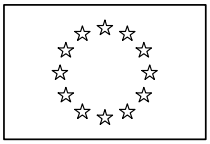

EUROPEAN COMMISSION

Brussels, 20.7.2010

COM(2010)385 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

Overview of information management in the area of freedom, security and justice

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

Overview of information management in the area of freedom, security and justice

1. INTRODUCTION

The European Union has come a long way since the leaders of five European countries agreed in Schengen in 1985 to abolish controls at their common borders. Their agreement gave rise in 1990 to the Schengen Convention, which contained the seeds of many of today's information management policies. The abolition of internal border checks has spurred the development of a whole range of measures at external frontiers, mainly concerning the issuing of visas, the coordination of asylum and immigration policies and the strengthening of police, judicial and customs cooperation in the fight against cross-border crime. Neither the Schengen area nor the EU internal market could function today without cross-border data exchange.

The terrorist attacks in the United States in 2001, as well as the bombings in Madrid and London in 2004 and 2005, triggered another dynamic in the development of Europe's information management policies. In 2006, the Council and the European Parliament adopted the Data Retention Directive to enable national authorities to combat serious crime by retaining telecommunication traffic and location data.[1] The Council then took up the Swedish initiative to simplify the cross-border exchange of information in criminal investigations and intelligence operations. In 2008, it endorsed the Prüm Decision to speed up the exchange of DNA profiles, fingerprints and vehicle registration data in the fight against terrorism and other forms of crime. Cross-border cooperation between Financial Intelligence Units, Asset Recovery Offices and cybercrime platforms and the Member States' use of Europol and Eurojust constitute further tools in the fight against serious crime in the Schengen area.

In the immediate aftermath of the terrorist attacks on 11 September 2001, the US government established its Terrorist Finance Tracking Program to thwart similar plots by monitoring suspicious financial transactions. The European Parliament has recently given its consent to the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program (EU-US TFTP Agreement).[2] The exchange of Passenger Name Records (PNR) with third countries has also helped the EU to combat terrorism and other forms of serious crime.[3] Having

---

1 There is currently no harmonised EU definition of 'serious crime.' For example, the Council Decision that empowers Europol to consult VIS (Council Decision 2008/633/JHA, OJ L 218, 13.8.2008, p. 129) defines 'serious criminal offences' with reference to the list of offences set out in the European Arrest Warrant (Council Decision 2002/584/JHA, OJ L 190, 18.7.2002, p. 1). The Data Retention Directive (Directive 2002/58/EC, OJ L 105, 13.4.2006, p. 54) leaves it to Member States to define 'serious crime.' The Europol Decision (Council Decision 2009/371/JHA, OJ L 121, 15.5.2009, p. 37) contains another list of offences defined as 'serious crime,' which is very similar, but not identical, to the list contained in the European Arrest Warrant.

2 European Parliament Resolution, P7_TA-PROV(2010)0279, 8.7.2010.

3 In contrast to serious crime, 'terrorist offences' are clearly defined in the Council Framework Decision on combating terrorism (Council Framework Decision 2002/475/JHA, OJ L 164, 22.6.2002, p. 3; amended by Council Framework Decision 2008/919/JHA, OJ L 330, 9/12/2008, p. 21).

concluded PNR agreements with the US, Australia and Canada, the Commission has recently gone back to the drawing board to reconsider its approach to establishing a PNR system in the EU and sharing such data with third countries.

The measures outlined above have enabled free movement in the Schengen area, contributed to the prevention of and fight against terrorist attacks and other forms of serious crime and enhanced the development of a common visa and asylum policy.

This communication presents, for the first time, a full overview of the EU-level measures in place, under implementation or consideration that regulate the collection, storage or cross-border exchange of personal information for the purpose of law enforcement or migration management. Citizens have a right to know what personal data are processed and exchanged about them, by whom and for what purpose. This document provides a transparent answer to these questions. It clarifies the main purpose of these instruments, their structure, the types of personal data they cover, the list of authorities with access to such data and the provisions governing data protection and retention. In addition, it contains a limited number of examples illustrating how these instruments operate in practice (see Annex I). Finally, it sets out the core principles that should underpin the design and evaluation of information management instruments in the area of freedom, security and justice.

By giving an overview of EU-level measures regulating the management of personal information and proposing a set of principles for the development and assessment of such measures, this communication contributes to an informed policy dialogue with all stakeholders. At the same time, it provides a first response to calls by Member States to develop a more 'coherent' approach to the exchange of personal information for law enforcement purposes, which was recently addressed by the EU Information Management Strategy,[4] and for reflection on the possible need for developing a European Information Exchange Model based on an evaluation of current information exchange measures.[5]

Purpose limitation is a key consideration for most of the instruments covered in this communication. A single, overarching EU information system with multiple purposes would deliver the highest degree of information sharing. Creating such a system would, however, constitute a gross and illegitimate restriction of individuals' right to privacy and data protection and pose huge challenges in terms of development and operation. In practice, policies in the area of freedom, security and justice have developed in an incremental manner, yielding a number of information systems and instruments of varying size, scope and purpose. The compartmentalised structure of information management that has emerged over recent decades is more conducive to safeguarding citizens' right to privacy than any centralised alternative.

This communication does not cover measures involving the exchange of non-personal data for strategic purposes, such as general risk analyses or threat assessments; neither does it analyse in detail the data protection provisions of the instruments under discussion, as the Commission is currently conducting, on the basis of Article 16 of the Treaty on the

---

4 Council Conclusions on an Information Management Strategy for EU internal security, Justice and Home Affairs Council, 30.11.2009 (EU Information Management Strategy); Freedom, Security, Privacy — European Home Affairs in an open world, Report of the Informal High Level Advisory Group on the Future of European Home Affairs Policy ("The Future Group"), June 2008.

5 The Stockholm Programme — An open and secure Europe serving and protecting citizens, Council Document 5731/10, 3.3.2010, Section 4.2.2.

Functioning of the European Union, a separate exercise on a new comprehensive framework for the protection of personal data in the EU. The Council is presently considering the draft negotiating directives for an EU-US agreement on the protection of personal data when transferred and processed for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police cooperation and judicial cooperation in criminal matters. As these negotiations are expected to establish the ways in which the two parties may ensure a high level of protection for fundamental rights and freedoms when transferring or processing personal data rather than the actual substance of such data transfers or processing, this communication does not cover this initiative.[6]

2. EU INSTRUMENTS REGULATING THE COLLECTION, STORAGE OR EXCHANGE OF PERSONAL DATA FOR LAW ENFORCEMENT OR MIGRATION PURPOSES

This section provides an overview of the European Union's instruments regulating the collection, storage or cross-border exchange of personal data for the purpose of law enforcement or migration management. Section 2.1 focuses on measures currently in force, under implementation or consideration; section 2.2 concerns initiatives set out in the Stockholm Programme Action Plan.[7] It provides information on the following aspects of each instrument:

– Background (whether the measure was proposed by Member States or the Commission);[8]

– Purpose(s) for which data are collected, stored or exchanged;

– Structure (centralised information system or decentralised data exchange);

– Personal data coverage;

– Authorities with access to the data;

– Data protection provisions;

– Data retention rules;

– State of implementation;

– Review mechanism.

---

6 COM(2010)252, 26.5.2010.

7 COM(2010)171, 20.4.2010 (Stockholm Programme Action Plan).

8 In the European Union's former third pillar concerning police and judicial cooperation in criminal matters, Member States and the Commission shared the right of initiative. The Amsterdam Treaty integrated the areas of external border control, visas, asylum and immigration into the Community (first) pillar, where the Commission enjoyed the exclusive right of initiative. The Lisbon Treaty has eliminated the Union's pillar structure, reaffirming the Commission's right of initiative. In the areas of police and judicial cooperation in criminal matters (including administrative cooperation), however, legislation may still be proposed on the initiative of a quarter of the Member States.

2.1. Instruments in operation, under implementation or consideration

EU instruments aiming to enhance the operation of the Schengen area and the customs union

The **Schengen Information System** (SIS) grew out of Member States' desire to create an area without internal border controls while facilitating the movement of persons across their external frontiers.[9] Operational since 1995, it seeks to maintain public security, including national security, within the Schengen area and facilitate the movement of persons using information communicated via this system. SIS is a centralised information system comprising a national part in each participating state and a technical support function in France. Member States may issue alerts for persons wanted for arrest for extradition; third-country nationals to be refused entry; missing persons; witnesses or those under judicial summons; persons and vehicles subject to exceptional monitoring on account of the threat they pose to public or national security; lost or stolen vehicles, documents and firearms; and suspect bank notes. Data entered in SIS include names and aliases, physical characteristics, place and date of birth, nationality and whether an individual is armed and violent. Police, border control, customs and judicial authorities in criminal proceedings may access these data in accordance with their respective legal powers. Immigration authorities and consular posts have access to data relating to third-country nationals on the entry ban list and alerts on lost and stolen documents. Europol may access some categories of SIS data, including alerts on persons wanted for arrest for extradition and those on persons subject to exceptional monitoring on account of the threat they pose to public or national security. Eurojust may access alerts on persons wanted for arrest for extradition and those on witnesses or persons under judicial summons. Personal data may only be used for the purpose of the specific alerts for which they were supplied. Personal data entered in SIS for the purpose of tracing persons may be kept only for the time required to meet the purposes for which they were supplied, and no longer than three years after they were entered. Data on persons subject to exceptional monitoring due to the threat they pose to public or national security must be deleted after one year. Member States must adopt national rules providing for a level of data protection at least equal to that resulting from the Council of Europe's 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and the Council of Europe Committee of Ministers' 1987 Recommendation regulating the use of personal data in the police sector.[10] While the Schengen Convention does not include a review mechanism, signatories may propose amendments to it, following which the amended text must be approved by unanimity and ratified by national parliaments. SIS is fully applicable in 22 Member States, as well as Switzerland, Norway and Iceland. The UK and Ireland participate in the police cooperation aspects of the Schengen Convention and SIS, with the exception of alerts relating to third-country nationals on the entry ban list. Cyprus has signed the Schengen Convention, but has not yet implemented it. Liechtenstein is due to implement it in 2010; Bulgaria and Romania are expected to do so in 2011. Searches in SIS produce a 'hit' when the details of a person or object sought match those of an existing alert. Having obtained a hit,

---

9 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.

10 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108), Council of Europe, 28.1.1981 (Council of Europe Convention 108); Recommendation No R (87) 15 of the Committee of Ministers regulating the use of personal data in the police sector, Council of Europe, 17.9.1987 (Police Recommendation).

law enforcement authorities may, via their network of SIRENE bureaux, request supplementary information about the subjects of an alert.[11]

As new Member States have joined the Schengen area, the size of the SIS database has grown correspondingly: between January 2008 and 2010, the total number of SIS alerts rose from 22.9 to 31.6 million.[12] Anticipating such an increase in data volumes and changes in user needs, Member States decided in 2001 to develop a **second-generation Schengen Information System** (SIS II), entrusting this task to the Commission.[13] Currently under development, SIS II aims to ensure a high level of security in the area of freedom, security and justice by enhancing the functions of the first-generation system and to facilitate the movement of persons using information communicated via this system. In addition to the original data categories covered by the first-generation system, SIS II will be able to handle fingerprints, photographs, copies of the European Arrest Warrant, provisions to protect the interests of people whose identity is being misused and links between different alerts. For example, SIS II will be able to link alerts relating to a person wanted for abduction, the abducted individual and the vehicle used for this offence. Access rights and data retention rules are identical to those for the first-generation system. Personal data may only be used for the purpose of the specific alerts for which they were supplied. Personal data in SIS II must be processed in accordance with the specific provisions of the basic legal acts governing this system (Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA), which clarify the principles of Directive 95/46/EC and in accordance with Regulation (EC) No 45/2001, Council of Europe Convention 108 and the Police Recommendation.[14] SIS II will use s-TESTA, the Commission's secure data communication network.[15] Once operational, this system will be applicable in all Member States, Switzerland, Liechtenstein, Norway and Iceland.[16] The Commission is required to send to the European Parliament and the Council a biannual progress report on the development of SIS II and potential migration from the first-generation system.[17]

The development of **EURODAC** may be traced back to the abolition of internal frontiers, which made it necessary to establish clear rules concerning the processing of asylum applications. EURODAC is a centralised automated fingerprint identification system containing the fingerprint data of certain third-country nationals. In operation since January 2003, its purpose is to assist in determining which Member State should be responsible, under

---

11 SIRENE stands for Supplementary Information Request at National Entry.

12 Council Document 5441/08, 30.1.2008; Council Document 6162/10, 5.2.2010.

13 Regulation (EC) No 1986/2006, OJ L 381, 28.12.2006, p. 1; Regulation (EC) No 1987/2006, OJ L 381, 28.12.2006, p. 4; Decision 2007/533/JHA, OJ L 205, 7.8.2007, p. 63.

14 Regulation (EC) No 1987/2006, OJ L 381, 28.12.2006, p. 4; Decision 2007/533/JHA, OJ L 205, 7.8.2007, p. 63; Directive 95/46/EC, OJ L 281, 23.11.1995, p. 31; Regulation (EC) No 45/2001, OJ L 8, 12.1.2001, p. 1; Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108), Council of Europe, 28.1.1981 (Council of Europe Convention 108); Recommendation No R (87) 15 of the Committee of Ministers regulating the use of personal data in the police sector, Council of Europe, 17.9.1987 (Police Recommendation).

15 S-TESTA, which stands for Secure Trans-European Services for Telematics between Administrations, is a Commission-financed data communication network that enables the secure and encrypted exchange of information between national administrations and EU institutions, agencies and bodies.

16 The UK and Ireland will participate in SIS II with the exception of alerts relating to third-country nationals on the entry ban list.

