Passport data with Interpol (2005)[51]	Arts. 30(1) (b), 34 (2)(a) TEU	Council Common Position	To prevent and combat serious and organised crime, including terrorism.	Present and future data on issued and blank passports, which are stolen, lost or misappropriated. Member states are obliged to exchange this information with the Interpol database on Stolen Travel Document, in parallel to entering them in the relevant national database and the SIS.	EU member states' law enforcement authorities, Interpol as well as Interpol member states.	Reference to data protection principles is made but adherence left to member states' authorities and national laws. The same applies to correctness of data.	EU 27
Terrorist offences (2005)[52]	Arts. 29, 30 (1), 31 and 34 (2) (c) TEU	Council Decision	Fight against terrorism. Relevant services need to have fullest and most up-to-date information possible.	Europol shall receive all relevant information concerning and resulting from criminal investigations conducted by law enforcement authorities in member states with respect to terrorist offences. Eurojust shall receive all relevant information concerning prosecutions and convictions for terrorist offences in member states.	Specialised services within member states police forces to make contacts with Europol. Eurojust national correspondents for terrorism matters or other competent authority. Europol and Eurojust	Unspecified reference to national law as well as to the Europol Convention/Eurojust decision is made. Apart from that only blanket statement in preamble that the Decision respects fundamental rights.	EU 27
Criminal records (2005)[53]	Arts. 31 and 34 (2) (c) TEU	Council Decision	To provide citizens with a high level of security within in an area of freedom, security and justice. To facilitate exchange of information concerning criminal convictions of persons who reside in the territory of the member states between the competent authorities of the member states.	Criminal convictions of EU citizens and subsequent measures. Information is normally provided on the basis of a formalised request procedure. However, if a national of one member state is convicted in another member state, the latter must inform the central authority of the other member state automatically and without delay.	One or more unspecified "central authority" in each member state.	Reference to the Council of Europe 1981 Convention for the Protection of individuals with regard to Automatic Processing of Personal Data in the preamble. Rules on purpose limitations are laid down.	EU 27

[50] Agreement on mutual legal assistance between the European Union and the United States of America, OJ L 181, 19.7.2003, p. 34; Council decision of 6 June 2003 concerning the signature of the Agreements between the European Union and the United States of America on extradition and mutual legal assistance in criminal matters, OJ L 181, 19.7.2003, p. 25.

[51] Council Common Position 2005/69/JHA of 24 January 2005 on exchanging certain data with Interpol, OJ L 27, 29.1.2005, p. 61.

[52] Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences, OJ L 253, 29.9.2005, p. 22.

[53] Council Decision 2005/876/JHA of 21 November 2005 on the exchange of information extracted from the criminal record, OJ L 322/33, 9.12.2005, p. 33.

	Cited Legal base	Instrument	Stated Purpose	Exchange of information on	Involved authorities	Data protection elements	Participating States
Prevention and combating of crime (2006)[54]	Non specified reference to article 30 TEU	Council recommendation	The progressive establishment of an area of freedom, security and justice by developing common action among member states in the field of police and judicial cooperation in criminal matters. To promote and ensure high level of liaison and cooperation between police forces, customs authorities and other competent authorities for the prevention and combating of crime. To achieve this, member states are encouraged to conclude agreements or other arrangements at national level.	"…relevant information and strategic, tactical and operational intelligence, where appropriate, in particular by facilitating mutual direct or indirect access to databases…"	Police forces, customs authorities and other competent authorities in relation to the prevention and combating of crime.	"…with due regard for individual rights and data protection rules."	EU 27
Simplifying exchange between law enforcement authorities between member states (2006)[55]	Arts. 30 (1) (a) and (b), 34 (2) (b) TEU	Council Framework Decision	To provide citizens with a high level of security within in an area of freedom, security and justice. To establish rules for effective and expeditious exchange of existing information and intelligence for the purpose of conducting criminal investigations or criminal intelligence operations.	Any type of information or data which is held by law enforcement authorities as well as any type of information or data which is held by public authorities or by private entities and which is available to law enforcement authorities without the taking of coercive measures.	Competent authorities of member states, defined as: a national police, customs or other authority that is authorised by national law to detect, prevent and investigate offences or criminal activities and to exercise authority and take coercive measures in the context of such activities. Agencies or units dealing especially with national security issues are not covered by the concept of competent law enforcement authority (member states' practice of consigning competent authorities to the Council Secretariat differs considerably, see Annex 2 of this paper). Europol, Eurojust. Exchange is allowed via any existing channel for international law enforcement cooperation.	Reference to the "established rules on data protection", when using the communication channels. Reference to national law of the receiving state as regards the use of data which has been exchanged. Reference to the Council of Europe 1981 Convention for the Protection of individuals with regard to Automatic Processing of Personal Data. Rules on purpose limitations are laid down. Rules on confidentiality and withholding data. Information exchange can be refused, e.g. if this would be clearly disproportionate for the purposes for which it is requested.	EU 27 plus Norway and Iceland. Switzerland and Liechtenstein soon.

[54] Council Recommendation of 27 April 2006 on the drawing up of agreements between police, customs and other specialised law enforcement services in relation to the prevention and combating of crime, OJ C 124, 25.5.2006, p. 1.
[55] Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, OJ L 386, 29.12.2006, p. 89.

