eucrim
2010 / 1
THE EUROPEAN CRIMINAL LAW ASSOCIATIONS' FORUM

Focus: Data Protection
Dossier particulier: Protection de données
Schwerpunktthema: Datenschutz

2010/1 ISSUE / ÉDITION / AUSGABE

Contents

News*

Articles

* News contain internet links referring to more detailed information. These links can be easily accessed either by clicking on the respective ID-number of the desired link in the online-journal or – for print version readers – by accessing our webpage www.mpicc.de/eucrim/search.php and then entering the ID-number of the link in the search form.

Editorial

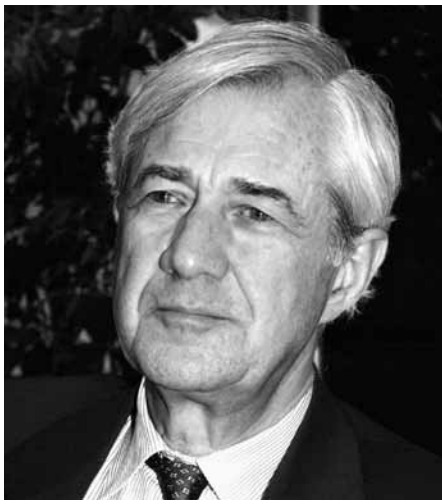
Dear Readers,

The decision by the eucrim editors to dedicate this entire issue to data protection confirms that data protection is increasingly relevant and also at the heart of European criminal law. An area of freedom, security and justice without internal borders can only exist if the national police and judicial authorities are able to exchange information as needed to fulfil their tasks. The use and exchange of information relating to persons also requires a solid and consistent system of data protection, not least because of technological developments. The term "surveillance society" is often used as a metaphor for a society that does not respect the fundamental interests of citizens to keep information safe and, if possible, to themselves.

It is an honour and a pleasure to write the editorial for this issue, which not only reinforces the importance of data protection but is also particularly well timed. On the level of the Member States, serious efforts are being made on the part of the Member States to implement Council Framework Decision 2008/977/JHA on data protection in the area of police and judicial cooperation into their national laws by 27 November 2010. At the same time, the implementation period for the most important parts of the Prüm system is still until August 2011.

Within the European Union, the playing field is changing considerably. The most important developments are that the Lisbon Treaty entered into force, that the Stockholm Programme was adopted, and that the European Commission organised public consultations on two highly relevant issues − the future framework for data protection within the European Union and the possibility of an agreement with the United States on data protection principles to be applied to transatlantic exchanges.

In March 2010, the highest national court in one of the largest Member States − Germany's *Bundesverfassungsgericht* − ruled on the compatibility of Directive 2006/24/EC on the retention of telecommunications data with essential values of privacy and data protection, and it decided that some of the national provisions violate fundamental rights. A week later, the European Court of Justice emphasised the need for strong data protection in a judgment on the independence of data protection authorities in the German *Länder*. In the political domain, the European Parliament recently took an important step, based on the non-respect of fundamental rights, by rejecting an agreement between the European Union and the United States that allowed US authorities to have access to personal data from SWIFT, under certain conditions, for purposes of counter-terrorism.



Peter Hustinx

These are all clear illustrations of the impact of data exchange and data protection. In my view, the most significant of these developments is the entry into force of the Lisbon Treaty. This Treaty marks a new era for data protection. It brings a number of general changes, such as the abolishment of the pillar structure − the cause of many deficiencies in the current data protection system −, giving a binding nature to the Charter of Fundamental Rights of the Union and the possibility for the EU to accede to the ECHR.

The Lisbon Treaty also resulted in Article 16 of the Treaty on the Functioning of the EU (TFEU). This article not only lays down the individual right of the data subject to the protection of his or her personal data, but it also obliges the European Parliament and the Council to provide for data protection in all areas of EU law, including the processing of personal data in the area of police and judicial cooperation and by institutions and bodies of the EU itself.

On the basis of Article 16, a comprehensive legal framework for data protection, combining consistency and solidity, will no longer be wishful thinking but a feasible policy objective.

I see it as one of my main tasks as EDPS to raise awareness of data protection, not only for individuals whose data are used but also amongst academics and policy makers. I am convinced that this issue of eucrim will be helpful in fulfilling this task.

Peter Hustinx
European Data Protection Supervisor

European Union*

Reported by Dr. Els De Busser (EDB), Sabrina Staats (ST), Cornelia Riehle (CR) and Nevena Kostova (NK)

Foundations

The Stockholm Programme

Action Plan Implementing the Stockholm Programme

On 20 April 2010, the European Commission proposed the action plan to implement the Stockholm Programme (COM(2010) 171 final). The 170 political objectives in the Programme (see also eucrim 4/2009, pp. 122-123 and eucrim 3/2009, pp. 62-63) that were agreed upon by the European leaders have now been translated into concrete measures and timetables by the Commission.

These measures are aimed at creating a genuine area of freedom, security and justice in the next five years. The entry into force of the Lisbon Treaty offered the EU institutions the necessary tools to develop balanced policies in order to strengthen the rights and freedoms of European citizens.

In the area of justice, fundamental rights and citizenship, the action plan includes inter alia the following actions:

- Improving data protection in all EU policies and in relations with third states. This includes a modernisation of Directive 95/46/EC;
- Strengthening the rights of the accused in criminal proceedings;
- Further developing the mutual recognition of judicial decisions and civil documents.

In the area of home affairs, the action plan includes inter alia the following actions:

- Defining a comprehensive security strategy to strengthen cooperation in law enforcement and civil protection as well as disaster and border management;
- Negotiating an agreement with the United States on the transfer of financial messaging data for the purpose of fighting terrorism (see also eucrim 4/2009, pp. 135-136);
- Developing an EU approach for the use of passenger name record data (PNR) for law enforcement purposes (see also eucrim 4/2009, p. 131; eucrim 1-2/2008, pp. 29-31 and eucrim, 3-4/2007, p. 101) and creating a framework for exchanging these data with third states;
- Strengthening the protection of citizens in the fight against cybercrime;
- Evaluating and, if necessary, amending the Data Retention Directive (see also eucrim 4/2009, pp. 136-137; eucrim 1-2/2009, pp. 2-3 and eucrim 1-2/2008, p. 2);
- Introducing a common EU asylum system.

The communication from the Commission presenting the action plan has been submitted to the European Parliament and the Council for approval. The Treaty of Lisbon has made it obligatory for the Commission to consult the Committee of the Regions and the European Economic and Social Committee. For this reason, the communication has also been addressed to both Committees. (EDB)

➤eucrim ID=1001001

Reform of the European Union

Accession of the EU to the European Convention on Human Rights

In the Lisbon Treaty, the EU has made the commitment to become a party to the European Convention on Human Rights (ECHR). Due to the fact that the EU is a legal entity in its own right, it can join the ECHR and protect citizens' rights under EU law. The process of accession started with the Commission adopting the Recommendation for a Council Decision authorising the Commission to negotiate the Accession Agreement of the EU to the ECHR. On 27 April 2010, the Recommendation was transmitted to the Council.

The accession ensures that the ECHR will be the minimum standard of protec-

* If not stated otherwise, the news reported in the following sections cover the period February 2010–April 2010.

tion of human rights, and it will give EU citizens an additional judicial mechanism to enforce their rights.

It must be noted that the accession of the EU to the ECHR creates several legal, technical, and institutional issues. On 8 March 2010, these issues were collected in a draft opinion of the Committee on Civil Liberties, Justice and Home Affairs. In its opinion, this Committee called upon the Committee on Constitutional Affairs, as the committee responsible, to incorporate the listed suggestions in its motion for a resolution.

First of all, the Committee on Civil Liberties, Justice and Home Affairs pointed out that the EU should not only accede to the ECHR but also to all its protocols.

Secondly, the EU's legal instruments (decisions, regulations, directives, etc.) would then be subject to the scrutiny of the European Court of Human Rights (ECtHR). The Committee on Civil Liberties, Justice and Home Affairs expressed the opinion that this should lead to an improved system of implementation of the subsidiarity principle rather than a case overload for the ECtHR.

Thirdly, the Court of Justice' cooperation with the ECtHR could be problematic as the latter would also be able to rule upon compliance with human rights by the Court of Justice.

Fourthly, the EU's representation in the CoE bodies should be clarified. For example, every State Party to the CoE has a member in the Parliamentary Assembly, which appoints the judges of the ECtHR. As the EU does not have a seat in the Assembly, the way in which the EU selects its judge needs to be decided. The Committee on Civil Liberties, Justice and Home Affairs calls for the EP to be represented in the procedure of electing a judge to the ECtHR.