17 Council Regulation (EC) 1104/2008, OJ L 299, 8.11.2008, p. 1; Council Decision 2008/839/JHA, OJ L 299, 8.11.2008, p. 43.

the Dublin Regulation, for examining a particular asylum application.[18] Individuals aged 14 years or over who request asylum in a Member State automatically have their fingerprints taken, as do third-country nationals apprehended in connection with the irregular crossing of an external border. By comparing these individuals' fingerprints with EURODAC records, national authorities seek to establish where that person might have submitted an asylum application or first entered the European Union. Authorities may also compare against EURODAC records the fingerprints of third-country nationals found illegally on their territory. Member States must specify the list of authorities with access to this database, which typically includes asylum and migration authorities, border guards and the police. Member States upload the relevant data to the central database through their national access points. Personal data in EURODAC may be used only for the purpose of facilitating the application of the Dublin Regulation; any other use is subject to penalties. The fingerprints of asylum-seekers are stored for 10 years; those of irregular migrants, for two years. Asylum-seekers' records are deleted once they acquire the citizenship of a Member State; those of irregular migrants are deleted once they obtain a residence permit or citizenship, or leave the territory of the Member States. Directive 95/46/EC applies to the processing of personal data under this instrument.[19] EURODAC runs on the Commission's s-TESTA network and is applicable in each Member State, as well as Norway, Iceland and Switzerland. An agreement enabling Liechtenstein's connection is awaiting conclusion. The Commission is required to submit to the European Parliament and the Council annual reports on the operation of EURODAC's central unit.

In the wake of the 11 September 2001 attacks, Member States resolved to step up the implementation of a common visa policy by creating a form of information exchange on short-stay visas.[20] The abolition of internal frontiers has also made it easier to abuse Member States' visa regimes. The **Visa Information System** (VIS) seeks to address both concerns: its purpose is to help implement a common visa policy by facilitating the examination of visa applications and external border checks while contributing to the prevention of threats to Member States' internal security.[21] VIS will be a centralised information system comprising a national part in each participating state and a technical support function in France. It will use a biometric matching system to ensure reliable fingerprint comparisons and verify the identity of visa-holders at external borders. It will include data on visa applications, photographs, fingerprints, related decisions of visa authorities and links between related applications. Visa, asylum, immigration and border control authorities will have access to this database for the purpose of verifying the identity of visa-holders and the authenticity of visas; the police and Europol may consult it for the purpose of preventing and combating terrorism and other forms of serious crime.[22] Application files may be retained for five years. Personal data in VIS must be processed in accordance with the specific rules contained in the basic legal acts governing this system (Regulation (EC) No 767/2008 and Council Decision 2008/633/JHA), which

---

18 Council Regulation (EC) No 343/2003, OJ L 50, 25.2.2003, p. 1 (Dublin Regulation), Council Regulation (EC) 2725/2000, OJ L 316, 15.12.2000, p. 1 (EURODAC Regulation). These instruments build upon the 1990 Dublin Convention (OJ C 254, 19.8.1997, p. 1), which sought to determine which Member State ought to examine asylum applications. The system of assessing asylum applications is known as the 'Dublin system.'

19 Directive 95/46/EC, OJ L 281, 23.11.1995, p. 31.

20 Extraordinary Justice and Home Affairs Council, 20.9.2001.

21 Council Decision 2004/512/EC, OJ L 213, 15.6.2004, p. 5; Regulation (EC) No 767/2008, OJ L 218, 13.8.2008, p. 60; Council Decision 2008/633/JHA, OJ L 218, 13.8.2008, p. 129. See also Declaration on combating terrorism, European Council, 25.3.2004.

22 Council Decision 2008/633/JHA, OJ L 218, 13.8.2008, p. 129.

complement the provisions of Directive 95/46/EC, Regulation (EC) No 45/2001, Council Framework Decision 2008/977/JHA, Council of Europe Convention 108, its Additional Protocol 181 and the Police Recommendation.[23] VIS will be applicable in each Member State (except the UK and Ireland), as well as Switzerland, Norway and Iceland. It will operate on the basis of the Commission's s-TESTA network. The Commission will evaluate this system three years after its launch and every four years thereafter.

Upon a Spanish initiative, the Council adopted in 2004 a directive regulating the transmission of **Advance Passenger Information** (API) by air carriers to border control authorities.[24] The purpose of this instrument is to improve border control and combat irregular migration. Upon request, air carriers must communicate to border control authorities the name, date of birth, nationality, point of embarkation and border-crossing entry point of passengers travelling to the EU from third countries. Such personal data are typically taken from the machine-readable part of passengers' passports and forwarded to the authorities after the completion of check-in. Following a flight's arrival, the authorities and air carriers may retain API data for 24 hours. The API system works in a decentralised fashion through information sharing between private operators and public authorities. This instrument does not allow the exchange of API between Member States; however, law enforcement authorities other than border guards may request access to this information for law enforcement purposes. Personal data may only be used by public authorities for the purposes of border control and combating irregular migration and must be processed in line with Directive 95/46/EC.[25] In force across the EU, this instrument is used only by a small number of Member States. The Commission will review this directive in 2011.

An important part of the Commission's 1992 Programme, which established the internal market, concerned the abolition of all checks and formalities in respect of goods moving within the Community.[26] The elimination of such procedures at internal borders heightened the risk of fraud, which made it necessary for Member States to establish, on the one hand, a mechanism of mutual administrative assistance to assist in preventing, investigating and prosecuting operations in breach of Community customs and agriculture legislation and, on the other hand, customs cooperation aiming to enable the detection and prosecution of violations of national customs provisions, notably by enhancing cross-border information exchange. Without prejudice to the competence of the EU in the customs union,[27] the **Naples II Convention** on mutual assistance and cooperation between customs administrations aims

---

23 Regulation (EC) No 767/2008, OJ L 218, 13.8.2008, p. 60; Council Decision 2008/633/JHA, OJ L 218, 13.8.2008, p. 129; Directive 95/46/EC, OJ L 281, 23.11.1995, p. 31; Regulation (EC) No 45/2001, OJ L 8, 12.1.2001, p. 1; Council Framework Decision 2008/977/JHA, OJ L 350, 30.12.2008, p. 60; Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108), Council of Europe, 28.1.1981 (Council of Europe Convention 108); Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows (ETS No 181), Council of Europe, 8.11.2001 (Additional Protocol 181); Recommendation No R (87) 15 of the Committee of Ministers regulating the use of personal data in the police sector, Council of Europe, 17.9.1987 (Police Recommendation).

24 Council Directive 2004/82/EC, OJ L 261, 6.8.2004, p. 24.

25 Directive 95/46/EC, OJ L 281, 23.11.1995, p. 31.

26 Council Regulation (EEC) 2913/92, OJ L 302, 19.10.2992.

27 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, amended by Regulation (EC) No 766/2008, OJ L 218, 13.8.2008, p. 48.

to enable national customs administrations to prevent and detect infringements of national customs provisions and to help them prosecute and punish infringements of Community and national customs provisions.[28] Under this instrument, a set of central coordinating units request assistance in writing from their counterparts in other Member States for criminal investigations concerning infringements of national and Community customs rules. These units may only process personal data for the purpose of the Naples II Convention. They may forward such information to national customs authorities, investigative authorities and judicial bodies and, subject to the prior consent of the Member State supplying the data, to other authorities. The data may be kept for a period not exceeding that necessary for the purpose for which they were supplied. Personal data in the recipient Member State enjoys at least the same level of protection as in the supplying Member State and its processing must comply with the provisions of Directive 95/46/EC and Council of Europe Convention 108.[29] The Naples II Convention has been ratified by each Member State. They may propose amendments to it, following which the amended text would have to be adopted by the Council of Ministers and ratified by Member States.

Complementing the Naples II Convention, the CIS Convention deploys the **Customs Information System** (CIS) to assist in preventing, investigating and prosecuting serious violations of national laws by increasing, through the rapid dissemination of information, the effectiveness of cooperation between Member States' customs administrations.[30] The CIS, managed by the Commission, is a centralised information system accessible via terminals in each Member State and at the Commission, Europol and Eurojust. It comprises personal data with reference to commodities, means of transport, businesses, persons and goods and cash retained, seized or confiscated. The personal data are names and aliases, date and place of birth, nationality, sex, physical characteristics, identity documents, address, any history of violence, the reason for entering the data in CIS, suggested action and the registration of the means of transport. In the case of goods and cash retained, seized or confiscated, only biographical data and an address may be entered in CIS. Such information may be used solely for the purposes of sighting, reporting or carrying out particular inspections or specific checks on, or for strategic or operational analyses concerning, persons suspected of breaching national customs provisions. National customs, taxation, agricultural, public health and police authorities, Europol and Eurojust may access CIS data.[31] The processing of personal data must comply with the specific rules established by the CIS Convention and the provisions of Directive 95/46/EC, Regulation (EC) No 45/2001, Council of Europe Convention 108 and the Police Recommendation.[32] Personal data may only be copied from CIS to other data-

---

28 Convention drawn up on the basis of Article K.3 of the Treaty on European Union, on mutual assistance and cooperation between customs administrations, OJ C 24/2, 23.1.1998 (Naples II Convention).

29 Directive 95/46/EC, OJ L 281, 23.11.1995, p. 31; Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108), Council of Europe, 28.1.1981 (Council of Europe Convention 108).

30 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, amended by Council Decision 2009/917/JHA, OJ L 323, 10.12.2009, p. 20.

31 As of May 2011, Europol and Eurojust will have reading access to CIS on the basis of Council Decision 2009/917/JHA (OJ L 323, 10.12.2009, p. 20).

32 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, amended by Council Decision 2009/917/JHA, OJ L 323, 10.12.2009, p. 20; Directive 95/46/EC, OJ L 281, 23.11.1995, p. 31; Regulation (EC) No 45/2001, OJ L 8, 12.1.2001, p. 1; Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108), Council of Europe, 28.1.1981 (Council

processing systems for risk management or operational analyses, which only the analysts designated by Member States may access. Personal data copied from CIS may only be kept for the time necessary to achieve the purpose for which they were copied and for no longer than 10 years. CIS also establishes a **Customs file identification database** (FIDE) to assist in preventing, investigating and prosecuting serious violations of national laws.[33] FIDE enables national authorities responsible for conducting customs investigations, when they open an investigation file, to identify other authorities that may have investigated a given person or business. These authorities may enter data in the FIDE from their investigation files, including the biographical data of persons under investigation and the business name, trading name, VAT number and address of businesses under investigation. Data sourced from investigation files where no customs fraud has been detected may be stored for a maximum of three years; those from files where an instance of customs fraud has been detected may be stored for a maximum of six years; and those from files where a conviction or penalty has been handed down may be kept for a maximum of 10 years. CIS and the FIDE use the Common communication network, Common system interface network or secure web access provided by the Commission. The CIS is in force in all Member States. The Commission, in cooperation with Member States, reports each year to the European Parliament and the Council on the operation of CIS.

EU instruments aiming to prevent and combat terrorism and other forms of serious cross-border crime

The March 2004 terrorist attacks in Madrid triggered several new initiatives at EU level. At the European Council's request, the Commission presented in 2005 a proposal for an instrument regulating the exchange of information under the principle of availability.[34] Instead of endorsing this proposal, the Council adopted in 2006 the **Swedish initiative**, which streamlines the sharing between Member States of any existing information or criminal intelligence that might be necessary for a criminal investigation or criminal intelligence operation.[35] This instrument is rooted in the policy principle of 'equivalent access,' according to which the conditions applicable to cross-border data exchange should be no stricter than those regulating domestic access. The Swedish initiative operates in a decentralised manner and enables the police, customs and any other authority with the power to investigate criminal offences (with the exception of the intelligence services, which typically handle intelligence relating to national or state security) to share information and criminal intelligence with their counterparts across the EU. Member States must designate national contact points to handle urgent requests for information. This measure sets clear time limits for the exchange of information and requires Member States to fill in a form when requesting data. Member States are required to respond to requests for information and intelligence within 8 hours in urgent cases, within one week in non-urgent cases and within two weeks in all other cases. The use of information and intelligence obtained via this instrument is subject to domestic data protection laws, where Member States are not permitted to apply differential treatment to

---

of Europe Convention 108); Recommendation No R (87) 15 of the Committee of Ministers regulating the use of personal data in the police sector, Council of Europe, 17.9.1987 (Police Recommendation).

33 FIDE, which stands for *Fichier d'Identification des Dossiers d'Enquêtes douanières*, is based on Council Regulation (EC) No 766/2008 and the Protocol established in accordance with Article 34 of the Treaty on European Union, 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.

34 COM(2005)490, 12.10.2005; Presidency Conclusions — The Hague Programme, 4/5.11.2004. See also Declaration on combating terrorism, European Council, 25.3.2004.

35 Council Framework Decision 2006/960/JHA, OJ L 386, 29.12.2006, p. 89.

domestically sourced data and those sourced from other Member States. A supplying Member State may, however, set conditions for the use of information or intelligence in other Member States. Personal data must be processed in accordance with national data protection legislation, as well as Council of Europe Convention 108, its Additional Protocol 181 and the Police Recommendation.[36] 12 of the 31 signatories to this measure (including EU Member States, as well as Norway, Iceland, Switzerland and Liechtenstein) have adopted national legislation to implement it; five states regularly fill in the form to request information; but only two states use it on a frequent basis to exchange information.[37] The Commission is to submit its evaluation report to the Council before the end of 2010.

The **Prüm Decision** builds upon an agreement concluded in 2005 by Germany, France, Spain, the Benelux states and Austria to step up cooperation in the fight against terrorism, cross-border crime and irregular migration. In response to the interest expressed by several Member States in joining this agreement, Germany proposed during its 2007 Council presidency to transform it into an EU instrument. The 2008 Prüm Decision, due to be implemented by August 2011, lays down the rules for the cross-border exchange of DNA profiles, fingerprints, vehicle registration data and information about individuals suspected of planning terrorist attacks.[38] It seeks to enhance the prevention of criminal offences, particularly terrorism and cross-border crime, and maintain public order in connection with major events. This system will work in a decentralised manner by interconnecting, via national contact points, the participating states' DNA, fingerprint and vehicle registration databases. Using the Commission's s-TESTA network, contact points will handle incoming and outgoing requests for the cross-border comparison of DNA profiles, fingerprints and vehicle registration data. Their powers to transmit such data to end-users are governed by national law. As of August 2011, data comparison will be fully automated. However, Member States must undergo a rigorous evaluation process (assessing, in particular, their compliance with data protection and technical requirements) to receive authorisation to begin automated data sharing. Personal data may not be exchanged under this instrument until Member States have guaranteed a level of data protection at least equal to that resulting from Council of Europe Convention 108, its Additional Protocol 181 and the Police Recommendation.[39] The Council will decide by unanimity whether this condition will have been met. Personal information may only be used for the purpose for which it is supplied, unless the supplying Member State consents to its use for other purposes. Individuals may also turn to their national data protection officers,

---

36 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108), Council of Europe, 28.1.1981 (Council of Europe Convention 108); Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows (ETS No 181), Council of Europe, 8.11.2001 (Additional Protocol 181); Recommendation No R (87) 15 of the Committee of Ministers regulating the use of personal data in the police sector, Council of Europe, 17.9.1987 (Police Recommendation).