	Cited Legal base	Instrument	Stated Purpose	Exchange of information on	Involved authorities	Data protection elements	Participating States
Terrorist kidnappings (2007)[56]	None provided	Council Recommendation	To successfully resolve situations of kidnappings by groups/individuals that can be placed within the spectrum of international terrorism.	Data on terrorist kidnappings (after a terrorist kidnapping has been resolved), including country and region in which the kidnapping took place, number and nationality of hostages, time and date of kidnapping, time and date of the end of the incident, perpetrators/responsible terrorist group, modus operandi of the kidnapping, motivation for the kidnapping, involvement of a mediator, hostages' reason for being in the country, language skills of the perpetrators, means used by the perpetrators to address the public, details on the modus operandi.	Member states through "bureau de liaison secure network channel". Europol (with a view of possibly setting up a database at Europol).	Reference to national law is made.	EU 27
Expulsion of third-country nationals (2007)[57]	None provided	Council Resolution	Combating terrorism, radicalisation and recruitment to terrorism.	Third-Country nationals who are subject to an expulsion decision issued by an administrative or judicial authority of a member state on the grounds of behaviour linked to terrorist activities or constituting acts of explicit and deliberate provocation of discrimination, hatred or violence against a specific individual or group of individuals.	Competent authorities of member states through the "bureau de liaison secure network channel"	Neither reference to data protection standards nor to fundamental rights in general.	EU 27
Cooperation of Asset Recovery Offices (2007)[58]	Arts. 30 (1)(a) and (b), 34(2) (c) TEU	Council Decision	To investigate and analyse financial trails of criminal activity in order to combat organised crime effectively.	Information for the purposes of the facilitation of the tracing and identification of proceeds of crime and other crime related property which may become the object of a freezing, seizure or confiscation order made by a competent judicial authority. This entails details on the property targeted or sought and/or the natural or legal persons presumed to be involved.	Asset Recovery Services, to be set up or designated by member states.	Reference to "established rules on data protection" as well as Council of Europe standards. Exchange shall take place under the procedures and conditions of Framework Decision 2006/960/JHA of 18 December 2006. Reference to national data protection laws.	EU 27

[56] Council Recommendation of 12 June 2007 concerning sharing of information on terrorist kidnappings, OJ L 214, 17.8.2007, p. 9.

[57] Council Resolution on information exchange on the expulsion of third-country nationals due to behaviour related to terrorist activity or inciting violence or racial hatred, adopted at the JHA Council meeting of 19.-20.4.2007, Council doc. 7159/07, 22.3.2007 and 8364/07 (Presse 77), p. 39.

[58] Council Decision 2007/845/JHA of 6 December 2007 concerning cooperation between Asset Recovery Offices of the Member States in the field of tracing and identification of proceeds from, or other property related to, crime, OJ L 332, 18.12.2007, p. 103.

II.2. Legislative proposals and possible further steps

	Cited legal base	Proposed Instrument	Proposed Purpose	Proposed exchange of information on/access to	Proposed involved authorities	Proposed data protections rules	Proposed participating States
Proposal: Principle of availability (2005)[59]	Arts. 30(1)(b) and 34 (2)(b) TEU	Council Framework Decision	To provide citizens with a high level of security within an area of freedom, security and justice by developing common action among member states in the field of police and judicial cooperation. To lay down an obligation for member states to give access to or provide certain types of information available to their authorities to equivalent authorities of other member states and Europol in so far as these authorities need this information to fulfil their lawful tasks for the prevention, detection or investigation of criminal offences prior to the commencement of a criminal procedure. Extend online access to national databases to all equivalent authorities of member states and Europol (at least online access to indices).	• DNA analysis files • Dactyloscopic (fingerprint) data • Ballistics • Vehicle registration data • Telephone numbers and other communication data (not content or traffic data, in principle) • Minimum data for the identification of persons contained in civil registers**.**	Equivalent competent authorities in member states and Europol. Competent authorities are those national authorities which are covered by Art. 29 TEU (i.e. "police forces, customs authorities and other competent authorities").The equivalence of authorities will be determined in a special procedure based on the specific type of information and the notified list of competent authorities in member states. Exchange via national contact points.	Reference to privacy rights and data protection requirements. Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation would govern the application of the proposal and would provide common, EU wide standards. Purpose limitation foreseen (prevention, detection or investigation of the criminal offence for which the information is provided). Verification of quality of information necessary. Protection of fundamental rights and freedoms can justify the refusal to provide information. Data subject's rights of access to information provided.	EU 27
Proposal: Organisation and content of the exchange of information extracted from criminal records (2005)[60] Note: This proposal is intended to repeal the decision listed above under II.1. on the exchange of information extracted from the criminal records.	Arts. 31 and 34(2)(b)	Council Framework Decision	Offering citizens a high level of safety in the area of freedom, security and justice. a) to define the ways in which a Member State in which a conviction is handed down against a national of another Member State may transmit such a conviction to the Member State of the convicted person's nationality b) to define storage obligations for the Member State of the person's nationality and to specify the methods to be followed when responding to a request for information taken from criminal records; c) to lay down the framework for a computerised conviction-information exchange system between Member States to be built and developed.	Criminal convictions of EU citizens.	One or more unspecified "central authority" in each member state	Reference to Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation. Reference to the Council of Europe Recommendation No R (84) on criminal records and rehabilitation of convicted persons as regards purpose limitation. Specific rules on purpose limitations are laid down.	EU 27

[59] Proposal for a Council Framework Decision on the exchange of information under the principle of availability, COM(2005) 490 final, 12.10.2005.

[60] Proposal for a Council Framework Decision on the organisation and content of the exchange of information extracted from criminal records, COM(2005) 690 final, 22.12.2005.