In accordance with Article 218(2), (3) and (8) of the Treaty on the Functioning of the European Union (TFEU), accession to the ECHR requires a recommendation from the Commission for a negotiation mandate; a unanimous Council decision to open accession negotiations with the CoE; a unanimous agreement by the Council on the outcome of these negotiations; the consent of the European Parliament to the Accession Agreement, and ratification of the Accession Agreement in all 27 EU Member States and in the remaining 20 countries that are signatories to the Convention (including Russia and Turkey). The accession process will thus potentially take several years. (EDB)

➤eucrim ID=1001002

Schengen

No SIS II Before the End of 2011

The development of the second generation of the Schengen Information System (SIS II), and the concerns that it has caused, have regularly been reported on (see eucrim 3/2009, p. 64; eucrim 1-2/2009, pp. 3-4; eucrim 1-2/2008, p. 8 and eucrim 3-4/2007, pp. 70-73). Technical difficulties caused supplementary costs. Although the transition from SIS I+ to SIS II was planned to lead to a new operational system in 2007, the European Parliament voted on 18 May 2010 to move the deadline to the end of 2011 as was proposed by the Commission and the Member States.

The legal instruments governing this migration (Regulation (EC) 1140/2008 and Decision 2008/839/JHA) foresaw the possibility for the Commission to, if necessary, extend the previous deadline (September 2009) until the expiry of these instruments on 30 June 2010. Tests of the new system that were undertaken in January 2010 were not very successful, and the evaluation of the test results is still ongoing. Possibly, the test will have to be repeated.

The latest forecasts say that the transition could be completed by the end of 2011. Therefore, the Commission proposed amending the migration instruments again before they expire. On 18 May 2010, the European Parliament agreed to do so. The Parliament's rapporteur on the matter called for stronger Parliamentary scrutiny of the migration to the new system in order to prevent additional delays and costs. (EDB)

➤eucrim ID=1001064

Institutions

Council

Measures for Protecting the External Borders and Combating Illegal Immigration

At the JHA-meeting from 25-26 February 2010, the Council adopted conclusions on 29 measures for reinforcing the protection of the external borders and combating illegal immigration. The measures aim at strengthening the EU's external borders in order to monitor migrants and track down criminals. Though these measures were already proposed in 2008 and have been worked on since, the timing could not be better because the Commission has just adopted a proposal to strengthen Frontex. The agreed conclusions include *inter alia*:

- Amendments to the Frontex Regulation;
- Enhancement of operational cooperation with third countries with regard to improving patrolling on land and at sea, maritime surveillance, and returning illegally staying third-country nationals to their countries of origin;
- Improving the collection, processing, and exchange of relevant information between the respective countries, Frontex, and other EU agencies;
- Plans for Frontex to carry out a pilot project in 2010 for the creation of an operational office in Piraeus or to establish other operational offices as appropriate;
- The request for the Member States to implement the phases and steps laid down for the development of EUROSUR – the European Surveillance Sys-

tem – as soon as possible and report on the EUROSUR progress by mid-2010;

■ Establishment of national border surveillance systems in every Member State as well as a network of national coordination centers, which should be compatible with the Frontex information system and fully operational on a pilot basis as of 2011.

The Commission is to report on the implementation of the adopted conclusions by the end of 2010. (ST)

➤eucrim ID=1001003

European Court of Justice (ECJ)

Article 255 TFEU Panel Appointed

On 25 February 2010, the Council adopted a Decision appointing Jean-Marc Sauvé, Peter Jann, Lord Mance, Torben Melchior, Péter Paczolay, Ana Palacio Vallelersundi, and Virpi Tiili as members of the panel provided for in Article 255 of the Treaty on the Functioning of the European Union (TFEU). The members were appointed for a period of four years from 1 March 2010, and the panel is comprised of persons chosen from among former members of the Court of Justice and the General Court, members of national supreme courts, and lawyers of recognised competence. The panel's main task is to prepare an opinion on the suitability of potential candidates to perform the duties of Judge and Advocate-General of the Court of Justice and the General Court before the Member States' governments make the appointments referred to in Articles 253 and 254 (TFEU). (ST)

➤eucrim ID=1001004

OLAF

Delegates of EP Question Appointment of OLAF Interim-Director

On 2 March 2010, coordinators from four political groups (EPP, S&D, Verts/ALE and GUE/NGL) of the European Parliament published a joint statement on the appointment of Nicholas Ilett as "acting director" of OLAF. The statement declares his appointment as an infringement of Parliament's rights, since the chosen person should have received prior approval of Parliament and the Member States. Also, they consider the appointment to be a "breach of the OLAF Regulation 1073/99" and "illegal". By not following the official nomination procedure, they believe that the Commission is putting at risk all cases currently handled by OLAF because they could be disputed before the Court of Justice. The statement adds that OLAF's Supervisory Committee as well as Parliament's legal service would "support this opinion".

Article 12 of 1073/99 foresees a consultation of the EP and the Council prior to appointing a new director which did not take place whereas rules on appointing an "acting Director" are not provided for. (ST)

➤eucrim ID=1001005

New OLAF Director-General Sought

The Commission is currently seeking to recruit the new Director-General of OLAF. The Director-General of OLAF is in charge of running the investigative activities of the Office, which are carried out in full independence of any EU institution or other body. The Director-General will be responsible for a Directorate-General comprising four Directorates, a staff of 500, and a budget of approx. EUR 50 million. The mandate is for 5 years, renewable once, and appointment follows the rules laid down by 1073/99/EC. (ST)

➤eucrim ID=1001006

New System for Reporting Corruption and Fraud Anonymously

OLAF has set up a new electronic system to report corruption and fraud: the "Fraud Notification System" (FNS). The new system is to make it easier for citizens and EU civil servants to report suspicious activities, by allowing informants to remain anonymous, while providing the possibility for OLAF investigators to contact the informants for further enquiries. The system operates like a "blind" letterbox where both parties can drop off messages. (ST)

➤eucrim ID=1001007

Commission Takes on Portuguese VAT Flat Rate Scheme

On 18 March 2010, the Commission announced the referral of a case to the ECJ concerning the VAT flat rate schemes in Portugal. According to the VAT Directive, Member States may apply a flat rate scheme designed to offset the VAT charged on purchases of goods and services made by flat rate farmers. Flat rate farmers are not covered by normal VAT rules, they may not deduct the VAT paid on their inputs, and they are released from their obligations relating to the payment of tax, invoicing, declaration, and accounting. A flat rate compensation is being paid in order to compensate for the VAT paid on inputs, which the farmers cannot deduct.

Portugal, however, has not introduced a flat rate scheme in accordance with the VAT Directive for farmers and has instead set up an optional exemption for agricultural activities. This means exempting VAT on supplies provided by farmers, unless they opt to apply the normal VAT rules. Also, there is no compensation for the VAT paid on the farmers' inputs whereas they have to pay VAT on agricultural inputs. The Commission believes that exemptions for agricultural activities are covered by the VAT Directive and that the Directive only foresees the flat rate scheme for this area. Therefore, the Commission considers Portugal's approach not to be in line with the VAT Directive and has therefore referred the case to the ECJ. (ST)

➤eucrim ID=1001008

Commission Tackles Hungarian VAT Credit Reimbursement Rules

As announced on 18 March 2010, the Commission is bringing Hungary before

the ECJ for not changing its legislation with respect to VAT credit reimbursement. Hungary grants taxable persons the option of choosing between carrying forward their excess VAT (which results from deductible VAT exceeding payable VAT in one tax period) to the next tax period or immediately claiming a refund for it. However, the reimbursement of excess VAT cannot be claimed on the basis of input VAT charged on a purchase that has not yet been paid for by the taxable person. As a result, taxable persons whose tax returns consistently show "excesses" are de facto obliged to carry forward the excess input VAT into the following tax period which, in the Commission's view, infringes Article 183 of the VAT Directive by not providing for an adequate refund opportunity. (ST)
➤eucrim ID=1001009

Refund of Unduly Paid VAT and Other Taxes – Commission Brings Greece before ECJ

Also on 18 March 2010, the Commission decided to refer three cases to the ECJ concerning the failure of Greece to completely implement previous ECJ judgements on the refund of unduly paid taxes. In these cases, the ECJ decided that Greek law does not adequately provide for the repayment of taxes that were levied by Member States in violation of EU law. (ST)
➤eucrim ID=1001010

Cooperation in VAT Matters – Action against Germany

The Commission has requested the ECJ to declare that Germany has failed to fulfil its obligations arising from Article 248 EC, Regulation 1605/2002 and Article 10 EC by refusing to permit the Court of Auditors to carry out audits in Germany concerning administrative cooperation in the field of VAT. Germany has refused to allow audits that are designed to assess how EU financial resources were collected and used. In the Commission's view, Germany has hereby infringed not only its obligation to cooperate in good faith (Article 10 EC), but also its obligation to take all appropriate legislative and administrative measures to ensure the collection of all VAT due on its territory. (ST)
➤eucrim ID=1001011

EDPS on Cooperation in Combating Fraud in the Field of VAT

Though he had not been consulted on the matter, the EDPS published an opinion in the Official Journal of 17 March 2010 on the proposal for a Council Regulation on administrative cooperation and combating fraud in the field of value-added tax (COM(2009)0427). The proposal aims at improving the effectiveness of tax authorities by making the competent authorities jointly responsible for VAT revenues in all Member States. In his opinion, the EDPS states that he is aware of the importance of collecting and processing personal data in order to enhance the effectiveness of measures against transnational fraud and to achieve better collection of VAT in the EU.