37 This information is based on replies to a questionnaire, the results of which the Spanish Council presidency presented at a meeting of the Ad Hoc Council Working Party on Information Exchange on 22 June 2010.

38 Council Decision 2008/615/JHA, OJ L 210, 6.8.2008, p. 1; Council Decision 2008/616/JHA, OJ L 210, 6.8.2008, p. 12.

39 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108), Council of Europe, 28.1.1981 (Council of Europe Convention 108); Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows (ETS No 181), Council of Europe, 8.11.2001 (Additional Protocol 181); Recommendation No R (87) 15 of the Committee of Ministers regulating the use of personal data in the police sector, Council of Europe, 17.9.1987 (Police Recommendation).

designated under Directive 95/46/EC, to enforce their rights concerning the processing of personal data under this instrument. The comparison of DNA profiles and fingerprints will operate on a 'hit/no hit' (anonymous) basis, whereby authorities will only be able to request personal information about a data subject if their original search will have produced a hit. Such requests for additional information will typically be channelled through the Swedish initiative. The Prüm Decision is being implemented across the EU-27, while Norway and Iceland are in the process of acceding to it.[40] The Commission is to submit its evaluation report to the Council in 2012.

In response to the July 2005 London bombings, Britain, Ireland, Sweden and France proposed the adoption of an EU instrument harmonising national rules applicable to data retention. The 2006 **Data Retention Directive** obliges telephony and internet service providers to retain, for the purpose of investigating, detecting and prosecuting serious crime, electronic communication traffic and location data, as well as information about subscribers (including their telephone number, IP address and mobile equipment identifier).[41] The Data Retention Directive regulates neither the access to nor the use of data retained by national authorities. Its scope explicitly excludes the content of electronic communication; in other words, wiretapping is not possible under this instrument. This measure leaves it to Member States to define 'serious crime.' Member States also determine which national authorities may access such data on a case-by-case basis and the procedures and conditions for granting access to the information. Data retention periods vary from 6 to 24 months. Directive 95/46/EC and Directive 2002/58/EC regulate the protection of personal data under this instrument.[42] Six Member States have not yet fully transposed this measure, and the constitutional courts in Germany and Romania have declared their national implementing legislation to be unconstitutional. The German constitutional court found that the rules governing access to and the use of the data, as laid down in national law, were unconstitutional.[43] The Romanian constitutional court found that data retention *per se* breached Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights) and was thus unconstitutional.[44] The Commission is currently evaluating this instrument and is to submit its assessment report to the European Parliament and the Council in late 2010.

The ongoing establishment of a **European Criminal Records Information System** (ECRIS) may be traced back to a 2004 Belgian initiative that sought to disqualify convicted sex offenders from working with children in other Member States. Member States relied in the past on the Council of Europe's Convention on Mutual Assistance in Criminal Matters to exchange information about their nationals' convictions, but this system proved inefficient.[45] The Council took a first step towards reform by adopting Council Decision 2005/876/JHA, which required each Member State to set up a central authority that would send, at regular

---

40 To date, ten Member States have been authorised to commence the automated exchange of DNA profiles, five have been authorised for fingerprints and seven for vehicle registration data. Germany, Austria, Spain and the Netherlands have supplied to the Commission partial statistics on their use of this instrument.

41 Directive 2006/24/EC, OJ L 105, 13.4.2006, p. 54.

42 Directive 95/46/EC, OJ L 281, 23.11.1995, p. 31; Directive 2002/58/EC, OJ L 201, 31.7.2002, p. 37 (e-Privacy Directive).

43 Ruling of the German Constitutional Court, Bundesverfassunggericht 1 BvR 256/08, 11.3.2008.

44 Decision No 1258 of the Romanian Constitutional Court, 8.10.2009.

45 European Convention on Mutual Assistance in Criminal Matters (ETS No 30), Council of Europe, 20.4.1959. See also COM(2005)10, 25.1.2005.

intervals, the convictions of non-nationals to the Member State(s) of nationality.[46] This instrument also enabled Member States to obtain, for the first time and subject to national law, previous convictions handed down against their own nationals in other Member States. They could request such information by filling in a standardised form rather than through mutual legal assistance procedures. In 2006 and 2007, the Commission presented a comprehensive legislative package consisting of three instruments: Council Framework Decision 2008/675/JHA obliging Member States to take account of previous convictions in new criminal proceedings; Council Framework Decision 2009/315/JHA on the organisation and content of the exchange of information extracted from criminal records; and Council Decision 2009/316/JHA establishing ECRIS as the technical means of exchanging information extracted from criminal records.[47] Due to be implemented by April 2012, Council Framework Decisions 2009/315/JHA and 2009/316/JHA aim to define the ways in which a convicting Member State must transmit information concerning a new conviction to the Member State(s) of the convicted person's nationality, storage obligations, and a framework for a computerised system of information exchange. ECRIS will be a decentralised information system that interconnects Member States' criminal record databases via the Commission's s-TESTA network. A set of central authorities will exchange data about citizens' new convictions and past criminal records. The data will be encrypted, structured according to a predetermined format and include the following: biographical details; the conviction, sentence and underlying offence; and additional information (including fingerprints, if available). As of April 2012, extracts from criminal records must be provided for ongoing criminal proceedings and sent to judicial or competent administrative authorities, such as bodies authorised to vet persons for sensitive employment or firearms ownership. Personal data supplied for criminal proceedings may only be used for that purpose; use for any other purpose requires the consent of the supplying Member State. The processing of personal data must be in line with the specific provisions established by Council Framework Decision 2009/315/JHA, which incorporates the rules of Council Decision 2005/876/JHA, as well as Council Framework Decision 2008/977/JHA and Council of Europe Convention 108.[48] For any personal data processing by EU institutions using ECRIS, for example to ensure data security, Regulation (EC) 45/2001 applies.[49] This legislative package does not contain rules on data retention, as the storage of information relating to criminal convictions is regulated by national law. Fifteen Member States are currently participating in a pilot project, nine of which have started the electronic exchange of information extracted from criminal records. The Commission must submit to the European Parliament and the Council two evaluation reports concerning the operation of this legislative package: Framework Decision 2008/675/JHA is to be reviewed in 2011; Framework Decision 2009/315/JHA is to be reviewed in 2015. As of 2016, the Commission must also publish regular reports on the operation of ECRIS.

Upon a Finnish initiative, the Council adopted in 2000 an instrument organising the exchange of information between Member States' **Financial Intelligence Units** (FIUs) for the purpose

---

46 Council Decision 2005/876/JHA, OJ L 322, 9.12.2005, p. 33.

47 Council Framework Decision 2008/675/JHA, OJ L 220, 15.8.2008, p. 32; Council Framework Decision 2009/315/JHA, OJ L 93, 7.4.2009, p. 23; Council Decision 2009/316/JHA, OJ L 93, 7.4.2009, p. 33. See also COM(2005)10, 25.1.2005.

48 Council Framework Decision 2009/315/JHA, OJ L 93, 7.4.2009, p. 23; Council Decision 2005/876/JHA, OJ L 322, 9.12.2005, p. 33; Council Framework Decision 2008/977/JHA, OJ L 350, 30.12.2008, p. 60; Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108), Council of Europe, 28.1.1981 (Council of Europe Convention 108).

49 Regulation (EC) No 45/2001, OJ L 8, 12.1.2001, p. 1.

of combating money laundering and, later, terrorist financing.[50] FIUs are typically established within law enforcement agencies, judicial authorities or administrative bodies reporting to financial authorities. They are required to share the necessary financial or law enforcement data, including the details of financial transactions, with their EU counterparts, except in cases where such disclosure would be disproportionate to the interests of natural or legal persons. Information supplied for the purpose of analysing or investigating money laundering or terrorist financing may also be used for criminal investigations or prosecutions unless the supplying Member State prohibits such use. The processing of personal data must respect the provisions of Council Framework Decision 2008/977/JHA, Council of Europe Convention 108 and its Police Recommendation.[51] In 2002, several Member States established FIU.net, a decentralised network application that handles data exchange between FIUs and runs on the Commission's s-TESTA network.[52] This initiative has twenty FIUs as members. There are ongoing discussions on deploying Europol's secure SIENA application to operate FIU.net.[53] Having assessed Member States' compliance with this instrument, the Council empowered FIUs, in the Third Anti-Money Laundering Directive, to receive, analyse and disseminate suspicious transaction reports relating to money laundering *and* terrorist financing.[54] As part of its Financial Services Action Plan, the Commission has been reviewing the implementation of the Third Anti-Money Laundering Directive since 2009.[55]

Taking up an initiative proposed by Austria, Belgium and Finland, the Council adopted in 2007 an instrument that seeks to enhance cooperation between **Asset Recovery Offices** (AROs) in tracking and identifying the proceeds of crime.[56] Similar to FIUs, AROs cooperate on a decentralised basis, albeit without the aid of an online platform. They are required to use the Swedish initiative to exchange information, specifying the details of targeted property, such as bank accounts, real estate and vehicles, as well as the details of natural or legal persons sought, including their name, address, date of birth and shareholder or company information. The use of information exchanged under this instrument is subject to domestic data protection laws, where Member States are not permitted to apply differential treatment to domestically sourced data and those sourced from other Member States. The processing of personal data must comply with the provisions of Council of Europe Convention 108, its Additional Protocol 181 and the Police Recommendation.[57] To date, more than twenty Member States have established AROs. In view of the sensitive nature of the information exchanged, there are ongoing discussions on deploying Europol's SIENA application for data

---

50 Council Decision 2000/642/JHA, OJ L 271, 24.10.2000, p. 4.

51 Council Framework Decision 2008/977/JHA, OJ L 350, 30.12.2008, p. 60; Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108), Council of Europe, 28.1.1981 (Council of Europe Convention 108); Recommendation No R (87) 15 of the Committee of Ministers regulating the use of personal data in the police sector, Council of Europe, 17.9.1987 (Police Recommendation).

52 http://www.fiu.net/

53 SIENA stands for Secure Information Exchange Network Application.

54 Directive 2005/60/EC, OJ L 309, 25.11.2005, p. 15 (Third Anti-Money Laundering Directive).

55 See, for example, Evaluation of the economic impacts of the Financial Services Action Plan — Final report (for European Commission, DG MARKT), CRA International, 03.2009.

56 Council Decision 2007/845/JHA, OJ L 332, 18.12.2007, p. 103.

57 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108), Council of Europe, 28.1.1981 (Council of Europe Convention 108); Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows (ETS No 181), Council of Europe, 8.11.2001 (Additional Protocol 181); Recommendation No R (87) 15 of the Committee of Ministers regulating the use of personal data in the police sector, Council of Europe, 17.9.1987 (Police Recommendation).

sharing between AROs. In a pilot project launched in May 2010, twelve AROs began to use SIENA to share information relevant for asset tracing. The Commission is required to submit an evaluation report to the Council in 2010.

In 2008, the French Council presidency invited Member States to establish national **Cybercrime Alert Platforms**, and Europol a European Cybercrime Alert Platform, for the purpose of collecting, analysing and exchanging information about offences committed on the internet.[58] Citizens may report to their national platforms cases of illicit content or behaviour detected on the internet. The European Cybercrime Platform (ECCP), managed by Europol, would act as an information hub, analysing and exchanging with national law enforcement authorities information related to cybercrime falling under Europol's mandate.[59] To date, almost all Member States have established national cybercrime alert platforms. Europol is working on the technical implementation of the ECCP and may soon deploy its SIENA application to enhance data sharing with national platforms. To the extent that such information sharing concerns the processing of personal data by Europol, the specific data protection rules contained in the Europol Decision (Council Decision 2009/371/JHA), as well as Regulation (EC) 45/2001, Council of Europe Convention 108, its Additional Protocol 181 and the Police Recommendation apply.[60] The provisions of Council Framework Decision 2008/977/JHA regulate the exchange of personal data between Member States and Europol.[61] In the absence of a legal instrument, there is no formal review mechanism for cybercrime alert platforms. However, Europol already covers this important area and, in future, will report on the activities of the ECCP in its Annual Report submitted to the Council for endorsement and to the European Parliament for information.

EU agencies and bodies mandated to assist Member States in preventing and combating serious cross-border crime

Established in 1995, the **European Police Office** (Europol) began operation in 1999 and became an EU agency in January 2010.[62] Its objective is to support Member States in preventing and combating organised crime, terrorism and other forms of serious crime affecting two or more Member States. Its main tasks include the collection, storage, processing, analysis and exchange of information and intelligence; assistance with investigations; and provision of intelligence and analytical support to Member States. The

---

58 Council Conclusions on setting up national alert platforms and a European alert platform for reporting offences noted on the Internet, Justice and Home Affairs Council, 24.10.2008; Council Conclusions concerning an Action Plan to implement the concerted strategy to combat crime, General Affairs Council, 26.4.2010. Europol has renamed its project the 'European Cybercrime Platform' (ECCP).

59 Europol's objective is the prevention and combating of organised crime, terrorism and other forms of serious crime affecting two or more Member States. See Council Decision 2009/371/JHA, OJ L 121, 15.5.2009, p. 37.

60 Council Decision 2009/371/JHA, OJ L 121, 15.5.2009, p. 37; Regulation (EC) No 45/2001, OJ L 8, 12.1.2001, p. 1; Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108), Council of Europe, 28.1.1981 (Council of Europe Convention 108); Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows (ETS No 181), Council of Europe, 8.11.2001 (Additional Protocol 181); Recommendation No R (87) 15 of the Committee of Ministers regulating the use of personal data in the police sector, Council of Europe, 17.9.1987 (Police Recommendation).

