**MEMO/10/349**

Brussels, 20 July 2010

# EU information management instruments

The Commission presents today a clear, comprehensive and transparent summary of instruments regulating the collection, storage or cross-border exchange of personal data for the purpose of law enforcement or migration management, setting out at the same time the core principles that should underpin the evaluation of information management instruments in the area of freedom, security and justice. These same principles will be followed in the future development of instruments for data collection, storage or exchange:

- ***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.

- ***Necessity***: In all future policy proposals, the Commission will assess the initiative's expected impact on individuals' right and set out why such an impact is necessary and why the proposed solution is proportionate. 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.

- ***Clear allocation of responsibilities***: 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.

Principles for evaluation and development include also: *subsidiarity*; *accurate risk management*; *cost-effectiveness*; *bottom-up policy design*;

The Communication provides an overview of the European Union's instruments. In particular, the following aspects of each instrument are identified:

- Purpose(s) for which data are collected, stored or exchanged;
- Personal data coverage;
- Authorities with access to the data;
- Data protection provisions;
- Review mechanism.

## Schengen Information System (SIS)

*Purpose*: To maintain public security, including national security, within the Schengen area and facilitate the movement of persons using information communicated via this system.

*Personal data covered*: 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.

*Access to data*: Police, border police, customs and 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.

*Data protection rules*: Council of Europe (CoE) Convention 108 and CoE Police Recommendation R (87) 15.

*Review mechanism*: Signatories may propose amendments to the Schengen Convention. The amended text would have to be adopted by unanimity and ratified by parliaments.

*How useful is it*? In 2009 only, more than 31,5 millions alerts were entered in the central SIS database (almost 28 millions were entered in 2008 and about 23 millions in 2007):

| 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 |

## Schengen Information System II (SIS II)

*Purpose*: 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.

*Personal data covered*: 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.

*Access to data*: 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.

*Data protection rules*: 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.

*Review mechanism*: 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.

*How useful is it*? 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.

## EURODAC

*Purpose*: To assist in determining which Member State should assess an asylum application

*Personal data covered*: 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.

*Access to data*: 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.

Data protection rules: Directive 95/46/EC

*Review mechanism*: The Commission must send an annual report to the EP and the Council on the operation of the EURODAC central unit

*How useful is it*? The EURODAC Regulation is in force in EU Member States, Norway, Iceland and Switzerland. In 2008, EURODAC processed 219.557 sets of fingerprints of asylum seekers, 61.945 sets of fingerprints of people crossing the borders irregularly and 75.919 sets of fingerprints of people apprehended while illegally staying on the territory of a Member State. 17,5% of the asylum applications in 2008 were subsequent (i.e. second or more) asylum applications.

## Visa Information System (VIS)

*Purpose*: To help implement a common visa policy and prevent threats to internal security.

*Personal data covered*: Visa applications, fingerprints, photographs, related visa decisions and links between related applications.

*Access to data*: 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.

*Data protection rules*: 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.

*Review mechanism*: 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.

*How useful is it*? VIS is under implementation and will be applicable in each Member State (except the UK and Ireland) plus Norway, Iceland and Switzerland

## Advance Passenger Information System (API)

*Purpose*: 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. 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

*Personal data covered*: Personal data from passports, the point of embarkation and the EU entry point

*Access to data*: Border control authorities and, upon request, law enforcement authorities

Data protection rules: Directive 95/46/EC

*Review mechanism*: The Commission will evaluate the API system in 2011.

*How useful is it*? API is in force in each Member State, but only a few of them use it.

## Naples II Convention

*Purpose*: The Naples II Convention on mutual assistance and cooperation between customs administrations aims 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. 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.

*Personal data covered*: All information relating to an identified or identifiable person

*Access to data*: 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

*Data protection rules*: 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.

*Review mechanism*: 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.

*How useful is it*? This Convention has been ratified by each Member State

### Customs Information System (CIS)

*Purpose*: To assist competent authorities to prevent, investigate and prosecute serious violations of national customs laws. 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.

*Personal data covered*: 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

*Access to data*: National customs authorities, Europol and Eurojust may access CIS data.

*Data protection rules*: 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.

*Review mechanism*: The Commission, in cooperation with Member States, reports each year to the EP and the Council on the operation of CIS

*How useful is it*? The Customs Information System is in force in all Member States; in 2009, more than 2.000 new cases were created and almost 12.000 queries were entered.

### "Swedish initiative"

*Purpose*: 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. 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.

*Personal data covered*: Any existing information or criminal intelligence available to law enforcement authorities.

*Access to data*: Police, customs and any other authority with the power to investigate crime (with exception of intelligence services).

*Data protection rules*: National data protection rules, as well as CoE Convention 108, CoE Additional Protocol 181 and CoE Police Recommendation No R (87) 15.

*Review mechanism*: The Commission is to submit its evaluation report to the Council in 2010.

*How useful is it*? 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.

Examples of the use of the Swedish initiative to investigate criminal offences:

*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.

## Prüm Decision

*Purpose*: 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.

*Personal data covered*: Anonymous DNA profiles and fingerprints, vehicle registration data and information about individuals suspected of links to terrorism

*Access to data*: Contact points transmit requests; domestic access is governed by national law.

*Data protection rules*: 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.

*Review mechanism*: The Commission is to submit its evaluation report to the Council in 2012.

*How useful is it*? 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.

## Data Retention Directive

*Purpose*: To enhance the investigation, detection and prosecution of serious crime by retaining telecommunication traffic and location data.

*Personal data covered*: Telephone number, IP address and mobile equipment identifier.