Nevertheless, in the EDPS' view, the proposed Regulation does not completely meet European data protection rules. The EDPS therefore recommends clarifying the respective responsibilities of the Member States, the Commission, and Eurofisc (a common operational structure allowing for fast information exchange in the fight against cross-border VAT fraud) regarding compliance with these European data protection standards, specifying the type and extent of personal data to be exchanged as well as limiting the purposes for which the information is exchanged. (ST)
➤eucrim ID=1001012

Strengthening Mutual Assistance in the Recovery of Taxes

On 16 March 2010, the Council adopted a Directive aimed at strengthening mutual assistance between Member States for the recovery of claims relating to taxes, duties, and other measures (see eucrim 4/2009, p. 128). The new Directive is

Fight against Fraud and Corruption: Strengthening Cooperation between Turkish Authorities and EU Institutions

29–30 April 2010, Istanbul, Turkey

The seminar, financed by the European Commission under the Hercule II Programme (managed by OLAF), built on the Trier conference of February 2010 "Combating Corruption in the EU – Focus on the EU accession policy" and was attended by over 100 lawyers, including representatives of the European Associations for the protection of the financial interests of the European Community.
The morning sessions of the seminar were dedicated to an overview of the European legal framework for combating corruption and protecting the EC's financial interests (representatives of OLAF and Eurojust were invited to present these topics).
The remaining sessions of the first day were devoted to EU anti-corruption policies with regard to candidate (and potential candidate) countries and had a specific focus on the Turkish experiences.
Throughout the planning and execution of this event, emphasis was placed on concrete and practical discussions rather than on academic debates. The importance of improving administrative cooperation between anti-corruption investigators is high on everyone's agenda and this approach was well reflected both in the conference programme and in the composition of the audience, which was made up of prosecutors and other legal professionals.
The overall theme had been chosen because, in candidate countries, as well as in third countries, the fight against corruption has become much more crucial during recent years. Although considerable results have been achieved and many of these countries have adopted national anti-corruption strategies, corruption remains a paramount problem.
In terms of participants, the event was clearly a success, and it maintained a good balance between European participants and participants from Turkey.

For further information, please contact Mr. Laviero Buono, Head of Section for European Public and Criminal Law, ERA. E-mail: lbuono@era.int

EU Member States' Investigative Techniques in Fraud and Corruption Cases

6–7 May 2010, Athens, Greece

The seminar, financed by the European Commission under the Hercule II Programme (managed by OLAF), provided participants with an in-depth analysis of recent developments in EU anti-corruption policy, with a specific focus on Greece and other Mediterranean countries.

The main topics of discussion were:

- Major European and international anti-corruption instruments;
- EU Member States' standards and investigative techniques, with a view to facilitating the detection, investigation, prosecution, and adjudication of corruption cases;
- Defence issues in cases of fraud and corruption;
- Interagency co-operation, joint investigations, and cross-border co-operation among Mediterranean and non-Mediterranean EU Member States;
- Cooperation between OLAF and other EU Institutions and bodies as well as national authorities specialised in investigating financial irregularities.

For further information, please contact Mr. Laviero Buono, Head of Section for European Public and Criminal Law, ERA. E-mail: lbuono@era.int

designed to provide for an improved assistance system, particularly simplifying rules on obtaining and exchanging information held by banks and other financial institutions. The intention is to better safeguard the financial interests of the Member States and the neutrality of the internal market as well as to better cope with cross-border financial crime. (ST)

➤eucrim ID=1001013

Directive on Reverse Charge Mechanism in Greenhouse Gas Emission Allowance Trading

On 16 March 2010, the Council adopted a Directive amending Directive 2006/112/EC on the common system of VAT as regards an optional and temporary application of the reverse charge mechanism in relation to supplies of certain services susceptible to fraud. The Directive stems from a Commission proposal that covered not only CO2 and other greenhouse gas emission allowances, but also mobile phones and electronic circuit devices, which are also affected by carousel fraud (see eucrim 3/2009, p. 70, eucrim 1-2/2007, p. 22, and eucrim 1-2/2008, pp. 17-18). The Council intends to continue working on other elements of the proposal with a view to reaching an agreement soon. (ST)

➤eucrim ID=1001014

Europol

EU Terrorism Situation and 2010 Trend Report Published

In April 2010, Europol published the European Union's Terrorism Situation and Trend Report 2010 (TE-SAT 2010). The TE-SAT 2010 contains basic facts and figures regarding terrorist attacks, arrests, and activities in the EU. The annual report is based on information contributed by EU Member States, Eurojust, neighbouring countries of the EU, and third states formally cooperating with Europol (for this report, contributions from Colombia, Croatia, Iceland, Norway, Switzerland, Turkey, and USA were included).

TE-SAT 2010 provides for a general overview on the situation in the EU in 2009 and outlines future trends. It distinguishes between five categories of terrorism based on the source of motivation: Islamist terrorism; ethno-nationalist and separatist terrorism; left wing and right wing terrorism; and single-issue terrorism.

The report offers the following key findings:

- According to TE-SAT, EU Member States continue to be exposed to a serious threat from Islamist, ethno-nationalist and separatist as well as left-wing and anarchist terrorism. However, the overall number of terrorist attacks in all Member States in 2009, excluding the UK, decreased by 33% compared to 2008 and is almost half the number of attacks reported in 2007.
- For 2009, a total of 294 failed, foiled, or successfully perpetrated terrorist attacks were reported by six Member States, while an additional 124 attacks in Northern Ireland were reported by the UK.
- Arrests on suspicion of offences related to terrorism decreased by 22% in comparison to 2008 and by about 30% compared to 2007.
- Financing of terrorism and membership in a terrorist organisation remain the most common reasons for arrests with regard to Islamist terrorism. Substantial amounts of money are transferred, using a variety of means, from Europe to conflict areas in which terrorist groups are active.
- Active youth branches supporting terrorist or extremist organisations are of particular concern to some Member States as being potential targets for radicalisation and recruitment.
- Internet and communication tools developed for use over the Web (e.g., social networking sites, instant messaging programmes) are a major tool for terrorist and extremist organisations and used to promote their agendas, organise campaigns, collect information on future targets, claim attacks, inform other members of the group, and even recruit with greater ease.
- The number of women arrested for terrorism-related offences remains low. Women accounted for 15% of suspects arrested in 2009, compared to 10% in 2007. The majority of these arrests were related to separatist terrorism.
- In 2009, a total of 125 court decisions related to terrorism offences were rendered in 11 Member States. The majority was related to separatist terrorism – in contrast to 2008 when the majority related to Islamist terrorism. The percent-

age of acquittals decreased from 23% in 2008 to 17% in 2009. Once more, since 2008, there has been an increase in the number of individuals tried.

■ In spite of only one attack in 2009, Islamist terrorism is still perceived as the biggest threat to most EU Member States as Islamist terrorist groups are still aiming to cause mass casualties. The EU is used as a platform to prepare and initiate terrorist attacks elsewhere in the world. The trend involving a steady decrease in the number of arrests relating to Islamist terrorism continued in 2009 with a 41% decrease compared to 2008.

■ Separatist terrorism continues to be the type of terrorism that affects the EU most in terms of the number of attacks carried out, although the number of attacks and arrests continued to decrease in 2009. Europe is important as a source of financial and logistical support to the PKK, the LTTE and the FARC.

■ In 2009, the total number of left-wing and anarchist terrorist attacks in the EU increased by 43% compared to 2008 and has more than doubled since 2007.