	Cited legal base	Proposed Instrument	Proposed Purpose	Proposed exchange of information on/access to	Proposed involved authorities	Proposed data protections rules	Proposed participating States
Proposal: Stepping up cross-border co-operation (Prüm Initiative, 2007)[61]	Arts. 30(1)(a) and (b), 31(1)(a), 32 and 34 (2)(c) TEU	Council Decision	Giving citizens a high degree of security by developing common procedures among member states in the field of police and judicial cooperation in criminal matters. Making the essential parts of the Prüm Treaty of 27 May 2005 applicable to all member states. Open a new dimension of crime fighting by networking member states national databases.	• **DNA analysis files** for investigation of criminal offences (hit/no hit system). • **Dactyloscopic (fingerprint) data** for prevention and investigation of criminal offences (hit/no hit system). • **Vehicle registration data** for prevention and investigation of criminal offences and in dealing with other offences coming within the jurisdiction of the courts or the public prosecution service in the searching member state, as well as in maintaining public order and security. • Exchange of personal and non-personal data in connection with **major events** with a cross-border dimension for prevention of criminal offences and in maintaining public order and security for major events with a cross-border dimension, in particular sporting events or European Council meetings (sic!). • Exchange of personal information for the prevention of **terrorist offences** in so far as necessary because particular circumstances give reason to believe that the data subjects will commit terrorist offences as defined in the Council Framework decision of 13 June 2002 on combating terrorism.	National contact points designated by member states. The powers of contact points shall be governed by applicable national law. Agencies responsible for the prevention and investigation of criminal offences.	Reference to privacy rights and data protection requirements. Special, extensive set of rules on data protection, including purpose limitations, accuracy, current relevance, etc. Information rights, complaint mechanisms and damage claims of the data subject must be provided. Reference to directive 95/46/EC (i.e. "first pillar" data protection rules!) is made in this regard. Involved authorities must ensure that data is protected against accidental or unauthorised destruction, accidental loss, unauthorised access, unauthorised or accidental alteration and unauthorised disclosure. Only specially authorised officers of national contact points may carry out automated searches. Implementing rules must guarantee that "state-of-the-art technical measures are taken to ensure data protection and data security, in particular data confidentiality and integrity". Supply of personal data is made conditional on the fact that the level of data protection in participating member state is at least equal to the Council of Europe standards. The existence of this level of protection will need to be formally acknowledged by a unanimous Council decision for each member state. Allowed storage time is linked to specific purposes; maximum period for keeping data is determined by national law of the supplying member state. Data supplied in the context of major events can only be used for the specific event and must be deleted once the purposes have been achieved or can no longer be achieved (max. 1 year).	EU 27

[61] Initiative of the Kingdom of Belgium, […] with a view to adopting a Council Decision on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ C 71, 28.3.2007, p. 35.

III. Common rules on exchange of information genuinely gathered by private parties

III.1. Enacted legislation as of 31.3.2008

	Cited legal base	Instrument	Stated Purpose	Gathering and exchanging information on X held by Y	Involved authorities	Data protection elements	Time limits for storage	Participating states
Passenger data[62]	Arts. 62(2)(a) and 63(3)(b) TEC	Council Directive	Improving border controls and combating illegal immigration.	Advance passenger data, • number and type of travel document used, • nationality, • full names, • date of birth, • border crossing point of entry into the territory of the member states, • code of transport, • departure and arrival time of the transportation, • total number of passengers carried on that transport, • initial point of embarkation. "Carriers" must transmit advance passenger data by the end of check-in concerning the passengers they will carry to an authorised border crossing point through which the passenger will enter the territory of a member state. Carriers are defined as any natural or legal person whose occupation it is to provide passenger transport by air.	Authorities responsible for carrying out checks on persons at external borders. Personal data may also be used for law enforcement purposes (subject to data protection provisions of directive 95/46 – first pillar data protection directive).	Directive 95/46/EC (i.e. "first pillar" data protection directive) is applicable. National data protection rules. Passengers must be informed by carriers about data storage and use	Data are saved in a temporary file by the border authorities of the border crossing point through which the passenger will enter the territory of a member state. After passengers have entered, the data must be deleted by the authorities within 24 hours, unless the data are needed later for the purposes of carrying out the statutory functions of the border authorities. Within 24 hours of the arrival of the means of transportation, carriers must delete the data.	EU-26 (not Denmark) plus Norway and Iceland. Switzerland and Liechtenstein soon.
Data retention[63]	Art. 95 TEC	European Parliament and Council Directive	Harmonising member states' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purposes of the investigation, detection and prosecution of serious crime, as defined by each member state in national law.	Traffic and location data (including unsuccessful call attempts) on legal entities and natural persons and the related data necessary to identify the subscriber or user generated or processed by providers of publicly available electronic communications services or by public communications networks. The content of the communication is not stored. For more details on the categories of data, see Art. 5 of the directive.	Competent national authorities in specific cases and in accordance with national law.	Procedure and conditions for accessing the retained data by national authorities shall be defined by each member state but must be in accordance with the principles of necessity and proportionality, EU and international public law, in particular the ECHR. Directive 95/46/EC (i.e. "first pillar" data protection directive) is applicable. Member states must ensure that private communication companies respect certain data security principles, which are further defined in the directive. Member states must designate independent supervisory authorities.	Not less than six months and not more than 2 years.	EU 27

[62] Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, OJ L 261, 6.8.2004, p. 24.