*Access to data*: Authorities with access rights are nationally defined

*Data protection rules*: Directive 95/46/EC and Directive 2002/58/EC

*Review mechanism*: The Commission is to submit its evaluation report to the EP and the Council in 2010.

*How useful is it*? Six Member States have not yet transposed this directive. Examples of Member States detecting cases of serious crime via data retention:

*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.

## European Criminal Records Information System (ECRIS)

*Purpose*: To improve cross-border data sharing concerning EU citizens' criminal records

*Personal data covered*: Biographical data; conviction, sentence and offence; additional data, including fingerprints (if available).

*Access to data*: Judicial and competent administrative authorities.

*Data protection rules*: 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.

*Review mechanism*: 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 Framework Decision 2009/316/JHA (ECRIS).

*How useful is it*? ECRIS is under implementation. Nine Member States have started exchanging information electronically

## Financial Intelligence Unit cooperation (FIU.net)

*Purpose*: 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 of combating money laundering and, later, terrorist financing. FIUs are typically established within law enforcement agencies, judicial authorities or administrative bodies reporting to financial authorities.

*Personal data covered*: Any data of relevance to the analysis or investigation of money laundering and terrorist financing.

*Access to data*: Financial Intelligence Units (within police forces, judicial authorities or administrative authorities reporting to financial authorities).

*Data protection rules*: Council Framework Decision 2008/977/JHA, CoE Convention 108 and CoE Police Recommendation R (87) 15.

*Review mechanism*: As part of its Financial Services Action Plan, the Commission has been reviewing the implementation of Directive 2005/60/EC since 2009.

*How useful is it*? Twenty Member States participate in FIU.net, an online data-sharing application. Over the period 2007-2009, National Financial Intelligence Units have put forward more than 9.000 information requests via FIU.net. In the same span of time, the number of Member States actively using the system has grown from 12 to 18.

### Asset Recovery Offices' (ARO) cooperation

*Purpose*: 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. Similar to FIUs, AROs cooperate on a decentralised basis, albeit without the aid of an online platform.

*Personal data covered*: 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.

*Access to data*: Asset Recovery Offices.

*Data protection rules*: CoE Convention 108, CoE Additional Protocol 181 and CoE Police Recommendation No R (87) 15

*Review mechanism*: The Commission is to submit its evaluation report to the Council in 2010

*How useful is it*? More than twenty Member States have set up Asset Recovery Offices.

Over the period 2006-2007, Eurojust handled 61 asset confiscation cases, mostly related to drug trafficking (15), money laundering (9), fraud (8) and tax fraud (8), participation in a criminal organisation (5). Most cases were initiated by Germany (27%), the Netherlands (21%), the UK (15%) and Finland (13%).

In 2004, Members States submitted 5 asset tracing requests that were handled by Europol. This number grew to 57 in 2005. In 2007 Europol handled 133 requests, related –for instance– to fraud (29), money laundering (26), drugs (25).

### National and EU Cybercrime Platforms

*Purpose*: 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. 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.

*Personal data covered*: Illicit content or behaviour detected on the internet.

*Access to data*: National platforms receive citizens' reports; Europol's EU Cybercrime Platform receives law enforcement authorities' reports on serious cross-border cybercrime

*Data protection rules*: 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.

*Review mechanism*: 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.

*How useful is it*? Almost all Member States have established national alert platforms; Europol is working on its EU Cybercrime Platform.

Examples of the French Cybercrime Alert Platform, Pharos, investigating cases of cybercrime:

*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.

## Europol

*Purpose*: To support Member States in preventing and combating organised crime, terrorism and other forms of serious crime affecting two or more Member States.

*Personal data covered*: 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.

*Access to data*: 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

*Data protection rules*: 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.

*Review mechanism*: 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.

*How useful is it*? Europol is actively used by each Member State and third countries with which it has an operational agreement.

Examples of Europol's contribution to the fight against cross-border serious crime:

*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.

ParticipantsItaly, 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.

## Eurojust

*Purpose*: To improve the coordination of investigations and prosecutions in Member States and enhance cooperation between relevant authorities.

*Personal data covered*: 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.

*Access to data*: Europol's 27 national members, who may share data with national authorities and third countries if the source of the information agrees

*Data protection rules*: 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.

*Review mechanism*: 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.

*How useful is it*? Eurojust's amended legal basis is currently being implemented by Member States.

Examples of Eurojust coordinating large cross-border judicial operations against serious crime:

*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.

## Passenger Name Records agreements with the US, Canada and Australia

*Purpose*: To prevent and combat terrorism and other forms of serious transnational crime.

*Personal data covered*: 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.

*Access to data*: 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

*Data protection rules*: The data protection rules are set out in the specific international agreements.

*Review mechanism*: Each agreement provides for a periodical review, while the Canadian and Australian agreements also include termination clauses.

*How useful is it*? 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.

Examples of PNR analysis yielding information for investigating serious cross-border crime:

*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.

## Terrorist Finance Tracking Program (TFTP) agreement with the US

*Purpose*: To prevent, investigate, detect or prosecute terrorism or terrorist financing.

*Personal data covered*: Financial messaging data containing, inter alia, the name, account number, address and ID number of the originator and recipients of financial transactions.

*Access to data*: 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.

*Data protection rules*: The agreement has strict purpose limitation and proportionality clauses.

*Review mechanism*: The Commission must review this agreement six months after its entry into force. Its evaluation report must be sent to the EP and the Council.

*How useful is it*? Examples of the TFTP yielding information for investigating terrorist plots:

*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.

**For more information**

Homepage of Cecilia Malmström, Commissioner for Home Affairs:

http://ec.europa.eu/commission_2010-2014/malmstrom/welcome/default_en.htm

IP/10/986