■ Two single-issue terrorist attacks were reported in 2009. The illegal activities of single-issue extremism continue to be dominated by Animal Rights Extremism (ARE) activists. (CR)

➤eucrim ID=1001015

EMCDDA and EUROPOL Launch Review of Cocaine Market

In April 2010, Europol and the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) launched a market analysis titled Cocaine: a European Union perspective in the global context. The review is the second title in an EMCDDA-Europol joint publication series launched in 2009 and covering key aspects of European drug markets. The review looks at the production of coca and cocaine in the Andean-Amazonian region, the suppressing of coca in Colombia, the production of cocaine base and cocaine hydrochloride, the main trafficking routes, importation and distribution to Europe, and the initiatives taken to reduce supply at the EU level. The report is available in English and Spanish.

In this analysis, Europol and the EMCDDA come to the following conclusions:

■ Europe has become an important destination for cocaine manufactured in South America.

■ Europe ranks third in the world for the amount of cocaine confiscated (after South and North America).

■ Cocaine landing points seem to have shifted within the main gateway regions, the Iberian Peninsula, and the Low Countries (Belgium and the Netherlands).

■ Trafficking networks seem to be spreading eastwards. Thus, Eastern and Central European countries face an increased risk of cocaine diffusion.

■ Different routes are used to smuggle cocaine into Europe using a wide variety of concealment methods and means of transport. "Secondary extraction" has become a new concealment and smuggling method where cocaine is incorporated into other materials and then removed by "secondary extraction" laboratories set up in Europe.

■ The West African route has become more and more important, which shows the diversification of drug trafficking itineraries.

■ Cocaine trafficking has been addressed in Europe by several initiatives such as the EU-LAC cooperation, the MAOC-N, or Europol's Project Cola.

■ Colombia produces most of the cocaine available in the world. Alternative measures to prevent coca cultivation and for the local economy have been developed and supported by the EU and its Member States. Nevertheless, efforts to intercept cocaine products at their source, trafficking routes, and consumer markets should be enhanced.

■ The understanding of cocaine production in South America and trafficking towards and within Europe is still limited. Thus, additional or better-developed information systems are necessary.

■ The precision of cocaine production estimates could be improved.

■ Concrete information on the amount of cocaine consumption in European markets and on how this consumption compares with the cocaine output of South America is lacking. Thus, a methodology to assess the size of the European consumer market for cocaine should be developed.

■ More insight into the merging of cocaine routes, multi-drug consignments, incorporation of cocaine into other "carrier" materials, organised criminal groups, and trafficking networks as well as additional studies of the intra-European cocaine markets are needed.

■ In order to draw a clear picture of cocaine supply and trafficking in Europe, quantitative indicators and alternative monitoring strategies need to be further developed.

■ To gain a clearer picture of potential processing sites in South America and Europe, better and more systematic information on illicit sources and trafficking routes for chemicals used to manufacture cocaine are needed.

■ In order to design adequate responses to counter cocaine production, better information on precursors would be necessary. (CR)

➤eucrim ID=1001016

Eurojust

Aled Williams New President

The College of Eurojust elected Aled Williams, National Member for the United Kingdom, as new President of Eurojust.

Aled Williams first joined Eurojust in July 2006 as Deputy National Member for the United Kingdom. In 2008, he was appointed National Member for the UK. Before working at Eurojust, Mr. Williams worked as the United Kingdom liaison magistrate to Spain where he dealt with mutual legal assistance, extradition, and the introduction of Eu-

What Are the Future Prospects for a European Public Prosecutor? The Protection of the EU's Financial and Fundamental Interests

11–12 February 2010, Paris, France

The Treaty of Lisbon was signed on 13 December 2007 and entered into force on 1 December 2009. It revived the European framework as far as criminal law is concerned and paved the way for a forthcoming European Public Prosecutor in charge of protecting the EU's financial and fundamental interests.

An international seminar, which was conducted in Paris on 11 and 12 February 2010 by the French Court of Cassation – thanks to the support of the European Commission and the European Anti-Fraud Office (OLAF) through the Hercule II programme –, brought together key French and European practitioners in charge of the fight against cross-border crime. The participants included EU Prosecutors General and representatives of the European Commission, the European Anti-Fraud Office, the European Court of Human Rights, the European Court of Justice, and the European Parliament.

This conference, which was also open to magistrates and to members of the Associations of European lawyers, aimed at increasing the participants' awareness of the reality of cross-border crime by reflecting on the practical means that enable reinforcement of the legal mechanisms currently in place. In particular, attention should be paid to improved interaction between the current actors in European judicial cooperation and to creating a forum for meetings and exchanges with the principal European actors in the fight against cross-border crime.

Three subjects were dealt with: the reasons and rationale for the creation of a European Public Prosecutor, the reinforcement of the current legal instruments, and "format" for a future European Public Prosecutor.

The transcripts of this conference will be published by a French publisher specialised in legal matters during the second half of 2010.

For further information, please contact Mr. Peimane Ghaleh-Marzban, Secretary-General, Public Prosecutor, Cour de cassation, Paris, France. E-mail: Peimane.Ghaleh-Marzban@justice.fr

ropean Arrest Warrant procedures. Mr. Williams started his legal career in 1984 as a solicitor and later as a prosecutor.

The election followed the resignation of the former President and Portugal's National Member, Mr. José Luís Lopes da Mota last December (see also eucrim 4/2009, p. 126). (CR)

➤eucrim ID=1001017

New Liaison Prosecutor for Croatia

For the first time, a Liaison Prosecutor for Croatia has been placed at Eurojust following a cooperation agreement that Eurojust concluded with the Republic of Croatia in 2007.

The new Liaison Prosecutor, Mr. Josip Čule, came to Eurojust in December 2009. In the previous years, Mr. Čule was Head of the International Legal Assistance and Co-operation Unit in Croatia and President of the Croatian State Attorney Council. He had already been serving as a contact point for Eurojust in Croatia since 2005. (CR)

➤eucrim ID=1001018

New National Member for Portugal

In February 2010, Mr. João Manuel Da Silva Miguel joined Eurojust as new National Member for Portugal. Before joining Eurojust, Mr. João Manuel Da Silva Miguel worked as an Agent of the Portuguese Government at the European Court of Human Rights, at the Committee of Human Rights of the United Nations, and as Deputy Prosecutor General at the Consultative Council of the Prosecutor General's office. At present, Mr. Da Silva Miguel is also Vice-President of the Consultative Council of European Prosecutors (CCPE) at the Council of Europe. (CR)

➤eucrim ID=1001019

New Application Form for JIT Funding

As of 9 April 2010, a new form by which to apply for financial assistance via Eurojust for a Joint Investigation Team (JIT) is available. Completion of the new form is necessary in order for an application for financial assistance to be considered (for details regarding JIT funding by Eurojust, see eucrim 3/2009, p. 81). (CR)

➤eucrim ID=1001020

Memorandum of Understanding with UNODC

On 26 February 2010, Eurojust and the United Nations Office on Drugs and Crime (UNODC) signed a Memorandum of Understanding with the purpose of facilitating their mutual cooperation in reinforcing the fight against serious crime.

In the Memorandum, both parties agree to maintain regular contacts and to facilitate direct contacts between their designated authorities, namely Eurojust's National Members, Liaison Magistrates and contact points, and the central and other national authorities designated under the relevant UN Conventions listed in the Memorandum. Furthermore, both parties agree to designate a central point of contact as well as one for terrorism-related matters and one for corruption and economic crime-related matters.

At the heart of the Memorandum is the agreement to exchange non-operational and non-sensitive information. Exchangeable information includes, for instance, legal and practical information concerning the judicial and procedural systems of the Member States as well as strategic information. Upon request, Eurojust will examine whether it can facilitate other information to UNODC. Additionally, Eurojust National Members and Liaison Officers are granted access to the legal tools of the UNODC, including its databases on Treaty-related information.

Finally, the Memorandum foresees that Eurojust and UNODC invite each other to certain meetings (Eurojust strategic meetings, UNODC working group meetings), professional training seminars, and study visits in addition to offering each other technical assistance. (CR)

➤eucrim ID=1001021

European Judicial Network (EJN)

New Tool: the EJN Forum

In February 2010, together with the Spanish Presidency, the EJN launched a new tool on its website: the EJN Forum. The EJN Forum offers a discussion platform for EJN contact points as well as all interested legal practitioners. The Forum is restricted. Access is granted by the EJN Secretariat to all EJN contact points and can be granted upon request to all interested legal practitioners through the registration form provided on the EJN website.

The first topic of discussion offered in the EJN Forum debates the use and gathering of foreign evidence obtained through mutual legal assistance in criminal proceedings. (CR)

➤eucrim ID=1001022

Draft Guidelines on the Structure of the European Judicial Network

At the beginning of the year, the EJN published draft guidelines regarding its operation and use of the Eurojust budget related to the activities of the EJN Secretariat.