61 Council Framework Decision 2008/977/JHA, OJ L 350, 30.12.2008, p. 60.

62 Council Decision 2009/371/JHA, OJ L 121, 15.5.2009, p. 37, replacing the Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office, OJ C 316, 27.11.1995, p. 2.

main liaison body between Europol and Member States are the Europol National Units (ENUs), which second liaison officers to Europol. The heads of the ENUs meet on a regular basis to assist Europol in operational matters, while the agency's functioning is overseen by its management board and director. Europol's information management tools include the Europol Information System (EIS), Analysis Work Files (AWF) and the SIENA application. EIS contains the personal data, including, *inter alia*, the biometric identifiers, criminal convictions and organised crime links, of persons suspected of crimes falling under Europol's mandate. Access is limited to ENUs, liaison officers, authorised Europol staff and the director. The AWFs, opened for the purpose of aiding criminal investigations, include data on individuals and any other information that ENUs may decide to add. Access is granted to liaison officers, but only Europol analysts may enter data in these files. An index system allows ENUs and liaison officers to verify whether an AWF contains information of interest to their Member State. Europol's SIENA application is increasingly used by Member States to share sensitive data for law enforcement purposes. Europol may process information and intelligence, including personal data, for the performance of its tasks; Member States may only use information retrieved from Europol's data files for the purpose of preventing and combating serious crime of a cross-border nature. Any restriction placed on the use of information by a supplying Member State also applies to other users who retrieve such data from Europol's data files. Europol may also exchange personal information with third countries that have concluded operational agreements with Europol and guarantee an adequate level of data protection. It may retain data for only as long as is necessary for the performance of its tasks. AWFs may be retained for a maximum of three years, with another three-year extension possible. Europol's processing of personal data must be in line with the specific data protection rules contained in its own governing instrument (Council Decision 2009/371/JHA), as well as Regulation (EC) 45/2001, Council of Europe Convention 108, its Additional Protocol 181 and the Police Recommendation.[63] The provisions of Council Framework Decision 2008/977/JHA apply to the exchange of personal data between Member States and Europol.[64] A Joint Supervisory Body, made up members of national supervisory bodies, monitors the processing of personal data by Europol, as well as Europol's transmission of personal data to other parties. It submits regular reports to the European Parliament and the Council. Europol submits an annual report on its activities to the Council for endorsement and to the European Parliament for information.

In addition to its impact on several instruments described above, the 11 September 2001 terrorist attacks prompted the establishment, in 2002, of the **European Union's Judicial Cooperation Unit** (Eurojust).[65] Eurojust is an EU body whose objective is to improve the coordination of investigations and prosecutions in Member States and to enhance cooperation between competent national authorities. It covers the same types of crime and criminal

---

63 Council Decision 2009/371/JHA, OJ L 121, 15.5.2009, p. 37; Regulation (EC) No 45/2001, OJ L 8, 12.1.2001, p. 1; Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108), Council of Europe, 28.1.1981 (Council of Europe Convention 108); Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows (ETS No 181), Council of Europe, 8.11.2001 (Additional Protocol 181); Recommendation No R (87) 15 of the Committee of Ministers regulating the use of personal data in the police sector, Council of Europe, 17.9.1987 (Police Recommendation).

64 Council Framework Decision 2008/977/JHA, OJ L 350, 30.12.2008, p. 60.

65 Council Decision 2002/187/JHA, OJ L 63, 6.3.2002, p. 1, amended by Council Decision 2009/426/JHA, OJ L 138, 4.6.2009, p. 14. See also Extraordinary Justice and Home Affairs Council, 20.9.2001.

offences as Europol. Within that mandate and for the performance of their tasks, Eurojust's 27 national members, who make up its College, have access to the personal data of suspects and offenders. Such data include, *inter alia*, the following: biographical information, contact details, vehicle registration data, DNA profiles, photographs, fingerprints, as well as traffic, location and subscriber data provided by telecommunications service providers. Member States are expected to share such information with Eurojust to enable it to perform its tasks. All case-related personal data must be entered in Eurojust's automated case management system, which runs on the Commission's s-TESTA network. An index system stores personal and non-personal data relevant for ongoing investigations. Eurojust may process personal data for the performance of its tasks, but such operations must comply with the specific rules contained in Eurojust's own governing instrument (Council Decision 2009/426/JHA), as well as Council of Europe Convention 108, its Additional Protocol 181 and the Police Recommendation. The provisions of Council Framework Decision 2008/977/JHA apply to the exchange of personal data between Member States and Eurojust.[66] Eurojust may exchange data with national authorities and third countries with which it has concluded an agreement, provided that the national member that supplied the data has consented to such a transfer and the third country guarantees an adequate level of personal data protection. Personal data may be retained for as long as is necessary to achieve Eurojust's objectives, but must be deleted once a case is closed. Member States must implement Eurojust's amended legal basis by June 2011. By June 2014, the Commission is to review, and may propose any changes it deems appropriate concerning, the exchange of information between Eurojust's national members. By June 2013, Eurojust is to report to the Council and the Commission on the experience of providing access at national level to its case management system. Member States may review national access rights on that basis. A Joint Supervisory Body, made up of judges nominated by the Member States, monitors the processing of personal data by Eurojust and reports annually to the Council. The President of the College submits to the Council an annual report on Eurojust's activities, which the Council forwards to the European Parliament.

International agreements aiming to prevent and combat terrorism and other forms of serious transnational crime

As a result of the 11 September 2001 terrorist attacks, the US adopted legislation requiring air carriers operating flights to, from or through its territory to provide to US authorities **Passenger Name Record** (PNR) data stored in their automated reservation systems. Soon, Canada and Australia decided to do the same. As the relevant EU legislation requires prior assessment of the level of data protection guaranteed by third countries, the Commission stepped in to perform this function and negotiated PNR agreements with these countries.[67] It signed the US agreement in July 2007, the Australian one in June 2008 and an API/PNR agreement with Canada in October 2005.[68] The US and Australian agreements are provisionally applicable, while the Canadian one remains in force despite the expiry, in September 2009, of the Commission's adequacy decision concerning Canadian data

66 Council Framework Decision 2008/977/JHA, OJ L 350, 30.12.2008, p. 60.

67 Directive 95/46/EC (Data Protection Directive), OJ L 281, 23.11.1995, p. 31.

68 The Canadian package consists of a Canadian commitment concerning the handling of API/PNR data, the Commission's adequacy decision concerning Canadian data protection standards and an international agreement (see OJ L 91, 29.3.2006, p. 49; OJ L 82, 21.3.2006, p. 14). The US agreement may be found in OJ L 204, 4.8.2007, p. 16; the Australian one in OJ L 213, 8.8.2008, p. 47.

protection standards.[69] Critical of their content, the European Parliament has called on the Commission to renegotiate all three agreements on the basis of a clear set of principles.[70] Sent well in advance of a flight's departure, PNR data help law enforcement authorities screen passengers for potential links to terrorism and other forms of serious crime. Accordingly, the purpose of each agreement is the prevention and combating of terrorism and other transnational forms of serious crime. In return for EU-sourced PNR data, the US Department of Homeland Security (DHS) shares 'lead information' resulting from its PNR analysis with EU law enforcement authorities, Europol and Eurojust; and both Canada and the US have pledged in their respective agreements to cooperate with the EU in setting up its own PNR system. The US and Australian agreements contain 19 data categories, including biographical, reservation, payment and supplementary information; the Canadian agreement contains 25 similar data items. The supplementary information includes, *inter alia*, data on one-way tickets, standby status and 'no show' status. The US agreement also permits, under special conditions, the use of sensitive information. The DHS may process such information if the life of a data subject or of others is at risk, but must delete it within 30 days. PNR data are sent to a set of central units within the DHS, the Canada Border Services Agency and the Australian Customs Service, which may transfer such data to other domestic authorities responsible for law enforcement or counter-terrorism. In the US agreement, the DHS expects the level of data protection it has to apply to the processing of EU-originating PNR data to be 'no stricter' than that applied by EU authorities in their domestic PNR systems. If this expectation is not met, it may suspend certain parts of the agreement. The EU considers Canada and Australia to provide an 'adequate' level of protection for EU-sourced PNR data if they comply with the terms of their respective agreements. In the US, EU-sourced PNR data are retained for seven years in an active, and a further eight years in a dormant database. In Australia, they are entered in an active database for 3.5 years, and then in a dormant database for two years. In both countries, the dormant database is only accessible by special authorisation. In Canada, the data are retained for 3.5 years, with information rendered anonymous after 72 hours. Each agreement provides for periodic reviews, while the Canadian and Australian agreements also include a termination clause. In the EU, only the United Kingdom has a PNR system. France, Denmark, Belgium, Sweden and the Netherlands have either enacted relevant legislation or are currently testing the use of PNR data in preparation for setting up PNR systems. Several other Member States are considering setting up PNR systems, and all Member States use, on a case-by-case basis, PNR data for law enforcement purposes.

Following the 11 September 2001 attacks, the US Treasury Department developed a **Terrorist Finance Tracking Program** (TFTP) to identify, track and pursue terrorists and their financial supporters. Under the TFTP, the US Treasury required, by means of administrative subpoenas, the US branch of a Belgian company to transfer to the Treasury limited sets of financial messaging data carried over its network. In January 2010, this company changed its system architecture, which reduced by more than half the amount of data under US jurisdiction typically subject to Treasury subpoenas. In November 2009, the Presidency of the Council of the European Union and the United States Government signed an interim agreement concerning the processing and transfer of financial messaging data from the EU to the US for TFTP purposes, which the European Parliament did not endorse.[71] On

---

69 In 2009, Canada made a commitment to the Commission, the Council Presidency and EU Member States that it would continue to apply its earlier, 2005, commitment concerning the use of EU PNR data. The Commission's adequacy decision was based on that earlier commitment.

70 European Parliament Resolution, P7_TA(2010)0144, 5.5.2010.

71 European Parliament Resolution, P7_TA(2010)0029, 11.2.2010.

the basis of a new mandate, the European Commission negotiated a new draft agreement with the US, presenting to the Council on 18 June 2010 a proposal for a Council Decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program (EU-US TFTP Agreement).[72] The European Parliament gave its consent to the conclusion of this agreement on 8 July 2010.[73] The Council is now expected to adopt a Council Decision concluding this agreement, following which the agreement would enter into force via an exchange of letters between the two parties. The purpose of the EU-US TFTP Agreement is to prevent, investigate, detect or prosecute terrorism or its financing. It obliges designated providers of financial messaging services to transfer to the US Treasury, on the basis of specific geographical threat assessments and tailored requests, sets of financial messaging data containing, *inter alia*, the name, account number, address and identification number of the originator and recipient(s) of financial transactions. The Treasury may only search such data for the purpose of the TFTP and only if it has a reason to believe that an identified person has a nexus to terrorism or its financing. Data mining and the transfer of data relating to transactions within the Single Euro Payment Area are prohibited. The US provides to EU Member States, Europol and Eurojust any 'lead information' concerning potential terrorist plots in the EU and will help the EU establish its own system equivalent to the TFTP. Should the EU set up such a programme, the two sides may readjust the terms of this agreement. Before any data can be transferred, each US information request must be vetted by Europol to ensure that it meets the conditions of this agreement. Information extracted from financial messages may be retained for no longer than necessary for specific investigations or prosecutions; non-extracted data may be kept for up to 5 years. Where necessary for the investigation, prevention or prosecution of terrorism or its financing, the Treasury may transfer to US law enforcement, public security or counter-terrorism authorities, EU Member States, Europol or Eurojust any personal data extracted from FIN messages. It may also share with third countries any lead information concerning EU nationals and residents, subject to the consent of the concerned Member State. The parties' compliance with the strict counter-terrorism purpose limitation of the agreement and other safeguards is subject to monitoring by independent overseers, including by a person appointed by the Commission. It has a duration of five years and may be terminated or suspended by either party. An EU review team led by the Commission and including representatives of two data protection authorities and a judicial person will review this agreement six months after its entry into force, assessing in particular the parties' implementation of its purpose limitation and proportionality provisions and compliance with their data protection obligations. The Commission's report will be submitted to the European Parliament and the Council.

2.2. Initiatives under the Stockholm Programme Action Plan

Legislative proposals to be presented by the Commission

In the Stockholm Programme, the European Council called on the Commission to present three proposals of direct relevance to this communication: an EU PNR system for the prevention, detection and prosecution of terrorism and serious crime; an Entry/Exit System; and a Registered Travellers Programme. The latter two, the European Council stressed, should be presented 'as soon as possible.' The Commission has incorporated all three requests in its

[72] COM(2010)316 final/2, 18.6.2010.

[73] European Parliament Resolution, P7_TA-PROV(2010)0279, 8.7.2010.

Stockholm Programme Action Plan.[74] It will now aim to implement these requests and, in the future, evaluate these instruments on the basis of the policy development principles set out in section 4.

In November 2007, the Commission presented a proposal for a Council framework decision on the use of PNR data for law enforcement purposes.[75] This initiative received support in the Council and was subsequently modified to take account of amendments proposed by the European Parliament and the views of the European Data Protection Supervisor. With the entry into force of the Lisbon Treaty, it lapsed. As indicated in the Stockholm Programme Action Plan, the Commission is now working to present, in early 2011, a **Passenger Name Record package** consisting of the following: a communication on an EU external PNR strategy that outlines the core principles guiding the negotiation of agreements with third countries; negotiating directives for the renegotiation of PNR agreements with the US and Australia; and negotiating directives for a new agreement with Canada. The Commission is also in the process of preparing a new EU PNR proposal.

In 2008, the Commission put forward a number of suggestions to develop the EU's integrated border management by facilitating travel for third-country nationals while enhancing internal security.[76] Noting that 'overstayers' constituted the largest group of irregular migrants in the EU, it suggested the possible introduction of an **Entry/Exit System** (EES) for third-country nationals entering the EU for short stays of up to three months. This system would record the time and place of entry and length of authorised stay and would transmit automated alerts to the competent authorities identifying individuals as 'overstayers.' Based on biometric data verification, it would deploy the same biometric matching system and operational equipment as that used by SIS II and VIS. The Commission is currently conducting an impact assessment and, as stated in the Stockholm Programme Action Plan, will seek to present a legislative proposal in 2011.

A **Registered Travellers Programme** (RTP) was the third proposal to be considered.[77] This programme would allow certain groups of frequent travellers from third countries to enter the EU, subject to appropriate pre-screening, using simplified border checks at automated gates. The RTP would also be based on identity verification through the use of biometric data and allow a gradual move away from the current generic border control approach towards one based on individual risk. The Commission has conducted an impact assessment and, in line with the Stockholm Programme Action Plan, expects to present a legislative proposal in 2011.

Initiatives to be studied by the Commission

In the Stockholm Programme, the European Council called on the Commission to study three initiatives of relevance to this communication: the possibilities to track terrorist financing within the EU; the possibility and usefulness of developing a European System of Travel Authorisation; and the need for and added value of setting up of a European Police Records Index System. The Commission also incorporated these initiatives in its Stockholm Programme Action Plan. It will now assess their feasibility and decide whether and how to proceed with them on the basis of the policy development principles outlined in section 4.