	Cited legal base	Instrument	Stated Purpose	Gathering and exchanging information on X held by Y	Involved authorities	Data protection elements	Time limits for storage	Participating states
EU-Canada PNR agreement[64]	Arts. 95, 300(2) and 300(3) TEC	International Agreement/Council Decision	To ensure that API/PNR data of persons on eligible journeys is provided in full respect of fundamental rights and freedoms, in particular the right to privacy.	Advance Passenger Information (API) and Passenger Name Record (PNR) data contained in reservation systems of air carriers located within the Community that operate flights from the Community to Canada. API data elements include among others: • A person's names • Date of birth • Gender • Citizenship/nationality • Type, issuing country and number of travel document PNR data elements include among others: • Name • API data • Date of intended travel • Date of reservation • Date of ticket issuance • Travel agencies • Travel agent • Contact telephone information • Billing address • All forms of payment information • Travel itinerary • Travel status of passenger • Ticketing information • Bag tag numbers • Seat information, including seat number • all historical changes Sensitive data (e.g. racial or ethnic origin, political opinions, religious or philosophical beliefs, etc) will not be gathered.	Authorities responsible in Canada or in the EU for processing API/PNR data. In Canada: Canada Border Services Agency (CBSA). Under certain circumstances and in a limited way, data may be disclosed to other Canadian departments, agencies and also third states.	Data will be processed in accordance with applicable laws and constitutional requirements and without unlawful discrimination. Legally binding rules on access to data by data subject, correction and notation. Joint reviews of the implementation of the agreement on an annual basis. First pillar data protection directive 95/46/EC of 24.10.1995 is applicable. That entails that an assessment had to be made whether Canada ensures an adequate level of data protection and whether member state laws comply with the directive on certain other points. This positive assessment was concluded with Commission decision of 6 September 2005. The Agreement itself contains rules on access and correction requests of data by data subjects.	In principle, the maximum storage time of personal data is 3.5 years. If the data relates to a person that is under investigation for terrorism, terrorism-related crime or other serious crimes that are transnational in nature (e.g. organized crime), the data may be stored for a longer period, however, usually for not more than six years.	EU 27 and Canada

[63] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provisions of publicly available electronic communications services or public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, p. 54.

[64] Council Decision of 18 July 2005 on the conclusion of an Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record data, OJ L 82, 21.3.2005, p. 14; Commission decision of 6 September 2005 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the Canada Border Services Agency, OJ L 91, 29.3.2006 p. 49.

	Cited legal base	Instrument	Stated Purpose	Gathering and exchanging information on X held by Y	Involved authorities	Data protection elements	Time limits for storage	Participating states
EU-US PNR agreement[65]	Arts. 24 and 38 TEU	International Agreement/ Exchange of letters/ Council Decision	To prevent and combat terrorism and transnational effectively as a means of protecting the EU's and the US's democratic societies and common values	Passenger Name Record data contained in reservation systems of air carriers located within the EU that operate passenger flights in foreign air transportation to or from the US. Transfer will be automated (push/pull system). Types of PNR Data include among others: • Date of reservation/issue of ticket • Dates of intended travel • Names • Available frequent flyer and benefit information • All available contact information • All available payment/billing information • Travel itinerary • Travel agency • Travel status of passenger • Ticketing information • All baggage information • Seat information, including seat number • All historical changes	US Department of Homeland Security. Analytical information flowing from PNR may be exchanged between US and member states' police and judicial authorities as well as Europol and Eurojust.	General reference to fundamental rights and freedoms, notably privacy, to a shared common basis of US and European privacy laws, Article 6(2) TEU and respect for fundamental rights and data protection as well as to the Privacy Act of 1974 in preamble of Agreement. Data will be processed in accordance with US laws and constitutional requirements and without unlawful discrimination. Periodical review of the implementation of the system by a specifically designated person. DHS is deemed to ensure an adequate level of protection for PNR data transferred from the EU and EU will therefore not interfere with relationships between the US and third countries for the exchange of passenger information on data protection grounds. Further details are provided in a legally non binding Letter of Assurances for the protection of PNR data by the US Department of Homeland Security (DHS). Included in this letter are, inter alia the following elements: • Purpose specification • Access to data by data subjects • Obligation to promptly delete sensitive data (racial or ethnic origin, political opinions, religious or philosophical beliefs, etc), in principle. In exceptional cases, however, DHS may use such sensitive data. • Time limits for storage of data as provided in previous column. • Information to the travelling public about processing of data.	7 years in active analytical database. After the active phase, data will be moved for 8 years into a dormant, non-operational status. Once in dormant status data can only be activated by certain officials and in exceptional circumstances. But: no definite maximum period of data retention agreed.	EU 27 and USA

[65] Council Decision 2007/551/CFSP/JHA of 23 July 2007 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS), OJ L 204, 4.8.2007, p. 16.