With a view to the EJN plenary meetings, the guidelines provide for detailed principles on their structure. Three meetings are foreseen per year: the first regular one shall take place in Brussels or The Hague, and the other two "Presidency" meetings shall take place towards the end of the actual Presidency period in the respective Member State. Whereas, for regular meetings, two contact points per Member State shall be invited, at least three contact points per Member State are recommended for the "Presidency" meetings. Regular meetings shall be devoted to practical and organisational matters and new initiatives; "Presidency meetings" shall deal with matters relating to the functioning of the EJN as well as topics left to the organising Member State.

The guidelines also include regulations with regard to the meetings of the national correspondents that take place twice a year in The Hague. The recommended tasks of these meetings include discussion and work on budgetary issues, internal and external EJN policy, IT strategy, feedback from the EJN contact points, implementation of the EJN Decision, and possible action plans.

Another point in the draft guidelines concerns the meetings and tasks of tool correspondents that shall, for instance, deal with the development of and training on EJN information tools.

The responsibilities of the EJN Secretariat shall cover, amongst other tasks, the proper administration of the EJN and its information system/website.

Finally, the draft guidelines include recommendations on budgetary matters such as a time frame for the preparation, adoption, and execution of the EJN budget, the organisation of current and forthcoming projects, relations with other bodies and structures, and the promotion of the EJN. (CR)

➤eucrim ID=1001023

EJN Manual Published

In November 2009, the first EJN Manual was adopted at its 33rd Plenary meeting. The new instrument serves two purposes: first, to identify the actions required in order to achieve the EJN's objectives as outlined in the EJN Council Decision, the Council Decisions to strengthen Eurojust and the EJN, and the EJN Guidelines; and second, to locate responsibility for the required actions.

For each of the following nine areas, the Manual outlines the underlying legal framework, identifies the required action, locates responsible actors, and identifies the required resources, expected results, and risks with regard to EJN contact points, national correspondents, tool correspondents, the EJN Secretariat, plenary meetings in the Member States, regular meetings, regional meetings, budgetary matters, and ad hoc groups.

To give some examples, the actions and activities suggested by the Manual for the EJN contact points include training on their role and function, and it recommends support from the EJN Secretariat and partnership with the EJN. According to the Manual, the tool correspondents shall, amongst other tasks, provide information to the EJN Website and check the accuracy of information on tools. The EJN Secretariat is asked to provide for training and assistance to the contact points. The risks anticipated in the Manual, which might limit the required actions of the EJN Secretariat, include a potential lack of human resources and budgetary reductions. Reflecting on "Presidency" meetings in the Member States, the Manual allocates the tasks and responsibilities for their organisation to the Member States and the EJN Secretariat. Finally, the EJN Secretariat, together with the support of the Budget and Finance Unit of Eurojust, is given the budgetary responsibility, for instance, to prepare the five-year Work Programme and Budget forecasts and monitor the overall budget and budget lines. (CR)

➤eucrim ID=1001024

Frontex

Proposal for a Frontex Regulation

On 24 February 2010, the Commission launched a proposal for a Regulation in order to strengthen the operational capabilities of Frontex. The proposed Regulation would adapt the existing Frontex Regulation of 2004 and takes the next logical step after a series of evaluations on the Agency that were conducted in the past several years (see eucrim 4/2009, p. 127).

The proposal shall enhance the operational capacities of Frontex. To achieve this aim *inter alia* the following measures shall be introduced:

- Frontex shall receive its own technical equipment as well as manage a "pool" of technical equipment provided on a compulsory basis by the Member States.

- Furthermore, to ensure effective operations, an appropriate number of border guards shall be made available by the Member States, and border guards should be seconded to Frontex on a semi-permanent basis.
- In the future, an operational plan shall support the coordination of joint operations between Frontex and the Member States.
- A reporting scheme shall make sure that breaches of the Regulation or the Schengen Border Code are transmitted to the relevant public authorities and the Management Board.
- Training on control and surveillance, removal of illegally present third country nationals, and in particular on fundamental rights, shall be provided to Frontex for the national services.
- Frontex shall provide assistance and coordinate the organisation of joint return operations of the Member States. It shall define a Code of Conduct to be followed during the removal of third-country nationals illegally present in the territory of any of the Member States.
- Cooperation with Europol, the European Asylum Support Office, the Fundamental Rights Agency, and other EU agencies and bodies as well as with third countries and relevant international organisations is endorsed if necessary to fulfil its mission. To advance cooperation with relevant third countries, Frontex shall conduct projects on technical assistance and deploy liaison officers. Furthermore, representatives of third countries shall be enabled to participate in Frontex activities.
- Data protection shall be guaranteed by the application of Directive 95/46/EC.
- Constituting a development of the Schengen Acquis, the new Regulation also addresses Iceland, Norway, Switzerland, Liechtenstein (opt-outs), and Denmark (opt-in) while the UK and Ireland are not taking part.

The proposal is currently under discussion in the European Parliament. (CR)

➤eucrim ID=1001025

Specific Areas of Crime / Substantive Criminal Law

Counterfeiting & Piracy

Anti-Counterfeiting Trade Agreement: State of Play

On 21 April 2010, the negotiating parties of the Anti-Counterfeiting Trade Agreement (ACTA), the EU, and a number of other WTO members published the documents of the 8th round of negotiations held in Wellington, New Zealand, from 12-16 April. The objective of the ACTA agreement, for which formal negotiations started in June 2008, is to have a new multilateral treaty to more effectively combat trade in counterfeit and pirated goods that improves global standards for the enforcement of intellectual property rights. After the previous seven negotiation rounds, the ACTA parties have now released a consolidated draft text as the outcome of these discussions with a view to reaching a final agreement soon. The text indicates that the new agreement will not include provisions that modify substantive intellectual property law, create new rights, or change their duration. It aims to set minimum rules on how inventors and entrepreneurs can enforce their rights in courts, at borders, or over the Internet. The purpose of the new agreement is to address large-scale infringements of intellectual property rights with a significant economic impact. In contrast to public speculations prior to the release of the text (see for example the EDPS's opinion of 22 February 2010), "three strikes" or "gradual response" rules to fight copyright infringements and internet piracy are not foreseen. (ST)

➤eucrim ID=1001026

Major Success for Joint Customs Operation "Matthew II"

On 13 April 2010, the results of the Joint Customs Operation "Matthew II," aimed at detecting the smuggling of cigarettes in commercial consignments entering the EU by road, has led *inter alia* to the seizure of more than 16 million cigarettes, 20 tons of counterfeit perfumes as well as 53,418 other counterfeit items and 1,515,75 kilograms of cannabis. From 24 November to 3 December 2009, controls focused on all means of transport entering the EU customs territory from third countries via the eastern EU border. The operation was organised by the Czech Republic in cooperation with Poland and OLAF. Due to the huge success of "Matthew II," the partners involved in the operation are thinking about conducting similar operations in the near future. (ST)

➤eucrim ID=1001027

Organised Crime

Commission Steps up the Fight against Trafficking in Human Beings

On 29 March 2010, the Commission adopted a proposal for a Directive on preventing and combating trafficking in human beings and protecting victims, thus repealing Framework Decision 2002/629/JHA. The proposal builds upon the 2000 United Nations protocol on trafficking in persons, especially women and children, and the 2005 Council of Europe Convention on action against trafficking in human beings. It follows up on a 2009 Commission proposal that was under negotiation but lapsed with the entry into force of the Lisbon Treaty (see eucrim 4/2009, p. 132). The new Directive covers various actions to be taken, such as:

- Revising criminal law provisions, including the development of a common definition of the crime, and introducing higher penalties;
- Implementing extraterritorial jurisdiction (the possibility to prosecute EU nationals for crimes committed in other countries) and using investigative tools typical for organised crime cases, such as phone tapping and tracing proceeds of crime;

■ Strengthening victims' rights in proceedings and supporting victims, e.g., by providing victims with shelters, medical and psychological assistance, information, and interpretation services;
■ Fostering prevention measures aimed at discouraging the demand for trafficking;
■ Establishing monitoring bodies in the Member States.