---

74 The Stockholm Programme — An open and secure Europe serving and protecting citizens, Council Document 5731/10, 3.3.2010; COM(2010)171, 20.4.2010 (Stockholm Programme Action Plan).

75 COM(2007)654, 6.11.2007.

76 COM(2008)69, 13.2.2008.

77 COM(2008)69, 13.2.2008.

The EU-US TFTP Agreement calls on the European Commission to carry out a study into the possible introduction of an **EU terrorist finance tracking system** equivalent to the US TFTP, allowing for a more targeted transfer of data from the EU to the US. The draft Council Decision on the conclusion of this agreement also invites the Commission to submit to the European Parliament and the Council, no later than one year after the entry into force of the EU-US TFTP Agreement, a legal and technical framework for the extraction of data on EU territory.[78] Within three years from this agreement's entry into force, the Commission is to present a progress report on the development of such an equivalent EU system. If such a system will not have been set up within five years from the agreement's entry into force, the EU may decide to terminate the agreement. The EU-US TFTP Agreement also commits the US to cooperate with the EU and to provide assistance and advice should the EU decide to establish such a system. Without prejudice to any eventual decision, the Commission has begun to consider the data protection, resource and practical implications of this endeavour. As indicated in the Stockholm Programme Action Plan, the Commission will present in 2011 a communication on the feasibility of establishing an EU Terrorist Finance Tracking Programme (EU TFTP).

In its 2008 communication on integrated border management, the Commission suggested the potential establishment of an **Electronic System of Travel Authorisation** (ESTA) for third-country nationals not subject to visa requirements.[79] Under this programme, eligible third-country nationals would be requested to make an electronic application supplying, in advance of travel, their biographical, passport and travel details. Compared to the visa procedure, ESTA would offer a faster and simpler method of verifying whether a person fulfils the necessary entry conditions. The Commission is currently conducting a study of the advantages, disadvantages and practical implications of introducing ESTA. As indicated in the Stockholm Programme Action Plan, it is aiming to present in 2011 a communication on the feasibility of establishing such a programme.

During its 2007 Council presidency, Germany launched a discussion on the potential establishment of a **European Police Records Index System** (EPRIS).[80] EPRIS would help law enforcement officers locate information across the EU, particularly concerning connections between individuals suspected of organised crime. The Commission will present to the Council in 2010 its draft terms of reference for its feasibility study on EPRIS. As stated in the Stockholm Programme Action Plan, it will seek to present in 2012 a communication on the feasibility of setting up such a system.

3. ANALYSIS OF INSTRUMENTS IN OPERATION, UNDER IMPLEMENTATION OR CONSIDERATION

The above overview suggests the following preliminary observations:

Decentralised structure

Of the various instruments currently in operation, under implementation or consideration, only six involve the collection or storage of personal data at EU level, namely SIS (and SIS

[78] Council Document 11222/1/10 REV 1, 24.6.2010; Council Document 11222/1/10 REV1 COR1, 24.6.2010.

[79] COM(2008)69, 13.2.2008.

[80] See Council Document 15526/1/09, 2.12.2009.

II), VIS, EURODAC, CIS, Europol and Eurojust. All the other measures regulate the decentralised, cross-border, exchange or transfer to third countries of personal information collected at national level by public authorities or private companies. The majority of personal data is collected and stored nationally; the EU seeks to add value by enabling, under certain conditions, the exchange of such information with EU partners and third countries. The Commission has recently submitted to the European Parliament and the Council an amended proposal on establishing an Agency for the operational management of large-scale IT systems in the area of freedom, security and justice.[81] The future IT Agency's task will be to fulfil the operational management of SIS II, VIS and EURODAC, and any other future IT system in the area of freedom, security and justice, so as to keep these systems functioning on a permanent basis, thus ensuring the uninterrupted flow of information.

Limited purpose

Most of the instruments analysed above have a unitary purpose: EURODAC seeks to enhance the functioning of the Dublin system; API to improve border control; the Swedish initiative to enhance criminal investigations and intelligence operations; the Naples II Convention to help prevent, detect, prosecute and punish customs fraud; CIS to assist in preventing, investigating and prosecuting serious violations of national laws by increasing the effectiveness of cooperation between national customs administrations; ECRIS, FIUs and AROs to streamline cross-border data sharing in particular areas; and the Prüm Decision, Data Retention Directive, TFTP and PNR to combat terrorism and serious crime. SIS, SIS II and VIS appear to be the main exceptions to this pattern: the original purpose of VIS was to facilitate the cross-border exchange of visa data, but this was later extended to preventing and combating terrorism and serious crime. SIS and SIS II aim to ensure a high level of security in the area of freedom, security and justice and facilitate the movement of persons using information communicated via this system. With the exception of these centralised information systems, purpose limitation appears to be a core factor in the design of EU-level information management measures.

Potential overlaps in function

The same personal information may be collected via several different instruments, but may only be used for a limited purpose under a particular instrument (with the exception of VIS, SIS and SIS II). For example, an individual's biographical data, including his or her name, date and place of birth and nationality, may be processed via SIS, SIS II, VIS, API, CIS, the Swedish initiative, the Prüm Decision, ECRIS, FIUs, AROs, Europol, Eurojust and the PNR and TFTP agreements. However, such data may only be processed for the purpose of border control in the case of API; for the prevention, investigation and prosecution of customs fraud in the case of CIS; for criminal investigations and intelligence operations in the case of the Swedish initiative; for the prevention of terrorism and cross-border crime in the case of the Prüm Decision; for examining a person's criminal background in the case of ECRIS; for investigating a person's links with organised crime and terrorist networks in the case of FIUs; for asset tracing in the case of AROs; for investigating and helping to prosecute serious cross-border crime in the case of Europol and Eurojust; to prevent and combat terrorism and other forms of serious transnational crime in the case of PNR; and to identify and pursue terrorists and their financiers in the case of the TFTP. Biometric data, such as fingerprints and photographs, may be processed under SIS II, VIS, EURODAC, the Swedish initiative, the

[81] COM(2010)93, 19.3.2010.

Prüm Decision, ECRIS, Europol and Eurojust — again, for the limited purpose of each measure. The Prüm Decision is the only instrument that enables the cross-border exchange of anonymous DNA profiles (although such data may also be forwarded to Europol and Eurojust). Other measures process highly specialised personal information relevant for their unique objectives: PNR systems process passengers' flight reservation details; FIDE, data relevant for the investigation of customs fraud; the Data Retention Directive, IP addresses and mobile equipment identifiers; ECRIS, criminal records; AROs, private assets and company details; cybercrime platforms, internet offences; Europol, links to criminal networks; and the TFTP, financial messaging data. The cross-border exchange of information and intelligence for criminal investigations provides the only example of a substantial overlap in functions. From a legal point of view, the Swedish initiative would be sufficient to exchange *any* type of information relevant for such investigations (provided that the exchange of such personal data is permitted under national law). From an operational perspective, however, the Prüm Decision may be preferable for sharing DNA profiles and fingerprint data, as its 'hit/no hit' system ensures instantaneous replies and its automated data sharing method guarantees a high level of data security.[82] Likewise, it may be more efficient for FIUs, AROs and cybercrime platforms to liaise directly with their EU counterparts without filling in the forms required by the Swedish initiative to request information.

Controlled access rights

Access rights for instruments triggered by the logic of counter-terrorism and serious crime tend to be limited to a narrower definition of the law enforcement community, i.e. the police, border control and customs authorities. Access rights for measures driven by the 'Schengen' logic are typically granted to immigration authorities and, under certain conditions, the police, border control and customs authorities. The flow of information is controlled by national interfaces in the case of the centralised SIS and VIS and through national contact points or central coordinating units in the case of decentralised instruments, such as the Prüm Decision, the Swedish initiative, the Naples II Convention, ECRIS, TFTP, PNR agreements, FIUs, AROs and cybercrime platforms.

Variable data retention rules

Data retention periods vary widely depending on the objectives of the various instruments. The PNR agreement with the US has the longest data retention period — 15 years, while API has the shortest — 24 hours. The PNR agreements introduce an interesting distinction between data in active and passive use: after a certain period, information must be archived and can only be 'unlocked' by special authorisation. The Canadian use of EU PNR data offers a good example: information must be rendered anonymous after 72 hours, but remains available to authorised officers for 3.5 years.

Effective identity management

Several measures analysed above, including the future SIS II and VIS, aim to allow identity verification through the use of biometric data. The implementation of SIS II is expected to

---

[82] The Prüm Decision (Council Decision 2008/615/JHA, OJ L 210, 6.8.2008, p. 1) has a corresponding implementing decision (Council Decision 2008/616/JHA, OJ L 210, 6.8.2008, p. 12), which aims to guarantee the use of state-of-the-art technical measures to ensure data protection and data security, as well as encryption and authorisation procedures for accessing the data and includes specific rules regulating the admissibility of searches.

enhance security in the area of freedom, security and justice by helping, for example, to identify individuals for whom European Arrest Warrants have been issued, those who are to be refused entry into the Schengen Area and those who are being sought for other specific investigative reasons (such as missing persons or witnesses in court cases) regardless of the availability or authenticity of identification documents. The implementation of VIS ought to facilitate the visa issuing and management process.

Data security via EU solutions

For exchanging sensitive information across European borders, Member States prefer EU solutions. Several instruments of varying size, structure and purpose rely on the Commission-funded s-TESTA data communication network for sharing sensitive information. They include the centralised SIS II, VIS and EURODAC systems, the decentralised Prüm, ECRIS and FIU instruments, as well as Europol and Eurojust. CIS and the FIDE use the Common communication network, Common system interface network or secure web access provided by the Commission. Meanwhile, Europol's SIENA information exchange network application seems to have become the application of choice for some recent initiatives that rely on secure data transfer: there are ongoing discussions on having FIU.net, AROs and cybercrime alert platforms operate on the basis of this application.

Divergent review mechanisms

The instruments analysed above contain a range of different review mechanisms. In the case of complex information systems, such as SIS II, VIS and EURODAC, the Commission must submit to the European Parliament and the Council annual or biannual reports on the operation or state of implementation of these systems. Decentralised information exchange instruments require the Commission to submit to the other institutions a single evaluation report a few years after implementation: the Data Retention Directive, Swedish initiative and ARO measures must be evaluated in 2010; the Prüm Decision in 2012; and ECRIS in 2016. The three PNR agreements provide for periodic and *ad hoc* reviews, and two of them also include sunset clauses. Europol and Eurojust submit annual reports to the Council, which forwards them for information to the European Parliament. These considerations suggest that the current structure of information management in the EU is not conducive to the adoption of a single evaluation mechanism for all instruments. In view of that diversity, it is essential that the future amendment of any instrument in the field of information management take account of its potential impact on all other measures that regulate the collection, storage or exchange of personal data in the area of freedom, security and justice.

4. PRINCIPLES OF POLICY DEVELOPMENT

Section 2 described several initiatives that the European Commission has implemented, presented or considered in recent years. The sheer number of new ideas and the growing body of legislation in the field of internal security and migration management make it necessary to define a core set of principles to serve as a benchmark for the initiation and evaluation of policy proposals in the years to come. These principles build upon and seek to complement the general principles laid down in the EU Treaties, the jurisprudence of the European Court of Justice and European Court of Human Rights and the relevant Inter-Institutional Agreements between the European Parliament, the Council and the European Commission. The Commission proposes to develop and implement new initiatives and evaluate current instruments on the basis of the following two sets of principles:

Substantive principles

Safeguarding fundamental rights, in particular the right to privacy and data protection

Safeguarding persons' fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union, particularly their right to privacy and personal data protection, will be a primary concern for the Commission when developing new proposals that involve the processing of personal data in the field of internal security or migration management. Articles 7 and 8 of the Charter proclaim everyone's right to 'respect for his or her private and family life' and 'the protection of personal data concerning him or her.'[83] Article 16 of the Treaty on the Functioning of the European Union (TFEU), which is binding on the activities of Member States, Union institutions, agencies and bodies, reaffirms everyone's right to 'the protection of personal data concerning them.'[84] When developing new instruments that rely on the use of information technology, the Commission will seek to follow the approach known as 'privacy by design.' This implies embedding personal data protection in the technological basis of a proposed instrument, limiting data processing to that which is necessary for a proposed purpose and granting data access only to those entities that 'need to know.'[85]

Necessity

Interference by a public authority with individuals' right to privacy may be necessary in the interest of national security, public safety or the prevention of crime.[86] The jurisprudence of the European Court of Human Rights establishes three conditions under which such restrictions may be justified: if it is lawful, if it pursues a legitimate aim and if it is necessary in a democratic society. Interference with the right to privacy is considered necessary if it answers a pressing social need, if it is proportionate to the aim pursued and if the reasons put forward by the public authority to justify it are relevant and sufficient.[87] In all future policy proposals, the Commission will assess the initiative's expected impact on individuals' right to privacy and personal data protection and set out why such an impact is necessary and why the proposed solution is proportionate to the legitimate aim of maintaining internal security within the European Union, preventing crime or managing migration. Compliance with the rules on personal data protection will in all cases be subject to control by an independent authority at national or EU level.

Subsidiarity

The Commission will seek to justify its new proposals in the light of the principles of subsidiarity and proportionality, in line with Article 5 of Protocol No 2 attached to the Treaty on European Union. Any new legislative proposal will contain a statement making it possible to appraise compliance with the principle of subsidiarity, as laid down in Article 5 of the Treaty on European Union. This statement will contain an assessment of the proposal's financial, economic and social impact and, in the case of a directive, of its implications for the

---

83 Charter of Fundamental Rights of the European Union, OJ C 83, 30.3.2010, p. 389.

84 Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, OJ C 83, 30.3.2010.2008, p. 1.

85 For a comprehensive description of 'privacy by design,' refer to the Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy, European Data Protection Supervisor, 18.3.2010.

86 See Article 8, Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No 5), Council of Europe, 4.11.1950.

87 See *Marper v the United Kingdom*, European Court of Human Rights judgment, Strasbourg, 4.12.2008.

rules to be put in place by Member States.[88] The reasons for concluding that an EU objective can be better achieved at EU level will be substantiated by qualitative indicators. Legislative proposals will take account of the need for any burden falling upon the EU, national governments, regional authorities, economic operators and citizens to be minimised and commensurate with the objective to be achieved. In the case of proposals calling for new international agreements, this statement will consider the proposal's expected impact on relations with the third countries in question.