III.2. Legislative proposals and possible future steps

	Cited legal base	Proposed instrument	Proposed Purpose	Proposed gathering and exchanging information on X held by Y	Proposed Involved authorities	Proposed data protection elements	Proposed time limits for storage	Proposed participating states
EU-PNR proposal[66]	Arts. 29, 30 (1)(b) and 34 (2)(b) TEU	Council Framework Decision	To offer a high level of security and protection within an area of freedom, security and justice: This Framework Decision provides for the making available by air carriers of PNR data of passengers of international flights to the competent authorities of the member states, for the purpose of preventing and combating terrorist offences and organised crime, as well as the collection and retention of those data by these authorities and the exchange of those data between them.	PNR data collected and processed in air carriers' reservation systems by air carriers operating international flights to or from the territory of one or more member states of the EU (no intra-EU flights). "Push system" is the preferred method and should be mandatory for all carriers established in the EU. PNR data include among others: Data for all passengers • Date of reservation/issue of ticket • Date(s) of intended travel • Name (s) • Address and Contact information (telephone number, e-mail address) • All forms of payment information, including billing address • All travel itinerary for specific PNR • Frequent flyer information • Travel agency /Travel agent • Travel status of passenger including confirmations, check-in status, no show or go show information • Ticketing field information, including ticket number, date of ticket issuance and one-way tickets, Automated Ticket Fare Quote fields • Seat number and other seat information • All baggage information • Number and other names of travellers on PNR • All historical changes Additional data for unaccompanied minors under 18 years • Name and gender of child • Age • Language(s) spoken • Name and contact details of guardian on departure and relationship to the child • Name and contact details of guardian on arrival and relationship to the child • Departure and arrival agent Sensitive data (e.g. racial or ethnic origin, political opinions, religious or philosophical beliefs, etc) will have to be deleted by the collecting authority (see next column) immediately.	A Passenger Information Unit (PIU) for each member state (two or more member states may establish joint PIUs), responsible for collecting PNR data and for carrying out risk assessments of passengers. PIUs then transmit the PNR data of passengers "requiring further examination" to the relevant competent authorities of the same member state. Competent authorities shall only include authorities responsible for the prevention or combating of terrorist offences and organised crime. Each member state shall adopt a list of the authorities entitled to receive PNR data from the PIU. Passenger Information Units of member states are allowed to exchange PNR data among themselves, to transmit it to 'their' competent authorities and to request it from each other. Under certain conditions law enforcement authorities of third member states may receive PNR data from member states.	Reference to privacy rights and data protection requirements. Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation would govern the application of the proposal and would provide common, EU wide standards. Rules on purpose limitation and data security provided in the proposal. Air carriers must inform passengers about the transmission of PNR data to the PIUs, the purposes of their processing, period of data retention, possible further uses, including exchanging and sharing of the data.	5 years in active analytical database. After the active phase, data will be moved for 8 years into a dormant, non-operational status. Once in dormant status data can only be activated by certain officials and in exceptional circumstances. Upon the expiry of this 8 year period, the data should be deleted. <u>However</u>: In case the data is being used for an ongoing criminal investigation of a terrorist offence or an organised crime against or involving the data subject, the data can be stored longer and must only be deleted once the investigation is concluded.	EU 27

[66] Commission Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, COM(2007) 654 final, 6.11.2007.

	Cited legal base	Proposed instrument	Proposed Purpose	Proposed gathering and exchanging information on X held by Y	Proposed Involved authorities	Proposed data protection elements	Proposed time limits for storage	Proposed participating states
	Aim and content of proposals/possible future steps							
EU-Australia PNR agreement	Following a recommendation of the Commission, the Council is currently debating negotiation guidelines for the Commission in order conclude a PNR agreement with Australian authorities. All Council documents on this matter are restricted[67]							
EU-South Korea PNR agreement	Apparently, as of 1 March 2008 European air carriers have to transfer passenger data (22 data elements) to South-Korean authorities based on bilateral agreements between the affected air carriers and South Korea. Interrogated by MEPs about a possible common EU framework in this respect, the Council replied that it has so far not been asked by a member state, the Commission or South Korea itself to negotiate a PNR agreement with South Korea.[68]							

[67] Council of the European Union, Recommendation from the Commission to the Council to authorise opening of negotiations for an agreement with Australia on the use of passenger name record (PNR) data to prevent and combat terrorism and related transnational crime, including organised crime, restricted Council doc. 13742/07, 10.10.2007; Council of the European Union, Draft negotiation guidelines for an agreement with Australia on the use of passenger name record (PNR) data to prevent and combat terrorism and related transnational crime, including organised crime, restricted Council doc. 5861/08, 15.2.2008.

[68] Letter from Peter Schaar on behalf of the Article 29 Data Protection Working Party to Minister of Justice Dr. Alberto Costa, 26.11.2007; European Parliament, Written Question by Sophia in 't Veld and Alexander Alvaro to the Council, PNR and South Korea, E-6007/07, 6.12.2007 with reply dated 30.1.2008.

Annex 2. The concept of "competent authority"

The following table provides an illustration of member states' practice in designating national "competent authorities" deemed to participate in EU systems of information exchange. The information is taken directly from the notifications made by member states.

Source: Public register of documents on the Council website, last accessed 31.3.2008.

Exemplary system:

Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union (OJ L 386, 29.12.2006, p. 89) is taken.

Article 2a of said framework decision provides:

> "'competent law enforcement authority': a national police, customs or other authority that is authorised by national law to detect, prevent and investigate offences or criminal activities and to exercise authority and take coercive measures in the context of such activities. Agencies or units dealing especially with national security issues are not covered by the concept of competent law enforcement authority. Every Member State shall, by 18 December 2007, state in a declaration deposited with the General Secretariat of the Council which authorities are covered by the concept of 'competent law enforcement authority'. Such a declaration may be modified at any time."

	National authorities designated as "competent law enforcement authority"	**Date of receipt (Council)**	**Council document number**
Belgium	n/a		
Bulgaria	National Police Service of the Ministry of the Interior.	21.12.2007	5023/08
Czech Republic	1. Customs Administration of the Czech Republic 2. Public prosecutors 3. Police bodies – in accordance with § 12 (2) of the Penal Code of the Czech Republic this notion covers following authorities: Police bodies mean the division of the Police of the Czech Republic and the division of the Ministry of Interior for inspection activity in criminal proceedings on crimes committed by policemen. The same position in criminal proceedings have entrusted bodies of Military Police regarding the members of armed forces, entrusted bodies of Prison Service of the Czech Republic in criminal proceedings regarding the members of the said Prison Service, and entrusted bodies of Security Information Service in criminal proceedings regarding the members of Security Information Service and entrusted bodies of the Office for Foreign Relations and Information in criminal proceedings of the members of this Office. Entrusted Customs bodies have also the position of police bodies in criminal proceedings regarding the crimes committed by violation of customs regulations and regulations of import, export or transit of goods, even in the event that these crimes are committed by members of armed forces or armed corps or services and also in cases of violation of legal regulations in cases of acquisition and placement of goods within the Member States of the European Community, in case that this goods is transported across the state borders of the Czech Republic, and in cases of violation of tax regulations, if custom bodies are the tax administrators in accordance with particular legal regulations. If not specified otherwise hereinafter, the said bodies are authorised to carry out all the acts of the criminal proceedings belonging to the competence of the police body.	20.12.2007	5004/08
Denmark	n/a		
Germany	n/a		
Estonia	n/a		
Greece	n/a		
Spain	Centro nacional de comunicaciones internacionales (Unidad de Cooperación Policial Internacional de la Comisaría General de Policial Judicial)	29.1.2008	5916/08