The proposal will now be discussed in the EP and in the Council. (ST)
➤eucrim ID=1001028

Piracy and Armed Robbery against Ships: Commission Recommendations

On 11 March 2010, the Commission adopted recommendations on measures for self-protection and the prevention of piracy and armed robbery against ships. Given that piracy figures for 2008 were the highest since the International Maritime Bureau began collecting data in 1991, the Commission requests the Member States to ensure the effective and harmonised application of preventive measures in order to deal with the threats ships may face during acts of piracy and armed robbery. The recommendation lists general measures, such as ensuring that the ships are sufficiently and effectively manned, as well as specific measures for the Gulf of Aden and the situation off the coast of Somalia, which include, e.g., a close risk assessment prior to transiting the high-risk area or rules of conduct to follow when being attacked by pirates. (ST)
➤eucrim ID=1001029

MEPs Discuss Use of Body Scanners

On 10 February 2010, the EP held a debate on the fight against terrorism and the use of body scanners. The body scanner debate – which focused on whether scanners are efficient, compatible with the right to privacy, and have an impact on health – has issued since the thwarted airline attack in Detroit that led to the events of 25 December 2009 (see eucrim 4/2009, p. 131). The MEPs concluded that one of the major reasons for the Detroit incident had to do with the problem of information exchange. Although MEPs appeared to be rather sceptical with regard to body scanners, they concluded that, if body scanners are to be used, they must be introduced across the entire EU. Prior to their introduction, questions about their efficiency, dangers to public health, and the risks to fundamental rights must be dealt with. (ST)
➤eucrim ID=1001030

Annual Forum on Combating Corruption in the EU: Incorporating Anti-Corruption Policy into the EU Accession Process

25–26 February 2010, Trier, Germany

This seminar was the fourth event that the Academy of European Law organised with the financial support of the European Commission/OLAF (under the Hercule II programme) on the anti-corruption policy of the EU.
This year's forum aimed mainly at discussing the incorporation of anti-corruption policy into EU accession policy.
The major theme was chosen by ERA and OLAF since, in candidate countries, as well as in third countries, the fight against corruption has become much more prominent during the past several years. Although significant results have been achieved and many of these countries have adopted national anti-corruption strategies, corruption remains paramount.
The conference participants debated and exchanged ideas on how to improve the EU's fight against corruption mainly from a practical perspective. Based on the experience gained in the first three annual fora held in Trier, the seminar provided a sound overview of existing anti-corruption legislation at the European and international levels (first morning session).
Then, the focus of the seminar shifted towards EU anti-corruption policy with regard to accession and third countries. Case studies were also presented (afternoon session and second morning session).

The seminar was intended to be a discussion forum where international, European, and national experts could present the subject matter from their own points of view. This objective was clearly met. Representatives from OLAF, the European Commission, and the Council of the EU as well as national experts (from Switzerland, Croatia, and Romania) attended the seminar. The main audience consisted of EU lawyers, prosecutors, and anti-fraud investigators. All in all, the seminar brought together 100 legal practitioners and experts, some of them from the national associations for the protection of the financial interests of the European Communities.
A second objective was to consolidate the ERA-OLAF practitioners' forum on EU anti-corruption policy even more. This goal was also achieved. In the summer of 2009, many prospective participants already informally approached the ERA organisers in order to obtain information about the 2010 forum so that they could block their agendas. This is a clear sign that they consider this forum to be an important annual event.

For further information, please contact Mr. Laviero Buono, Head of Section for European Public and Criminal Law, ERA. E-mail: lbuono@era.int

Cybercrime

Council Conclusions on Cybercrime Strategy

During its meeting on 26 April 2010, the Council adopted conclusions concerning an action plan to implement a concerted strategy to combat cybercrime. The conclusions include short and medium term actions to be taken in order to specify how the main points of the strategy should be implemented. The short term conclusions cover inter alia:
■ Obtaining knowledge on perpetrators and modus operandi and sharing this knowledge, in particular by using the Europol network;
■ Consolidation and revision of the functions assigned to Europol's European Cybercrime Platform (ECCP), in order to facilitate the collection, exchange, and analysis of information;
■ Implementation of priorities supported under the Safer Internet Programme 2009-2013 and the Prevention of and Fight against Crime (ISEC) Programme;
■ Continuation of current initiatives in

this field, such as the CIRCAMP project to develop a filtering system against child sexual abuse content, the Europol Working Group on Monitoring of Internet Communication, and the inventory of good practices to investigate commercial distribution of child abuse images (the European Financial Coalition (EFC) in cooperation with Eurojust);

- Promotion of the use of joint investigation teams.

The medium term conclusions cover inter alia:

- Ratification of the Council of Europe Cybercrime Convention;
- Improvement of the training of the police, judges, prosecutors, and forensic staff to a level appropriate for carrying out cybercrime investigations;
- Adoption of a common approach in the fight against cybercrime internationally, particularly in relation to the revocation of domain names and IP addresses;
- Setting up of a documentation pool on cybercrime, one to which all the actors involved have access, and serving as a permanent juncture between the respective authorities, users' and victims' organisations, and the private sector;
- Drawing up of a feasibility study on the possibility of creating a centre to carry out the aforementioned actions.

The Council requests these measures to be included in the Action Plan accompanying the Stockholm Programme and the future Internal Security Strategy mandated therein. (ST)

➤eucrim ID=1001031

Environmental Crime

Commission Sends out Warnings to Greece, Spain, Sweden, Austria, Romania, and the UK

The European Commission is becoming serious about Member States' failures at the environment's expense. Warnings about infringements of EU laws have recently been sent out to a number of countries and may be followed by actions before the ECJ in case the Member States do not comply.

Greece has again been warned about two failures to put into effect biodiversity legislation in a satisfactory manner. The Commission is also sending Greece two warnings about failures to protect wild birds. A separate warning is being sent about its failure to establish and implement a coherent, specific, and complete legal regime which would guarantee sustainable management and an efficient protection of the special protected areas that have already been designated.

➤eucrim ID=1001032

Spain has received a final warning about a breach of EU law governing the treatment and disposal of industrial waste. The case concerns the stockpiling of industrial waste in the Huelva estuary without the necessary waste management measures for the protection of the environment.

➤eucrim ID=1001033

Austria and Sweden have just received final warnings about industrial installations that are either operating without permits or with permits that are now out of date. Austria and Sweden have now been asked to issue new permits or update the outdated ones if they do not want to face proceedings before the Court of Justice.

➤eucrim ID=1001034

Romania has been warned about a breach of EU law regarding environmental impact assessments. A formaldehyde production plant was built in Romania in 2007 without a permit and before any impact assessment had been made.

➤eucrim ID=1001035

Finally, the United Kingdom has been warned about unfair costs of challenging decisions. It is a principle of EU environmental law (see, e.g., the Environmental Impact Assessment Directive and the Integrated Pollution Prevention Control Directive) that citizens have a right to know about the impact of industrial pollution and the potential impact projects may have on the environment as well as a right to challenge such decisions. Since legal proceedings in the UK can turn out to be very costly, the Commission is concerned that this might keep NGOs and individuals from bringing cases against public bodies. (ST)

➤eucrim ID=1001036

Sexual Violence

One Step ahead in the Fight against Child Pornography

On 29 March 2010, the European Commission adopted a proposal for a new Directive on combating sexual abuse, sexual exploitation of children, and child pornography. This is a follow-up on a 2009 Commission proposal and provides a large scope of actions, which tackle these offences on several levels (see eucrim 4/2009, pp. 133-134).

The proposed Directive takes into account the increasing forms of child sexual abuse and exploitation, envisaging the criminalisation of such new offences like "grooming" (luring children through Internet and abusing them) as well as viewing child pornography without downloading files. In addition, it determines that minimal levels of penalties be set to ensure that sanctions reflect the gravity of the crimes. By amending the rules on jurisdiction, the Directive also seeks to ensure the prosecution of offences committed abroad via so-called sex tourism, where child sexual abusers or exploiters from the EU have committed their crimes in non-EU countries.

The proposal further provides offender-specific measures, including an individual assessment as well as special programs aimed at preventing offenders from committing new crimes. With respect to child protection, the Directive determines that the prohibitions on activities involving contact with children imposed on offenders should be effective throughout the EU rather than solely within the country in which they have been convicted.

The protection of victims is also addressed through provisions aimed at reducing the additional trauma of child victims resulting from interviews by law enforcement and judicial authorities. They include the limitation of interviews as well as the provision of legal aid or a special representative.

The proposal, taking into account recent IT developments, provides for national mechanisms to block access to websites with child pornographic content. Objections to this approach have already been raised by German justice minister Sabine Leutheusser-Schnarrenberger, who argues that effectiveness demands the eradication of such sites rather than the mere denial of access.

The proposed Directive will now be discussed in the European Parliament and the EU Council of Ministers and, if approved, it will replace the current EU legislation dating from 2004 (Framework Decision 2004/68/JHA). (NK)

➤eucrim ID=1001037

Procedural Criminal Law

Data Protection

Mandate for new EU-US SWIFT Agreement

After rejection by the EP of the EU-US SWIFT Agreement (see eucrim 4/2009, pp. 135-136), the conclusion at the JHA Council of 25-26 February 2010 was that there is a pressing need to put in place a new EU-US Agreement to maintain the Terrorist Financing Tracking Programme (TFTP). Thus, the Commission – which wants a new agreement by June 2010 – adopted a draft mandate for negotiating bank data transfers with the US government under the TFTP on 24 March 2010.