Accurate risk management

Information in the area of freedom, security and justice is typically exchanged to analyse security threats, identify trends in criminal activity or assess risks in related policy areas.[89] Risk is often, but not necessarily, linked to individuals whose past behaviour or pattern of behaviour indicates a continued risk in the future. However, risks should be based on evidence and not be hypothetical. Necessity tests and purpose limitation are essential for any information management measure. The development of risk profiles — not to be confused with racial or otherwise discriminatory profiling, which is incompatible with fundamental rights — is relevant. Such profiles can help in focusing resources on specific individuals for the purpose of identifying security threats and protecting victims of crime.

Process-oriented principles[90]

Cost-effectiveness

Public services based on information technology should enable the delivery of better services and greater value for taxpayers. In view of the current economic climate, all new proposals, particularly where they concern the establishment or upgrading of information systems, will aim to be as cost-effective as possible. Such an approach will take account of pre-existing solutions to minimise overlap and to maximise possible synergies. The Commission will assess whether it may be possible to accomplish a proposal's objectives through better use of existing instruments. It will also consider adding auxiliary functions to existing information systems before proposing new systems.

Bottom-up policy design

The development of new initiatives must, at the earliest possible stage, draw on the input of all relevant stakeholders, including national authorities responsible for implementation, economic actors and civil society. Designing policies that take the interests of end-users into account requires horizontal thinking and wide-ranging consultation.[91] For this reason, the Commission will seek to establish permanent liaison with national officials and practitioners through Council structures, management committees and *ad hoc* formations.

---

88 The basic principles of impact assessments are set out in the European Commission's Impact Assessment Guidelines (SEC(2009)92, 15.1.2009).

89 Practical examples of risks successfully managed include preventing an expelled person who committed a serious crime in one Member State from re-entering the Schengen area via another Member State (SIS) or preventing a person from applying for asylum in several Member States (EURODAC).

90 These principles draw on the Council Conclusions on an Information Management Strategy for EU internal security, Justice and Home Affairs Council, 30.11.2009.

91 The general principles and minimum standards of public consultation are set out in COM(2002)704, 11.12.2002.

Clear allocation of responsibilities

In view of the technical complexity of information collection and exchange projects in the area of freedom, security and justice, particular attention must be paid to the initial design of governance structures. The experience of the SIS II project demonstrates that a failure to define clear and stable overarching objectives, roles and responsibilities early on may lead to significant cost overruns and delays in implementation. An early assessment of the Prüm Decision's implementation experience suggests that a decentralised governance structure may be no panacea either, as Member States have no project leader to turn to for advice concerning the financial or technical aspects of implementation. The future IT Agency may be able to provide such technical advice to the custodians of information systems in the area of freedom, security and justice. It can also offer a platform for the wide-ranging involvement of stakeholders in the operational management and development of IT systems. As a possible safeguard against cost overruns and delays resulting from changing requirements, any new information system in the area of freedom, security and justice, particularly if it involves a large-scale IT system, will not be developed before the underlying legal instruments setting out its purpose, scope, functions and technical details have been definitively adopted.

Review and sunset clauses

The Commission will evaluate each instrument covered in this communication. This will be done in relation to the whole range of instruments that exist in the field of information management. This should yield a reliable picture of how individual instruments fit into the broader landscape of internal security and migration management. Future proposals will include, where appropriate, an annual reporting obligation, periodic and *ad hoc* reviews, as well as a sunset clause. Existing instruments will only be maintained if they continue to serve the legitimate purpose for which they were designed. Annex II sets out the review date and mechanism for each instrument covered in this communication.

5. THE WAY FORWARD

This communication provides, for the first time, a clear and comprehensive summary of the EU-level measures in place, under implementation or consideration that regulate the collection, storage or cross-border exchange of personal information for the purpose of law enforcement or migration management.

It gives citizens an overview of what information is collected, stored or exchanged about them, for what purpose and by whom. It is a transparent reference tool for stakeholders who wish to engage in debate about the future direction of EU policy in this area. At the same time, it provides a first response to the call by the European Council for developing EU-level information management instruments in accordance with the EU Information Management Strategy[92] and for reflection on the need for a European Information Exchange Model.[93]

---

92 Council Conclusions on an Information Management Strategy for EU internal security, Justice and Home Affairs Council, 30.11.2009 (EU Information Management Strategy).

93 The Stockholm Programme — An open and secure Europe serving and protecting citizens, Council Document 5731/10, 3.3.2010, Section 4.2.2.

The Commission aims to follow up this communication by presenting a communication on the European Information Exchange Model in 2012.[94] To that end, the Commission launched an 'information mapping' exercise in January 2010 on the legal bases and practical operation of the exchange between Member States of criminal intelligence and information, the results of which the Commission aims to present to the Council and the European Parliament in 2011.[95]

Finally, this communication sets out, for the first time, the Commission's vision of the broad principles that it intends to follow in the future development of instruments for data collection, storage or exchange. These principles will also be used when evaluating existing instruments. Adopting such a principled approach to policy development and evaluation is expected to enhance the coherence and effectiveness of current and future instruments in a manner that fully respects citizens' fundamental rights.

[94] This is indicated in the Commission's Stockholm Programme Action Plan (COM(2010)171, 20.4.2010).

[95] This information mapping exercise is conducted in close cooperation with an Information Mapping Project Team made up of representatives of EU and EFTA Member States, Europol, Eurojust, Frontex and the European Data Protection Supervisor.

ANNEX I

The following data and examples aim to illustrate the operation in practice of information management measures currently in operation.

Schengen Information System (SIS)

Total number of SIS alerts entered in the central SIS (C.SIS) database[96]			
Alert categories	**2007**	**2008**	**2009**
Banknotes	177,327	168,982	134,255
Blank documents	390,306	360,349	341,675
Firearms	314,897	332,028	348,353
Issued documents	17,876,227	22,216,158	25,685,572
Vehicles	3,012,856	3,618,199	3,889,098
Wanted persons (aliases)	299,473	296,815	290,452
Wanted persons (main name)	859,300	927,318	929,546
Of which:			
Persons wanted for arrest for extradition	19,119	24,560	28,666
Third-country nationals on the entry ban list	696,419	746,994	736,868
Adult missing persons	24,594	23,931	26,707
Minor missing persons	22,907	24,628	25,612
Witnesses or persons subject to judicial summons	64,684	72,958	78,869
Persons subject to exceptional monitoring to prevent threats to public security	31,568	34,149	32,571
Persons subject to exceptional monitoring to prevent threats to national security	9	98	253
Total	**22,933,370**	**27,919,849**	**31,618,951**

[96] Council Document 6162/10, 5.2.2010; Council Document 5764/09, 28.1.2009; Council Document 5441/08, 30.1.2008.

EURODAC – The movement of asylum-seekers who submitted new applications in the same or other Member States (2008)

Member States sending fingerprints for comparison and obtaining 'hits' from Member States (columns) where a person previously applied for asylum	Member State where the first asylum application was submitted[97]																													Total 2nd applications	
	AT	BE	BG	CH	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HU	IE	IS	IT	LT	LU	LV	MT	NL	NO	PL	PT	RO	SE	SI	SK	UK	**Home hits**	**Total hits**
AT	1,725	74	2	0	1	87	274	5	2	31	12	25	115	212	5	0	134	3	14	0	9	52	49	1,371	1	42	111	17	260	61	**1,725**	**4,694**
BE	180	5,450	4	0	3	38	408	17	0	41	17	28	378	67	28	0	69	3	37	0	2	180	73	625	6	3	192	17	58	205	**5,450**	**8,129**
BG	5	2	116	0	1	1	5	1	0	7	0	0	0	1	0	0	1	0	2	0	0	1	3	0	0	6	8	0	0	4	**116**	**164**
CH	32	52	1	4	3	5	35	0	0	17	17	8	39	19	1	0	355	0	1	0	13	15	37	3	1	0	41	4	4	25	**4**	**732**
CY	1	0	0	0	68	0	1	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	**68**	**73**
CZ	55	12	0	0	0	637	48	4	0	0	3	4	13	0	1	0	8	2	1	0	0	7	6	17	1	0	13	0	1	6	**637**	**839**
DE	260	268	12	0	4	79	1,852	42	0	174	39	56	256	106	9	2	200	5	26	2	5	174	137	149	4	43	567	30	89	128	**1,852**	**4,718**
DK	44	43	3	0	0	13	126	119	0	27	13	44	36	13	4	0	47	0	7	0	0	30	225	55	2	4	436	2	7	41	**119**	**1,341**
EE	0	0	0	0	0	0	1	1	0	0	0	8	0	0	0	0	0	0	0	0	0	0	1	0	0	0	3	0	0	9	**0**	**23**
EL	66	88	27	0	12	9	131	10	0	766	8	8	35	3	9	0	48	0	1	0	0	33	24	3	0	13	141	0	8	316	**766**	**1,759**
ES	16	18	2	0	1	3	37	1	0	11	108	0	29	4	5	0	35	0	0	0	0	9	9	4	6	0	21	5	1	16	**108**	**341**
FI	37	44	1	0	1	10	115	25	0	48	5	229	14	30	10	1	194	0	3	0	90	49	107	44	2	4	362	3	3	81	**229**	**1512**
FR	365	339	0	0	8	97	502	29	0	92	78	31	860	161	8	0	336	11	26	1	29	106	74	1,739	8	9	286	37	75	190	**860**	**5,497**
HU	297	53	4	0	1	3	169	4	0	2	3	19	70	791	1	0	27	1	10	0	0	28	32	0	0	76	79	19	14	14	**791**	**1,717**
IE	20	21	0	0	4	2	24	1	0	9	8	0	23	4	309	0	35	0	4	0	4	16	7	0	0	0	22	2	2	187	**309**	**704**
IS	4	3	0	0	0	0	3	0	0	3	1	1	6	2	1	0	3	0	1	0	1	3	10	1	0	0	11	1	0	3	**0**	**58**
IT	390	111	5	0	6	33	349	11	0	270	47	27	192	60	23	5	3,290	0	11	0	58	78	116	9	2	6	201	59	224	680	**3,290**	**6,263**
LT	3	1	0	0	1	3	0	0	0	0	1	0	1	0	0	0	0	5	0	0	0	0	4	14	0	0	5	0	2	0	**5**	**40**
LU	7	21	4	0	0	0	12	2	0	0	0	1	9	6	0	1	8	0	2	0	1	6	4	0	0	0	10	3	1	3	**2**	**101**
LV	3	1	0	0	0	0	1	0	1	0	0	0	1	0	0	0	0	5	0	0	0	0	0	0	0	0	1	0	2	0	**0**	**15**
MT	1	0	0	0	0	0	0	0	0	0	0	5	1	0	0	0	6	0	0	0	16	0	1	0	0	0	1	1	0	0	**16**	**32**
NL	109	223	16	0	1	27	198	21	0	113	16	29	109	33	7	1	226	0	14	0	58	1,240	95	16	8	9	289	8	22	129	**1,240**	**3,017**
NO	84	103	6	0	2	13	256	76	0	199	55	57	78	23	8	0	524	8	13	1	83	86	276	164	1	9	826	10	21	96	**276**	**3,078**
PL	188	65	0	0	0	30	68	15	0	0	2	4	75	1	1	0	0	3	3	0	0	7	27	1,208	1	1	43	1	13	4	**1,208**	**1,760**
PT	1	10	0	0	0	0	4	1	0	0	11	0	9	0	0	0	2	0	2	0	0	2	2	0	3	0	2	0	1	2	**3**	**52**
RO	43	2	5	0	1	9	33	0	0	3	0	5	14	11	0	0	0	0	1	0	0	9	1	1	0	64	17	0	4	4	**64**	**227**
SE	243	133	30	0	4	36	516	173	0	143	29	143	145	80	16	3	276	0	16	0	130	98	430	147	5	13	1,914	11	26	122	**1,914**	**4,882**
SI	14	4	0	0	0	1	10	1	0	1	1	2	15	6	0	0	5	0	1	0	0	2	3	0	0	0	5	45	3	2	**45**	**121**
SK	105	4	0	0	0	7	33	0	1	0	0	1	2	12	0	0	3	0	0	1	0	4	4	4	0	0	9	2	195	6	**195**	**393**
UK	109	153	7	0	3	12	276	30	0	108	6	38	209	25	217	2	768	0	8	0	43	128	76	7	4	11	174	6	46	3,141	**3,141**	**5,607**
Total 1st applications	**4,407**	**7,298**	**245**	**4**	**125**	**1,155**	**5,487**	**589**	**4**	**2,067**	**480**	**773**	**2,734**	**1,670**	**663**	**15**	**6,600**	**46**	**204**	**5**	**542**	**2,363**	**1,833**	**5,581**	**55**	**313**	**5,791**	**283**	**1,082**	**5,475**	**24,433**	**57,889**

[97] COM(2009)494, 25.9.2009. 'Home hits' refer to the submission of a new asylum application in the Member State where the previous one was submitted.

Advance Passenger Information (API) System

The United Kingdom's use of Advance Passenger Information for improving border control and combating irregular migration[98]	
Number of actions taken in 2009	
Previous adverse history (person refused entry)	379
Lost, stolen or cancelled passports (document impounded)	56

[98] The UK Border Agency provided this information to the Commission for the purpose of this communication.

Customs Information System (CIS)

Total number of cases entered in CIS database (2009)[99]	
Action	**CIS (based on CIS Convention)**
Cases created	2,007
Active cases	274
Queried cases	11,920
Deleted cases	1,355

[99] This information was supplied by the Commission.

Swedish initiative

Examples of the use of the Swedish initiative to investigate criminal offences[100]	
Homicide	In 2009, a homicide attempt took place in a Member State capital. The police collected a biological sample from a glass from which the suspect had been drinking. Extracting DNA from this sample, forensic scientists generated a DNA profile. A comparison of this profile with other reference profiles in the national DNA database did not yield a match. Therefore, the investigating police force sent, via its Prüm contact point, a request for comparing it with DNA reference profiles held by other Member States that had been authorised to exchange such data on the basis of the Prüm Decision or Prüm Agreement. This cross-border comparison produced a 'hit.' On the basis of the Swedish initiative, the investigating police force requested further data about the suspect. Its national contact point received a reply from several other Member State within 36 hours, which enabled the police to identify the suspect.
Rape	In 2003, an unidentified suspect raped a woman. The police collected samples from the victim, but the DNA profile generated from the sample did not match any reference profile in the national DNA database. A request for DNA comparison, sent by the Prüm contact point to other Member States that had been authorised to exchange DNA reference profiles on the basis of the Prüm Decision or Prüm agreement, produced a 'hit.' The investigating police force then requested further information about the suspect under the Swedish initiative. Its national contact point received a reply within eight hours, which enabled the police to identify the suspect.