	National authorities designated as "competent law enforcement authority"	Date of receipt (Council)	Council document number
France	n/a		
Iceland	National Police Commissioner of Iceland	15.1.2008	5663/08
Ireland	1. An Garda Síochána 2. The Revenue Commissioners	19.12.2007	5337/08
Italy	International Police Cooperation Department in the Central Criminal Police Directorate of the Public Security Department at the Ministry of the Interior (Servizio per la Cooperazione Internazionale di Polizia della Direzione Centrale della Polizia Criminale del Dipartimento della Pubblica Sicurezza del Ministero dell'Interno).	21.12.2007	6181/1/08 REV 1
Cyprus	1. Unit for Combating Money Laundering (M.O.K.A.S), 2. Cyprus Police, European Union and International Police Cooperation Directorate, 3. Customs & Excise Department	8.1.2008	5545/08
Latvia	1. State Police, authority entitled to investigate any criminal offence, with exceptions for specialised law enforcement agencies 2. Security Police, investigate criminal offences that have been performed in the field of State security or in State security institutions, or other criminal offences within the framework of the competence thereof 3. Fiscal Police, investigate criminal offences in the field of State revenue and in the actions of officials and employees of the State Revenue Service. 4. Military Police, criminal offences committed in the military service and in military units, or in the places of deployment thereof, as well as criminal offences committed in connection with the execution of official duties by soldiers, national guardsmen, or civilians working in military units. 5. the Prisons Administration criminal offences committed by detained or convicted persons, or by employees of the Prisons Administration in places of imprisonment. 6. the Corruption Prevention and Combating Bureau shall investigate criminal offences that are related to violations of the provisions of the financing of political organisations (parties) and the associations thereof, and criminal offences in the State Authority Service, if such offences are related to corruption 7. customs authorities, investigate matters of smuggling. 8. the State Border Guard, investigate criminal offences that are related to the illegal crossing of the State border, the illegal transportation of a person across the State border, or illegal residence in the State, as well as criminal offences committed by a border guard as a State official. 9. Captains of seagoing vessels at sea shall investigate criminal offences committed on vessels of the Republic of Latvia. 10. The commander of a unit of the Latvian National Armed Forces shall investigate criminal offences committed by the soldiers of such unit, or that have been committed at the location of the deployment of such unit (in the closed territory of the place of residence), if the relevant investigative institutions of the foreign state are not investigating such offences; 11. a public prosecutor – directing the proceedings in a criminal prosecution; 12. a judge who leads the adjudication – directing the proceedings in preparing a case for trial, as well as from the moment when a adjudication is announced with which legal proceedings are completed in the court of the relevant instance, until the transferral of the case to the next court instance or until the execution of the adjudication; 13. the composition of a court – directing the proceedings during a trial. According to the national law these institutions are authorised to carry out investigations and they are entitled to receive data (personal data) from all data systems. Within their competence operational activities (intelligence) is entitled to perform State Police, Security Police, Fiscal Police, Military Police, Prisons Administration, Corruption Prevention and Combating Bureau, customs authorities and State Border Guard.	19.12.2007	5002/08

	National authorities designated as "competent law enforcement authority"	Date of receipt (Council)	Council document number
Lithuania	1. Financial Crime Investigation Service under the Ministry of the Interior, 2. Lithuanian Police, 3. Special Investigation Service of the Republic of Lithuania 4. Military Police of the Lithuanian Armed Forces, 5. Customs Department under the Ministry of Finance 6. Government Security Department under the Ministry of the Interior, 7. State Border Guard Service under the Ministry of the Interior,	30.1.2008	6261/08
Luxembourg	n/a		
Hungary	1. The Hungarian Police; 2. The Hungarian Prosecution Service; 3. The Hungarian Customs and Finance Guard; 4. The Protective Service of Law Enforcement Agencies; 5. The Hungarian Border Guard (please note that, as of 1/1/2008, the Hungarian Border Guard will be integrated into the Hungarian Police).	22.2.2208	7004/08
Malta	Malta Police Force	22.2.2008	6931/1/08 REV 1
Netherlands	n/a		
Norway	National Police, authority entitled to investigate any criminal offence.	20.2.2008	6910/08
Austria	1. The Federal Ministry of the Interior, Directorate General for Public Security (Bundesministerium für Inneres, Generaldirektion für die öffentliche Sicherheit) 2. The security directorates 3. The district administrative authorities 4. The federal police directorates 5. The Federal Ministry of Finance, Unit IV/3, for customs and tax matters	19.12.2007	5003/08
Poland	1. Internal Security Agency, 2. Central Anticorruption Bureau, 3. Public Prosecutor's Office, 4. Police, 5. Polish Border Guard, 6. Customs Service, 7. Military Police.	31.1.2008	6350/08
Portugal	n/a		
Romania	Ministry of Internal Affairs and Administrative Reform, which includes the Police, the Border Police, the Gendarmerie and the International Police Cooperation Centre as structures which collect and process information and intelligence within the meaning of the Framework Decision.	18.12.2007	5178/08
Slovenia	n/a		
Slovakia	1. Police Force 2. Railway Police 3. Military Police 4. Customs Criminal Office	17.12.2007	5990/08
Finland	n/a		
Sweden	n/a		
United Kingdom	1. All police forces in England, Wales, Scotland and Northern Ireland 2. Serious Organised Crime Agency (SOCA), 3. Her Majesty's Revenue and Customs (HMRC), 4. Border and Immigration Agency, 5. Serious Fraud Office, 6. Scottish Crime and Drug Enforcement Agency (SCDEA).	18.12.2007	5612/08

References

Bigo, D. (ed.) (2007), *The field of the EU internal security agencies*, L'Harmattan/Centre d'Etudes sur les Conflits: Paris.