The text of the draft mandate, which includes guidelines for the negotiations, has not been made public. During the press conference announcing the adoption of the mandate, the Commission's Vice President, Viviane Reding, stated that while drafting the mandate, the most essential concerns of the EP – notably the right to privacy and to effective redress – had been taken into account. Commissioner for Home Affairs, Cecilia Malmström, stated during the same press conference that the EP will be informed at all stages of the negotiation procedure.

Members of the EP, who had discussed the mandate during a meeting of the Committee for Civil Liberties, Justice and Home Affairs (LIBE Committee) on 7 April 2010, expressed concerns about the level of data protection of the mandate. On 5 May 2010 the EP adopted a Resolution on the Recommendation from the Commission to the Council to authorise the opening of negotiations for an agreement between the EU and the US to make available to the US Treasury Department financial messaging data to prevent and combat terrorism and terrorist financing. In this Resolution the EP explains its concerns inter alia regarding the principle of purpose limitation, the principles of necessity and proportionality, bulk transfers of data and judicial oversight.

During the JHA Council of 22-23 April 2010, political agreement was reached on the negotiating mandate for the EU-US agreement on the processing and transfer of financial messaging data for purposes of the TFTP. The agreement is meant to allow the US Department of the Treasury to receive financial messaging data stored in the EU in order to enable targeted searches in counter-terrorism investigations, while ensuring an adequate level of data protection.

Formal adoption of the mandate by the Council is still needed. (EDB)

➤eucrim ID=1001038

EU Terrorist Financing Tracking Programme

On 24 March 2010, the Commission's Vice President, Viviane Reding, announced that the future EU-US Agreement for financial messaging data transfers under the Terrorist Financing Tracking Programme (TFTP) would explicitly provide US reciprocity should the EU set up its own TFTP.

The TFTP is a programme set up by the US Department of the Treasury (UST) consisting of legislation and executive orders that allow the UST to use measures to identify, track, and pursue those who provide financial support for terrorist activity. It was based on this programme that the UST had received financial messaging data from SWIFT, the Belgian company that transfers instructions for interbank payments on an international scale.

The idea of setting up an EU version of the TFTP would be an important factor in negotiations with the US on the new agreement. It could mean that the EU could investigate its own financial messaging data before sending the results to US authorities. Nevertheless, this requires new EU legal instruments that would have to be approved by the EP and by the Member States.

The Commission aims to conclude a new agreement on the transfer of financial messaging data by June 2010, but the timing regarding an EU TFTP will be subject to negotiations with the US. (EDB)

➤eucrim ID=1001039

EP Postpones Vote on PNR Agreements with US and Australia

On 5 May 2010, the EP voted on a resolution that recommends postponing the vote to approve two agreements on the transfer of passenger name record (PNR) data.

It concerns the Agreement between the EU and the US on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the US Department of Homeland Security (DHS) signed on 23 and 26 July 2007 as well as the Agreement between the EU and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carri-

ers to the Australian Customs Service signed on 30 June 2008.

These two agreements have only been provisionally applied since they were signed subject to their conclusion at a later date. On 18 December 2009, the Commission submitted to the Council proposals for a Decision on the conclusion of both agreements. Due to the entry into force of the Lisbon Treaty, the conclusion of both agreements now needs to be approved by the EP.

The PNR agreements have been the subject of criticism by the EP in the past (see also eucrim 1-2/2008, pp. 29-31; eucrim, 3-4/2007, p. 101 and eucrim 1-2/2007, pp. 9-10) due to their lack of solid data protection safeguards. In relation to the PNR agreements, the Civil Liberties, Justice and Home Affairs Committee (LIBE Committee) requested the assessment of the Article 29 Data Protection Working Party. The Working Party concluded on 6 April 2010 that the EU-US PNR Agreement remains a challenge while the PNR Agreements with Australia and Canada (with regard to the EU-Canada Agreement, approval of the EP has not been asked for yet) show that it is possible to reach a higher level of data protection. Issues concerning the PNR Agreement with the US pointed out by the Working Party include proportionality, unclear periods of data retention, the nature of the data that are collected, the broad definition of the purposes data can be used for, and the method of transfer.

The motion for resolution of 19 April 2010 proposes the postponement in order to give the Commission time to work on the "PNR package" that Commissioner for Home Affairs, Cecilia Malmström, announced during the plenary debate of 21 April 2010. This package should include a list of requirements for negotiating agreements with third states and renegotiating PNR agreements with the US, Australia, and Canada. The motion for resolution already sets out minimum requirements for new legal instruments ensuring solid data protection. These requirements include respect for the principles of proportionality, legality, purpose limitation and data retention; legal redress; regulation of onward transfers and the transfer of data based on the push-method (transferring requested data rather than allowing the requesting authority to pull data from the relevant database) only. (EDB)

➤eucrim ID=1001040

Collecting Data on Processes of Radicalisation

On 16 April 2010, the General Affairs Council of the Council of the EU presented draft conclusions on the use of a standardised, multidimensional, semi-structured instrument for collecting data and information on the processes of radicalisation in the EU.

This instrument has its background in the Revised EU Radicalisation and Recruitment Action Plan – Implementation Plan (9915/09 ADD 1). It is seen as a first step towards facilitating and promoting a common approach for Member States' experts to document violent radicalisation processes and should result in a better exchange of information on them.

Europol is (within the limits of its competences) invited to support the production of lists of those involved in radicalising/recruiting or transmitting radicalising messages. SitCen is invited to use the proposed instrument for making analyses on the phenomenon of radicalisation in the EU.

Coreper has been requested to confirm the agreement on the text of the draft conclusions. (EDB)

➤eucrim ID=1001065

Victim Protection

Two Parallel Proposals for Directive on the Right to Interpretation and Translation

On 22 January 2010, the Council and the Parliament introduced an initiative – put forward by 13 Member States – for a Directive on the right to interpretation and translation in criminal proceedings.

This particular right was already the subject of a proposal for a Framework Decision presented by the Commission in July 2009. A general approach regarding the accompanying resolution had even been reached (see also eucrim 3/2009, p. 72). However, the decision-making process did not proceed fast enough for the instruments to be adopted before the Treaty of Lisbon entered into force. Framework Decisions – the typical legal instrument of the EU's former third pillar – have disappeared as legal instruments and have been replaced by decisions and directives in the Treaty of Lisbon.

Thus, the proposed Framework Decision was turned into a proposal for a Directive. Since the preparatory work was already done in 2009, the negotiations regarding the Directive could now proceed faster.

On 26 February 2010 the proposed Directive was discussed during the JHA Council meeting, where the Presidency stressed the good cooperation between the Council, the European Parliament, and the Commission in order to reach a text that would be satisfactory to all parties concerned. With this good cooperation in mind, it was particularly surprising for the Council to see that the Commission presented a parallel proposal for a Directive on the right to interpretation and translation on 9 March 2010.

The Council therefore expressed its regret about the Commission's decision to adopt a parallel proposal in a letter to Vice-President Reding. In this letter, the Council also expressed concerns regarding the confusion that the existence of two proposals could cause, for instance with national parliaments who will be asked again for their assessment of compliance with the principle of subsidiarity. Additionally, this situation may jeopardise the objective of reaching a quick agreement on the proposed Directive.

Both proposals were discussed by the

EP's Committee for Civil Liberties, Justice and Home Affairs (LIBE Committee) on 17 March 2010. As both proposals were similar but not identical – slight differences are apparent in scope and wording – the Commission suggested merging the two texts. This suggestion was rejected by LIBE Committee's rapporteur, Baroness Sarah Ludford. Her point of view was that the basic text used to formulate the amendments would still be the text proposed by the Member States, but that the Commission's proposal will be taken into close consideration. This procedure would ensure a faster agreement, supported by the fact that the United Kingdom Government and Ireland have opted-in to the Commission's proposal (despite the fact that both had previously been opposed to the measures). Not all members of the LIBE Committee agreed with the rapporteur and consultations continued.

Finally, on 8 April 2010, the Committee voted on a text that integrates the three main points of the Commission's proposal:

- Written translation of all essential documents (detention order, indictment, etc.);
- Interpretation for communication with lawyers as well as during investigations – such as police questioning – and at trial;
- The right to legal advice before waiving the right to interpretation and translation.