[100] A Member State police force provided these examples to the Commission for the purpose of this communication.

Germany obtaining 'hits' in the cross-border comparison of DNA profiles, according to the type of offence (2009)[101]

Hits by type of offence	Austria	Spain	Luxembourg	Netherlands	Slovenia
Offences against public interests	32	4	0	5	2
Offences against personal freedom	9	3	5	2	0
Sexual offences	40	22	0	31	4
Crimes against the person	49	24	0	15	2
Other offences	3,005	712	18	1,105	71

[101] German Government's reply to Parliamentary Question by Ulla Jelpke, Inge Höger and Jan Korte (Reference No 16/14120), Bundestag, 16th Session, Reference No 16/14150, 22.10.2009. These figures relate to the period commencing with a Member State beginning data exchange with Germany and ending on 30 September 2009.

Data Retention Directive

Examples of Member States detecting cases of serious crime via data retention[102]	
Murder	A Member State police authority managed to trace a group of murderers responsible for the racially motivated killing of six individuals. The perpetrators tried to evade capture by changing their SIM cards, but their dial lists and mobile equipment identifiers gave them away.
Homicide	A police authority was able to prove the involvement of two suspects in a homicide case by analysing traffic data from the victim's mobile phone. This allowed detectives to reconstruct the route that the victim and the two suspects had travelled together.
Burglary	Authorities traced an offender responsible for 17 burglaries by studying traffic data from his anonymous prepaid SIM card. By identifying his girlfriend, they were able to locate the offender too.
Fraud	Investigators unravelled a scam in which a gang advertising expensive motorcars on the internet 'for cash' systematically robbed those who turned up to take possession of their vehicles. An IP address allowed the police to trace the subscriber and arrest the offenders.

[102] These anonymous examples are based on Member States' replies to a 2009 Commission questionnaire concerning the transposition of Directive 2006/24/EC (Data Retention Directive).

Financial Intelligence Unit (FIU) cooperation

Total number of information requests made by national FIUs via FIU.net[103]		
Year	**Information requests**	**Active users**
2007	3,133	12 Member States
2008	3,084	13 Member States
2009	3,520	18 Member States

[103] The FIU.net Bureau provided this information to the Commission for the purpose of this communication.

Asset Recovery Office (ARO) cooperation

Asset tracing requests submitted by Member States and handled by Europol[104]				
Year	**2004**	**2005**	**2006**	**2007**
Requests	5	57	53	133
Of which:				
Cases related to fraud				29
Cases related to money laundering				26
Cases related to drugs				25
Cases related to other offences				18
Cases related to drugs and money laundering				19
Cases related to fraud and money laundering				7
Cases related to mix of offences				9

Asset confiscation cases handled by Eurojust (2006-2007)[105]			
Case types		**Cases initiated by**	
Cases related to environmental crime	1	Germany	27%
Cases related to participation in a criminal organisation	5	Netherlands	21%
Cases related to drug trafficking	15	UK	15%
Cases related to tax fraud	8	Finland	13%
Cases related to fraud	8	France	8%
Cases related to VAT fraud	1	Spain	6%
Cases related to money laundering	9	Portugal	4%
Cases related to corruption	1	Sweden	2%
Cases related to crime against property	2	Denmark	2%
Cases related to trafficking in arms	1	Latvia	2%
Cases related to counterfeiting and product piracy	2		
Cases related to advance fee fraud	2		
Cases related to the forgery of administrative documents	1		
Cases related to vehicle crime	1		
Cases related to terrorism	1		
Cases related to forgery	2		
Cases related to trafficking in human beings	1		

104 Assessing the effectiveness of EU Member States' practices in the identification, tracing, freezing and confiscation of criminal assets – Final Report (for European Commission, DG JLS), Matrix Insight, 6.2009.

105 *Ibid*.

Cybercrime Alert Platforms

Examples of the French Cybercrime Alert Platform, Pharos, investigating cases of cybercrime[106]	
Child pornography	An internet user alerted Pharos to the existence of a blog containing photographs and cartoon-style images of child sexual abuse. The blog's editor, appearing nude in one picture, also groomed children on his blog. Investigators identified a mathematics tutor as their main suspect. A search of his home turned up 49 videos containing images of child pornography. The enquiry also revealed that he had made preparations to set up a home tutoring course. The defendant was subsequently convicted and given a suspended prison sentence.
Child sexual abuse	The French police was tipped off about an individual offering money on the internet for sex with children. A Pharos detective posing as a minor made contact with the suspect, who offered him cash for sex. The ensuing internet chat enabled Pharos to identify the suspect's Internet Protocol address, tracing him to a town known for its high incidence of child sexual abuse. The defendant was subsequently convicted and sentenced to a suspended term of imprisonment.

[106] Pharos stands for *plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements*.

Examples of Europol's contribution to the fight against cross-border serious crime[107]	
Operation Andromeda	In December 2009, Europol helped implement a large cross-border police operation against a drug-trafficking network with contacts in 42 countries. This network was based in Belgium and Norway and trafficked drugs from Peru, via the Netherlands, to Belgium, the UK, Italy and other Member States. Police cooperation was coordinated by Europol; judicial cooperation by Eurojust. The participating authorities set up a mobile office in Pisa; Europol, an operations room in The Hague. Europol cross-referenced information between the suspects and produced a report depicting the criminal network.
Participants	Italy, the Netherlands, Germany, Belgium, the United Kingdom, Lithuania, Norway and Eurojust.
Results	Participating police forces seized 49 kg of cocaine, 10 kg of heroin, 6000 ecstasy pills, two firearms, five false identity documents and €43,000 in cash and arrested 15 persons.
Operation Typhon	Between April 2008 and February 2010, Europol provided analytical support to police forces from 20 countries involved in Operational Typhon. In this large operation against a paedophile network distributing images of child pornography via an Austrian website, Europol performed technical support and criminal intelligence analysis on the basis of the images received from Austria. It then assessed the reliability of the data and restructured it before preparing its own intelligence material. By cross-referencing the data with information contained in its Analytical Work File, it produced 30 intelligence reports that triggered investigations in several countries.
Participants	Austria, Belgium, Bulgaria, Canada, Denmark, France, Germany, Hungary, Italy, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Romania, Slovakia, Slovenia, Spain, Switzerland and the United Kingdom.
Results	Participating forces identified 286 suspects, arrested 118 suspects and rescued five victims in four countries who suffered abuse in this case.

[107] Europol provided this information to the Commission for the purpose of this communication. Further information on Operation Andromeda may be accessed on http://www.eurojust.europa.eu/.

Examples of Eurojust coordinating large cross-border judicial operations against serious crime[108]	
Trafficking in human beings and terrorist financing	In May 2010, Eurojust coordinated a cross-border operation that resulted in the arrest of five members of an organised crime network active in Afghanistan, Pakistan, Romania, Albania and Italy. The group equipped Afghan and Pakistani nationals with forged documents, trafficking them via Iran, Turkey and Greece to Italy. Upon arrival in Italy, the migrants were despatched to Germany, Sweden, Belgium, the UK and Norway. The proceeds of trafficking were intended to finance terrorism.
Bank card fraud	By coordinating cross-border police and judicial cooperation, Europol and Eurojust helped unravel a bank card fraud network active in Ireland, Italy, the Netherlands, Belgium and Romania. This network stole the identification data of some 15,000 payment cards, causing a loss of €6.5 million. In advance of this operation, which resulted in 24 arrests in July 2009, Belgian, Irish, Italian, Dutch and Romanian magistrates facilitated the issuing of European Arrest Warrants and requests for wiretapping against the suspects.
Trafficking in human beings and drugs	Following a coordination meeting organised by Eurojust in March 2009, Italian, Dutch and Colombian authorities arrested 62 individuals suspected of trafficking human beings and drugs. This network trafficked vulnerable women from Nigeria to the Netherlands, forcing them into prostitution in Italy, France and Spain. The proceeds of prostitution financed the network's purchase of cocaine in Colombia, shipped to the EU for consumption.

[108] These examples originate from http://www.eurojust.europa.eu/.

Passenger Name Records (PNR)

Examples of PNR analysis yielding information for investigating serious cross-border crime[109]	
Child trafficking	PNR analysis revealed that three unaccompanied children were travelling from an EU Member State to a third country, with no indication of who would meet them upon arrival. Alerted by the Member State's police after departure, the third country's authorities arrested the person who turned up to receive the children: a sex offender registered in the Member State.
Trafficking in human beings	PNR analysis uncovered a group of human traffickers always travelling on the same route. Using fake documents to check in for an intra-EU flight, they would use authentic papers to simultaneously check in for another flight bound for a third country. Once in the airport lounge, they would board the intra-EU flight.
Credit card fraud	Several families travelled to a Member State with tickets purchased by stolen credit cards. Research showed that a criminal group used these cards to purchase the tickets, selling them over the counter in long-distance call centres. It was PNR data that linked the travellers to the credit cards and vendors.
Drug trafficking	A Member State police authority had information suggesting that a man was involved in drug trafficking from a third country, but border guards never found anything on him when he arrived in the EU. PNR analysis revealed that he always travelled with an associate. An inspection of his associate yielded large quantities of drugs.

[109] These examples have been rendered anonymous to protect the sources of the information.

Terrorist Finance Tracking Program (TFTP)

Examples of the TFTP yielding information for investigating terrorist plots[110]	
2008 Barcelona terrorist plot	In January 2008, ten suspects were arrested in Barcelona in connection with a foiled attempt to carry out an attack on the city's public transport system. TFTP data were used to identify the suspects' links to Asia, Africa and North America.
2006 transatlantic liquid bomb plot	TFTP information was used to investigate and convict individuals in connection with a foiled plot to blow up, in August 2006, ten transatlantic flights bound for the US and Canada from the UK.
2005 London bombings	TFTP data were used to provide new leads to investigators, corroborate suspects' identities and reveal relationships between individuals responsible for this attack.
2004 Madrid bombings	TFTP data were provided to several EU Member States to aid their investigations launched in the wake of this attack.

[110] Second report on the processing of EU-originating personal data by the United Stated Treasury Department for counter-terrorism purposes, Judge Jean-Louis Bruguière, January 2010.

ANNEX II

Table form overview of instruments in operation, under implementation or consideration

Instrument	Background	Purpose(s)	Structure	Personal data coverage	Access to data	Data protection	Data retention	Implementation state	Review
Schengen Information System (SIS)	Initiated by Member States.	To maintain public security, including national security, within the Schengen area and facilitate the movement of persons using information communicated via this system.	Centralised: N.SIS (national parts) connected by interface to C.SIS (central part).	Names and aliases, physical characteristics, place and date of birth, nationality and whether a person is armed or violent. SIS alerts relate to several different groups of persons.	Police, border police, customs, judicial authorities have access to all data; immigration and consular authorities to the entry ban list and lost and stolen documents. Europol and Eurojust can access some data.	Council of Europe (CoE) Convention 108 and CoE Police Recommendation R (87) 15.	Personal data entered in SIS for the purpose of tracing persons may be kept only for the time required to meet the purpose for which they were supplied, and no longer than three years. Data on persons subject to exceptional monitoring on account of the threat they pose to public or national security must be deleted after one year.	SIS is fully applicable in 22 Member States plus Switzerland, Norway and Iceland. The UK and Ireland participate in SIS, with the exception of alerts on third-country nationals on the entry ban list. Bulgaria, Romania and Liechtenstein are expected to implement this measure soon.	Signatories may propose amendments to the Schengen Convention. The amended text would have to be adopted by unanimity and ratified by parliaments.

Table form overview of instruments in operation, under implementation or consideration

Instrument	Background	Purpose(s)	Structure	Personal data coverage	Access to data	Data protection	Data retention	Implementation state	Review
Schengen Information System II (SIS II)	Initiated by the Commission.	To ensure a high level of security in the area of freedom, security and justice and facilitate the movement of persons using information communicated via this system.	Centralised: N.SIS II (national parts) connected by interface to CS-SIS (central part). SIS II will run on the secure s-TESTA network.	The data categories in SIS plus fingerprints and photographs, copies of European Arrest Warrant, misused identity alerts and links between alerts. SIS II alerts relate to several different groups of persons.	Police, border police, customs, judicial authorities will have access to all data; immigration and consular authorities to the entry ban list and lost and stolen documents. Europol and Eurojust will be able to access some data.	Specific rules established under the basic legal acts governing SIS II and Directive 95/46/EC, Regulation (EC) 45/2001, Council Framework Decision 2008/977/JHA, Regulation (EC) 45/2011, CoE Convention 108 and CoE Police Recommendation R (87) 15.	Personal data entered in SIS for the purpose of tracing persons may be kept only for the time required to meet the purpose for which they were supplied, and no longer than three years. Data on persons subject to exceptional monitoring on account of the threat they pose to public or national security must be deleted after one year.	SIS II is under implementation. Once operational, it will be applicable in the EU-27, Switzerland, Liechtenstein, Norway and Iceland. The UK and Ireland will participate in SIS II, with the exception of alerts on third-country nationals on the entry ban list.	The Commission must send biannual progress reports to the European Parliament (EP) and the Council on the development of SIS II and potential migration from SIS.
EURODAC	Initiated by the Commission.	To assist in determining which Member State should assess an asylum application.	Centralised, consisting of national access points connected by an interface to the EURODAC central unit. EURODAC runs on the s-TESTA network.	Fingerprint data, sex, the place and date of the application for asylum, the reference number used by the Member State of origin and the date on which the fingerprints were taken, transmitted and entered in the system.	Member States must specify the list of authorities with access to the data, which typically includes asylum and migration authorities, border guards and the police.	Directive 95/46/EC.	10 years for asylum-seekers' fingerprints; 2 years for those of third country nationals apprehended in connection with the irregular crossing of an external border.	The EURODAC Regulation is in force in each Member State, Norway, Iceland and Switzerland. An agreement enabling Liechtenstein's connection is awaiting conclusion.	The Commission must send an annual report to the EP and the Council on the operation of the EURODAC central unit.