Bigo, D. and Carrera, S. (2004), *From New York to Madrid: Technology as the Ultra-Solution to the Permanent State of Fear and Emergency in the EU*, CEPS Commentary.

Bonditti, P. (2007), 'Biometrics and surveillance', in Bigo, D. (ed.), *The field of the EU internal security agencies*, L'Harmattan/Centre d'Etudes sur les Conflits: Paris, 2007, pp. 97 - 114.

Commission of the European Communities (2008), Commission Staff Working Document, Accompanying document to the Communication, Preparing the next steps in border management in the European Union, SEC(2008) 153, 13.2.2008.

Commission of the European Communities (2007a), Report from the Commission to the European Parliament and the Council on the evaluation of the Dublin system, COM(2007) 299 final, 6.6.2007.

Commission of the European Communities (2007b), Commission Staff Working Document, Annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit in 2006, SEC(2007) 1184 final, 11.9.2007.

Commission of the European Communities (2007c), Commission Staff Working Document, Accompanying document to the Proposal for a Council Decision on the installation, operation and management of a Communication Infrastructure for the Schengen Information System (SIS) environment (…), SEC(2007) 809, 11.6.2007.

Commission of the European Communities (2005a), Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the second generation Schengen information system (SIS II), COM(2005) 236 final, 31.5.2005.

Commission of the European Communities (2005b), Communication on improved effectiveness, enhanced interoperability, and synergies among European databases in the area of Justice and Home Affairs, COM(2005) 597 final, 24.11.2005, p. 8

Commission of the European Communities (2004), Proposal for a Regulation of the European Parliament and of the Council concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas, COM(2004) 835 final, 28.12.2004.

Council of the European Union (2008), SIS database statistics dd. 01/01/2008, Council doc. 5441/08, 30.1.2008.

Council of the European Union (2007a), Information Sheet, Enlargement of the Schengen Area, REV 1, 8.11.2007.

Council of the European Union (2007b), Proposal for the report from the High Contracting Parties to the Agreement related to the application of the CIS Convention, exercising the functions attributed to the Committee provided for in Article 16 of the CIS Convention, Council doc. 14694/2/06 REV 2, 12.1.2007.

Counter-terrorism Coordinator (2007), Implementation of the EU Counter-terrorism strategy - Discussion paper, Council doc. 15448/07, 23.11.2007.

Eurojust (2007), Eurojust Annual Report 2006, Council doc. 7550/07, 21.3.2007.

European Data Protection Supervisor, EDPS (2007), EURODAC Supervision Coordination Group, Report of the first coordinated inspection, 17.7.2007.

Europol (2007), Europol Annual Report 2006, File no. 1423-45r1, 21.3.2007.

Guild, E. and Carrera, S. (2005), *No Constitutional Treaty?*, CEPS Working Document No. 231, Centre for European Policy Studies: Brussels.

House of Lords (2007), Schengen Information System II (SIS II), Report with Evidence, 9th Report of Session 2006-07, HL Paper 49, March 2007.

Further Readings

Aus, J. P., *Eurodac: A solution looking for a problem?*, Arena Working Paper No. 09, Arena Centre for European Studies: Oslo, 2006.

Balzacq, T., 'The policy tools of securitization: Information exchange, EU foreign and interior policies', *Journal for Common Market Studies*, vol. 46 no. 1, 2008, pp. 75-100.

Balzacq, T. and Carrera, S., *The EU's Fight against International Terrorism - Security Problems, Insecure Solutions*, CEPS Policy Brief No. 80, Centre for European Policy Studies: Brussels, July 2005.

Balzacq, T. and Carrera, S., *Migration, Borders and Asylum – Trends and Vulnerabilities in EU Policy*, Centre for European Policy Studies: Brussels, 2005.

Bigo, D., Carrera, S. and Guild, E., *What Future for the Area of Freedom, Security and Justice? Recommendations on EU Migration and Borders Policies in a Globalising World*, CEPS Policy Brief No. 156, Centre for European Policy Studies: Brussels, March 2008.

Bigo, D., Carrera, S., Guild, E. and Walker, R. B. J., *The Changing Landscape of European Liberty and Security: Mid-Term Report on the Results of the CHALLENGE Project*, CHALLENGE Research Paper No. 4, Centre for European Policy Studies: Brussels, February 2007.

Bigo, D., *The Principle of Availability*, Briefing Paper, European Parliament, DG Internal Policies, Policy Unit C – Citizens' rights and constitutional affairs, January 2006.

Broeders, D., 'The new digital borders of Europe: EU databases and surveillance of irregular migrants', *International Sociology*, vol. 22, no. 1, 2007, pp. 71 – 92.

Brouwer, E., *The other side of Moon - The Schengen Information System and Human Rights: A Task for National Courts*, CEPS Working Document No. 288, Centre for European Policy Studies: Brussels, April 2008.