Table form overview of instruments in operation, under implementation or consideration

Instrument	Background	Purpose(s)	Structure	Personal data coverage	Access to data	Data protection	Data retention	Implementation state	Review
Visa Information System (VIS)	Initiated by the Commission.	To help implement a common visa policy and prevent threats to internal security.	Centralised, consisting of national parts that will be connected by an interface to the central part. VIS will run on the s-TESTA network.	Visa applications, fingerprints, photographs, related visa decisions and links between related applications.	Visa, asylum, immigration and border control authorities will have access to all data. The police and Europol may consult VIS for the prevention, detection and investigation of serious crime.	Specific rules established by basic legal acts governing VIS and Directive 95/46/EC, Regulation (EC) 45/2001, Council Framework Decision 2008/977/JHA, CoE Convention 108, CoE Additional Protocol 181 and CoE Police Recommendation R (87) 15.	5 years.	VIS is under implementation and will be applicable in each Member State (except the UK and Ireland) plus Norway, Iceland and Switzerland.	The Commission must report to the EP and the Council on the operation of VIS three years after its launch and every four years thereafter.
Advance Passenger Information System (API)	Initiated by Spain.	To improve border control and combat irregular migration.	Decentralised.	Personal data from passports, the point of embarkation and the EU entry point.	Border control authorities and, upon request, law enforcement authorities.	Directive 95/46/EC.	Data must be deleted 24 hours after a flight's arrival in the EU.	API is in force in each Member State, but only a few of them use it.	The Commission will evaluate the API system in 2011.

Table form overview of instruments in operation, under implementation or consideration

Instrument	Background	Purpose(s)	Structure	Personal data coverage	Access to data	Data protection	Data retention	Implementation state	Review
Naples II Convention	Initiated by Member States.	To help national customs authorities prevent and detect infringements of national customs provisions and to help them prosecute and punish infringements of Community and national customs provisions.	Decentralised, operating through a set of central coordinating units.	All information relating to an identified or identifiable person.	Central coordinating units forward data to national customs authorities, investigative authorities and judicial bodies and, subject to the prior consent of the Member State supplying the data, to other authorities.	Directive 95/46/EC and CoE Convention 108. The data in the receiving Member State must enjoy a level of protection at least equivalent to that in the supplying Member State.	The data may be kept for a period not exceeding that necessary for the purpose for which they were supplied.	This Convention has been ratified by each Member State.	Signatories may propose amendments to the Naples II Convention. The amended text would have to be adopted by the Council and ratified by Member States.
Customs Information System (CIS)	Initiated by Member States.	To assist competent authorities to prevent, investigate and prosecute serious violations of national customs laws.	Centralised, accessible via terminals in each Member State and at the Commission. CIS and FIDE operate on the basis of AFIS, which uses the Common communication network, Common system interface network or secure web access provided by the Commission.	Names and aliases, date and place of birth, nationality, sex, physical characteristics, identity documents, address, any history of violence, the reason for entering data in CIS, suggested action and the registration of the means of transport.	National customs authorities, Europol and Eurojust may access CIS data.	Specific rules established by the CIS Convention and Directive 95/46/EC, Regulation (EC) No 45/2001, CoE Convention 108 and CoE Police Recommendation No R (87) 15.	Personal data copied from CIS to other systems for risk management or operational analyses may only be kept for the time necessary to achieve the purpose for which they were copied and no longer than 10 years.	In force in each Member State.	The Commission, in cooperation with Member States, reports each year to the EP and the Council on the operation of CIS.

Table form overview of instruments in operation, under implementation or consideration

Instrument	Background	Purpose(s)	Structure	Personal data coverage	Access to data	Data protection	Data retention	Implementation state	Review
Swedish initiative	Initiated by Sweden.	To streamline information exchange for the purpose of criminal investigations and criminal intelligence operations.	Decentralised, Member States must designate national contact points that handle urgent requests for information.	Any existing information or criminal intelligence available to law enforcement authorities.	Police, customs and any other authority with the power to investigate crime (with exception of intelligence services).	National data protection rules, as well as CoE Convention 108, CoE Additional Protocol 181 and CoE Police Recommendation No R (87) 15.	Information and intelligence supplied under this instrument may only be used for the purpose for which they were supplied and under specific conditions set by the supplying Member State.	12 of the 31 signatories (EU and EFTA states) have passed national laws to implement this instrument; five fill in the form to request data; and two use it frequently to exchange information.	The Commission is to submit its evaluation report to the Council in 2010.
Prüm Decision	Initiated by Member States.	To enhance the prevention of crime, particularly terrorism, and maintain public order.	Decentralised, interconnected via the s-TESTA network. National contact points handle outgoing and incoming requests for data comparison.	Anonymous DNA profiles and fingerprints, vehicle registration data and information about individuals suspected of links to terrorism.	Contact points transmit requests; domestic access is governed by national law.	Specific rules established by the Prüm Decision and CoE Convention 108, CoE Additional Protocol 181 and CoE Police Recommendation No R (87) 15. Individuals may turn to their national data protection supervisor to enforce their rights concerning the processing of personal data.	Personal data must be deleted once they are no longer necessary for the purpose for which they were supplied. The maximum domestic data retention period of the supplying state is binding on the receiving state.	The Prüm Decision is under implementation. Ten Member States have been authorised to exchange DNA, five to exchange fingerprints, seven to exchange vehicle registration data. Norway and Iceland are about to accede to this instrument.	The Commission is to submit its evaluation report to the Council in 2012.

Table form overview of instruments in operation, under implementation or consideration

Instrument	Background	Purpose(s)	Structure	Personal data coverage	Access to data	Data protection	Data retention	Implementation state	Review
Data Retention Directive	Initiated by Member States.	To enhance the investigation, detection and prosecution of serious crime by retaining telecommunication traffic and location data.	Decentralised, this instrument imposes obligations on telecommunication service providers to retain data.	Telephone number, IP address and mobile equipment identifier.	Authorities with access rights are nationally defined.	Directive 95/46/EC and Directive 2002/58/EC.	Ranging from 6 to 24 months.	Six Member States have not yet transposed this directive, and the German and Romanian constitutional courts ruled implementing laws to be unconstitutional.	The Commission is to submit its evaluation report to the EP and the Council in 2010.
European Criminal Records Information System (ECRIS)	Initiated by Belgium and proposed by the Commission.	To improve cross-border data sharing concerning EU citizens' criminal records.	Decentralised, interconnected via a set of central authorities that will exchange information extracted from criminal records using the s-TESTA network.	Biographical data; conviction, sentence and offence; additional data, including fingerprints (if available).	Judicial and competent administrative authorities.	Specific rules established by Council Framework Decision 2009/315/JHA, which incorporates the rules of Council Decision 2005/876/JHA, as well as Council Framework Decision 2008/977/JHA, CoE Convention 108 and Regulation (EC) No 45/2001.	Domestic data retention rules apply, as this instrument only regulates data exchange.	ECRIS is under implementation. Nine Member States have started exchanging information electronically.	The Commission is to submit two evaluation reports to the EP and Council: on Framework Decision 2008/675/JHA in 2011; on Framework Decision 2009/315/JHA in 2015. As of 2016, the Commission must publish regular reports on the operation of Council Decision 2009/316/JHA (ECRIS).

Table form overview of instruments in operation, under implementation or consideration

Instrument	Background	Purpose(s)	Structure	Personal data coverage	Access to data	Data protection	Data retention	Implementation state	Review
Financial Intelligence Unit cooperation (FIU.net)	Initiated by the Netherlands.	To exchange information necessary for analysing and investigating money laundering and terrorist financing.	Decentralised, FIUs exchange data via FIU.net, which runs on the s-TESTA network. Europol's SIENA application may soon underpin FIU.net.	Any data of relevance to the analysis or investigation of money laundering and terrorist financing.	Financial Intelligence Units (within police forces, judicial authorities or administrative authorities reporting to financial authorities).	Council Framework Decision 2008/977/JHA, CoE Convention 108 and CoE Police Recommendation R (87) 15.	Domestic data retention rules apply, as this instrument only regulates data exchange.	Twenty Member States participate in FIU.net, an online data-sharing application running on s-TESTA.	As part of its Financial Services Action Plan, the Commission has been reviewing the implementation of Directive 2005/60/EC since 2009.
Asset Recovery Offices' (ARO) cooperation	Initiated by Member States.	To exchange information necessary for tracking and identifying the proceeds of crime.	Decentralised, AROs are required to exchange information via the Swedish initiative. Europol's SIENA application may soon underpin ARO cooperation.	Details of targeted property, such as bank accounts, real estate and vehicles, as well as details of persons sought, such as name, address, shareholder and company information.	Asset Recovery Offices.	CoE Convention 108, CoE Additional Protocol 181 and CoE Police Recommendation No R (87) 15.	Domestic data retention rules apply, as this instrument only regulates data exchange.	More than twenty Member States have set up AROs; twelve are participating in a pilot project that has deployed Europol's SIENA application to exchange data relevant for asset tracing.	The Commission is to submit its evaluation report to the Council in 2010.

Table form overview of instruments in operation, under implementation or consideration

Instrument	Background	Purpose(s)	Structure	Personal data coverage	Access to data	Data protection	Data retention	Implementation state	Review
National and EU Cybercrime Platforms	Initiated by France.	To collect, exchange and analyse information about offences committed on the internet.	Decentralised, bringing together national alert platforms and Europol's EU Cybercrime Platform. Europol's SIENA application may soon underpin data exchange between alert platforms.	Illicit content or behaviour detected on the internet.	National platforms receive citizens' reports; Europol's EU Cybercrime Platform receives law enforcement authorities' reports on serious cross-border cybercrime.	Specific rules established by the Europol Decision and Council Framework Decision 2008/977/JHA, CoE Convention 108, CoE Additional Protocol 181, CoE Police Recommendation R (87) 15 and Regulation (EC) 45/2001.	Domestic data retention rules apply, as this measure only regulates information exchange.	Almost all Member States have established national alert platforms; Europol is working on its EU Cybercrime Platform.	Europol covers cybercrime and, in future, will report on the activities of the EU Cybercrime Platform in its Annual Report submitted to the Council for endorsement and to the European Parliament for information.
Europol	Initiated by Member States.	To support Member States in preventing and combating organised crime, terrorism and other forms of serious crime affecting two or more Member States.	Europol is an EU agency based in The Hague. It is developing SIENA, its own secure information exchange network application.	The Europol Information System (EIS) contains the personal data, including biometric identifiers, convictions, and organised crime links, of persons suspected of crime falling under Europol's mandate. Analysis Work Files (AWF) contain any personal data of relevance.	EIS can be accessed by Europol National Units, liaison officers, Europol staff and the director. AWF access is granted to liaison officers. Personal data may be exchanged with third countries that have agreements with Europol.	Specific rules established by the Europol Decision and Council Framework Decision 2008/977/JHA, CoE Convention 108, CoE Additional Protocol 181, CoE Police Recommendation R (87) 15 and Regulation (EC) 45/2001.	AWF files may be retained for a maximum of three years, with another three-year extension possible.	Europol is actively used by each Member State and third countries with which it has an operational agreement. Europol's new legal basis has been implemented by each Member State.	A Joint Supervisory Body monitors Europol's processing of personal data and the transmission of such data to other parties. It submits periodical reports to the EP and the Council. Europol also submits an annual report on its activities to the Council for endorsement and to the EP for information.

Table form overview of instruments in operation, under implementation or consideration

Instrument	Background	Purpose(s)	Structure	Personal data coverage	Access to data	Data protection	Data retention	Implementation state	Review
Eurojust	Initiated by Member States.	To improve the coordination of investigations and prosecutions in Member States and enhance cooperation between relevant authorities.	Eurojust is an EU body based in The Hague, which uses s-TESTA for data exchange.	Personal data of suspects and offenders in cases of serious crime affecting two or more Member States, including biographical data, contact details, DNA profiles, fingerprints, photographs and telecommunication traffic and location data.	Europol's 27 national members, who may share data with national authorities and third countries if the source of the information agrees.	Specific rules established by the Eurojust Decision and Council Framework Decision 2008/977/JHA, CoE Convention 108, CoE Additional Protocol 181 and CoE Police Recommendation No R (87) 15.	Information must be deleted once the purpose for which it was supplied is accomplished, and once a case is closed.	Eurojust's amended legal basis is currently being implemented by Member States.	By June 2014, the Commission is to review data exchange between Eurojust's national members. By June 2013, Eurojust is to report to the Council and the Commission on the provision of national access to its case management system. A Joint Supervisory Body monitors Eurojust's processing of personal data and reports annually to the Council. The President of the Eurojust College submits to the Council an annual report on Eurojust's activities, which the Council forwards to the EP.

Table form overview of instruments in operation, under implementation or consideration

Instrument	Background	Purpose(s)	Structure	Personal data coverage	Access to data	Data protection	Data retention	Implementation state	Review
PNR agreements with the US and Australia; API/PNR agreement with Canada	Initiated by the Commission.	To prevent and combat terrorism and other forms of serious transnational crime.	International agreements.	The US and Australian agreements contain 19 PNR data categories, including biographical, reservation, payment and supplementary information; the Canadian agreement contains 25 similar data items.	The US Department of Homeland Security, the Canada Border Services Agency and the Australian Customs Services, which may share data with domestic law enforcement and counter-terrorism services.	The data protection rules are set out in the specific international agreements.	US: seven years active, eight years passive use; Australia: 3.5 years active, two years passive use; Canada: 72 hours active, 3.5 years passive use.	The US and Australian agreements are provisionally applicable; the Canadian one is in force. The Commission will renegotiate these agreements. Six EU Member States have enacted laws enabling the use of PNR data for law enforcement purposes.	Each agreement provides for a periodical review, while the Canadian and Australian agreements also include termination clauses.
EU-US TFTP Agreement	Initiated by the Commission.	To prevent, investigate, detect or prosecute terrorism or terrorist financing.	International agreement.	Financial messaging data containing, *inter alia*, the name, account number, address and ID number of the originator and recipients of financial transactions.	The US Treasury may share personal data extracted from financial messages with US law enforcement, public security or counter-terrorism authorities, Member States, Europol or Eurojust. Onward transfer to third countries is subject to Member States' consent.	The agreement has strict purpose limitation and proportionality clauses.	Personal data extracted from financial messages may be kept for no longer than necessary for individual investigations or prosecutions; non-extracted data may only be kept for 5 years.	The EP gave its consent to the conclusion of the EU-US TFTP Agreement on 8 July 2010. The Council is now expected to adopt a Council Decision concluding this agreement, following which the agreement would enter into force via an exchange of letters between the parties.	The Commission must review this agreements six months after its entry into force. Its evaluation report must be sent to the EP and the Council.