Brouwer, E., *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System*, Wolf Legal Publishers: Nijmegen, 2007.

Brouwer, E., 'Data surveillance and border control in the EU: Balancing efficiency and legal protection', in Balzacq, T. and Carrera, S. (eds), *Security versus Freedom? A Challenge for Europe's Future*, Ashgate: Aldershot, 2006, pp. 137 - 154.

Carrera, S. and Geyer, F., 'The Reform Treaty and Justice and Home Affairs – Implications for the *common* Area of Freedom, Security and Justice', in Guild, E. and Geyer, F. (eds), *Security versus Justice? Police and Judicial Cooperation in the European Union*, Ashgate: Aldershot, 2008, pp. 289 - 307.

De Hert, Paul, *What are the risks and what guarantees need to be put in place in view of interoperability of police databases?*, Briefing Paper, European Parliament, DG Internal Policies, Policy Unit C – Citizens' rights and constitutional affairs, February 2006.

European Data Protection Supervisor, Preliminary comments on the Commission's Border Package, 3.3.2008.

European Data Protection Supervisor, Opinion on the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, 20.12.2007.

European Data Protection Supervisor, Opinion on the Initiative of the Federal Republic of Germany, with a view to adopting a Council Decision on the implementation of Decision 2007/…/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, 19.12.2007

Frattini, F., *Data protection in the area of justice, freedom and security*, Meeting with the Joint Supervisory Authorities under the Third Pillar, SPEECH/04/549, Brussels, 21.12.2004.

Garside, A., *The political genesis and the legal impact of proposals for the SIS II: what cost for data protection and security in the EU*, Sussex Migration Working Paper No. 30, Sussex Centre for Migration Research, March 2006.

Guild, E., Carrera S. and Geyer, F., *The Commission's new Border Package: Does it take us one step closer to 'Cyber Fortress Europe'?*, CEPS Policy Brief No. 154, Centre for European Policy Studies: Brussels, March 2008.

Guild, E. and Brouwer, E., The political life of data - The ECJ Decision on the PNR Agreement between the EU and the US, CEPS Policy Brief No. 109, Centre for European Policy Studies: Brussels, July 2006.

Guild, E., *Moving the borders of Europe*, Publicaties Faculteit der Rechtsgeleerdheid, KU Nijmegen no. 14, 2001.

Hobbing, P., *A comparison of the now agreed VIS package and the US-VISIT system*, Briefing Paper, European Parliament, DG Internal Policies, Policy Unit C – Citizens' rights and constitutional affairs, July 2007.

Hobbing, P., *An assessment of the proposals of regulation and decision which define the purpose, functionality and responsibilities of the future SIS II*, Briefing Paper, European Parliament, DG Internal Policies, Policy Unit C – Citizens' rights and constitutional affairs, February 2006.

Hobbing, P., *An analysis of the Commission Communication on improved effectiveness, enhanced operability and synergies among European databases in the area of Justice and Home Affairs*, Briefing Paper, European Parliament, DG Internal Policies, Policy Unit C – Citizens' rights and constitutional affairs, February 2006.

Liberatore, A., *Balancing Security and Democracy: The politics of biometric identification in the European Union*, EUI Working Papers No. 2005/30, European University Institute: San Domenico di Fiesole, 2005.

Lodge, J. (ed.), *Are You Who You Say You Are? The EU and Biometric Borders*, Wolf Legal Publishers: Nijmegen, 2007.

Lodge, J., 'Biometrics: A Challenge For Privacy Or Public Policy - Certified Identity And Uncertainties', REGIO, no. 1, 2007, pp. 193 - 206.

McGinley, M. and Parkes, R., *Data protection in the EU's internal security cooperation*, SWP Research Paper, Stiftung Wissenschaft und Politik: Berlin, May 2007.

Mitsilegas, V., 'Contrôle des étrangers, des passagers, des citoyens: surveillance et anti-terrorisme', Cultures & Conflits, no. 58, 2005, pp . 155 – 181.

Pastore, F. 'Visas, Borders, Immigration: formation, structure and current evolution of the EU entry control system', in Walker, N. (ed.), *Europe's Area of Freedom, Security and Justice*, Oxford University Press: Oxford, 2004, pp. 89 – 142.

Peers, S., 'The Schengen Information System and EC immigration and asylum law', in de Zwaan, J. W. and Goudappel, F.A.N.J, *Freedom, Security and Justice in the European Union*, TMC Asser Press: The Hague, 2006, pp. 172 – 192.

Preuss-Laussinotte, S., 'L'Union européenne et les technologies de sécurité', *Cultures & Conflits*, no. 64, 2006, pp. 97 – 108.

Pring, J. *Up close and personal: data protection and EU-US relations*, EPC Policy Brief, European Policy Centre: Brussels, June 2007.

Scandamis, N., Sigalas, F. and Stratakis, S., *Rival Freedoms in terms of security: The case of data protection and the criterion of connexity*, CHALLENGE Research Paper No. 7, Centre for European Policy Studies: Brussels, December 2007.

Schreiber, W., 'Biometrics – Applications, Costs and Risks', REGIO no. 1, 2007, pp. 207 – 216.

Standing Committee of experts on international immigration, refugee and criminal law (Meijers Commissie), Proposal to give law enforcement authorities access to Eurodac, 6.11.2007.

Westphal, D., 'Die Richtlinie zur Vorratsdatenspeicherung von Verkehrsdaten – Brüsseler Stellungnahme zum Verhältnis von Freiheit und Sicherheit in der "Post-911-Informationsgesellschaft"', *Europarecht*, vol. 41, no. 5, 2006, pp. 706 – 723.