The next step is a vote by the EP in one of the upcoming plenary sessions, followed by discussions in the Council. (EDB)

➤eucrim ID=1001041

Proposal for a Directive on Protecting Victims of Trafficking in Human Beings

On 29 March 2010, the Commission presented its proposal for a Directive on preventing and combating trafficking in human beings and protecting victims, repealing Framework Decision 2002/629/JHA on combating trafficking in human beings.

The proposal had already been presented on 25 March 2009 as a Framework Decision. Due to the entry into force of the Lisbon Treaty, it was converted in a Directive.

The proposed Directive builds upon the CoE Convention on action against trafficking in human beings and adopts the same comprehensive approach including prevention, prosecution, protection of victims, and monitoring. In addition, the proposal includes precise penalties adapted to the severity of the offence, a wider scope of the provision on non-application of penalties to victims for their involvement in criminal activities, a higher standard of assistance to victims – including acting as witnesses in criminal proceedings and having access to witness protection programmes –, and special protective measures for child victims.

A significant feature of the proposal is also the broader and more binding extraterritorial jurisdiction rule, obliging Member States to prosecute nationals and "habitual residents" who have committed the crime of trafficking outside the territory of the Member State. (EDB)

➤eucrim ID=1001042

Cooperation

Police Cooperation

Erasmus Programme for Police Training Adopted

In April 2010, the Council's Police Cooperation Working Party reached agreement on draft conclusions on the exchange programme for police officers inspired by Erasmus (see eucrim 4/2009, p. 139).

In their draft, the Police Cooperation Working Party invites the European Police College (CEPOL) to develop an exchange programme within the following framework: the programme should aim at conducting exchanges for the purpose of study, mutual learning, and the pooling of knowledge and best practices in police work. Ultimately, these exchanges should improve efficiency, effectiveness, mutual trust, and mobility, thus creating a European police culture. The programme should initially cover a four-year period and take into account existing initiatives to apply the Bologna-related criteria in police training. CEPOL has been asked to present an evaluation report of the programme. Furthermore, CEPOL may consider enlarging the scope of the programme to all ranked police officers and police students. In addition, recommendations on the elements that should be included in a continuing exchange programme after the first four years are given.

Furthermore, the Police Working Party invites the Commission to examine the financial implications of a possible legislative proposal to enlarge the scope of CEPOL's activity, as appropriate, in order to allow it to manage and financially support an exchange programme for police officers of all levels as well as police students. Based on these results, the Commission has been asked to consider tabling such a proposal. (CR)

➤eucrim ID=1001043

Judicial Cooperation

European Investigation Order Launched

On 29 April 2010, Belgium, Bulgaria, Estonia, Spain, Austria, Slovenia and Sweden have launched an initiative for a Directive regarding the European Investigation Order in criminal matters (see eucrim 4/2009, p. 122 and p. 143).

For quite some time, the developed mechanisms with regard to gathering foreign evidence in the EU have been criticised for being fragmented and too complicated. The limited scope of the Framework Decision on the execution of orders freezing property or evidence (2003/577/JHA) under which the transfer of the evidence is still subject to the

rules of mutual legal assistance as well as its reluctant implementation by the Member States has resulted in many practitioners not seeing added value in the use of the instrument and thus, continue to apply the traditional ways of mutual legal assistance.

An even more critical approach has been taken with regard to the Framework Decision on the European Evidence Warrant (2008/978/JHA). Its limited scope only covering certain evidence that already exists as well as speculations about the likely issuing of either a second Evidence Warrant or a single comprehensive document covering all types of evidence has caused legislators to place its implementation low on their agendas and practitioners to prefer using the traditional procedures of mutual legal assistance.

The European Investigation Order (EIO) shall now offer a comprehensive system based on the principle of mutual recognition and covering, as far as possible, all types of evidence and replacing all existing instruments in the area.

The scope of the draft EIO, now broadened as much as possible, covers almost all investigative measures. Exemptions foreseen only concern JITs under Article 13 of the Convention of 29 May 2000 and Framework Decision 2002/465/JHA as well as some specific forms of interception of telecommunications. Furthermore, the EIO would not apply to cross-border observations under Article 40 of the Convention implementing the Schengen Agreement.

The EIO would be a judicial decision issued by a competent authority of a Member State in order to have one or several specific investigative measures carried out in another Member State with a view to gathering evidence. The EIO would be set out in a form for which a proposal is annexed to the draft Directive.

Transmission of the EIO could be done by any means capable of producing a written record. If required, the secured telecommunication system of the EJN could be used and EJN contact points could assist with identifying the executing authority.

The EIO shall be recognised without any further formality being required. Measures for its execution shall be taken the same way and under the same modalities as done for a national order. A new option is introduced by the possibility for the issuing authority to request to assist in the execution of the EIO. The executing authority is asked to comply with the formalities and procedures indicated in the EIO.

Recourse from an investigative measure other than that provided in the EIO is only possible in limited cases, namely if the measure does not exist under national law, if it is restricted to certain offences, or if an alternative measure achieves the same result by less coercive means.

Furthermore, a limited number of grounds for non-recognition and non-execution is foreseen, including immunity, essential national interests, the risk of jeopardising the source of information or disclosing classified information.

The decision of the recognition or execution shall be taken as soon as possible and no later than 30 days after the receipt of the EIO. The decision may be postponed if the execution would interfere with ongoing criminal investigations and prosecutions or the requested object(s) is already used in other proceedings. Receipt of an EIO shall be acknowledged by means of a form (Annex B to the draft Directive) without delay and at the latest within a week, unless there are reasons to inform immediately. The investigative measure shall be carried out without delay and no later than 90 days after the decision to recognise and execute. Under specific circumstances, shorter deadlines can be indicated in the EIO and extensions of the deadlines are possible. The evidence shall then be transmitted without undue delay.

The issue of legal remedies is left to national law but reasons for issuing an EIO can only be challenged in an action brought before a court of the issuing state.

Furthermore, the draft Directive contains provisions concerning criminal and civil liability regarding officials.

A detailed provision sets out rules for confidentiality of the investigation.

The fourth chapter of the draft Directive finally deals with specific provisions for certain investigative measures, namely the temporary transfer to the issuing State and to the executing State of persons held in custody for the purpose of investigation; hearing by video and telephone conference; information on bank accounts and banking transactions; monitoring of banking transactions; controlled deliveries, and investigative measures implying gathering of evidence in real time.

According to the draft Directive, an EIO may be issued for the temporary transfer of a person in custody in the executing/issuing state in order to have an investigate measure carried out for which his presence is required. In these cases, additional grounds for refusal are provided. The period of custody shall be deducted from the period of detention. Prosecution, detention, or other restrictions of personal liberty for acts or convictions conducted anterior to the departure are interdicted.

Regarding the hearing of witnesses, experts, and under certain conditions also of accused persons, in cases in which their appearance is not desired or possible, an EIO explaining these reasons may be issued in order to hear the witness or expert per videoconference or telephone conference. Again, additional grounds for refusal are provided. Furthermore, the Directive provides for several rules for the hearing by video- or telephone conference. Costs are to be refunded by the issuing Member State.

An EIO stating certain reasons can be issued to determine whether a natural or legal person subject of a criminal investigation holds or controls one or more accounts in any bank in the executing State. Several additional grounds are

foreseen to refuse the execution of such an EIO. Additionally, an EIO can be issued to obtain the particulars of a specified banc account and of certain banking operations and to monitor certain banking operations.

Finally, an EIO may be issued to undertake a controlled delivery on the territory of the executing State. (CR)

➤eucrim ID=1001044

European Arrest Warrant

The Proportionality Test Regarding the European Arrest Warrant (EAW)

On 25 February 2010, the Higher Regional Court of Stuttgart, Germany, decided on a Spanish EAW and took the opportunity to make fundamental observations on the principle of proportionality.

The case involved Mr. C., who is a Liberian national living in Germany, where he is serving a prison sentence and has a criminal record. The Spanish Public Prosecutor is seeking a prison sentence of 4 years against Mr. C. for trying to sell a bag of 0.199 gram cocaine to an undercover police officer in Spain. On application by the General Public Prosecution Service, the Court issued an arrest warrant for the purpose of extraditing Mr C. to Spain.

The principle of proportionality of criminal offences and penalties forms part of the constitutional traditions common to the Member States and is a general principle of the Union's law through Article 49 (3) of the EU Charter of Fundamental Rights on the prohibition of disproportionate penalties. This Article is binding on the Member States when they are implementing Union law. Thus, execution of an EAW must respect Article 49 (3).

The sentence of four years for the offence that Mr. C. is prosecuted for is not disproportionate due inter alia to the fact that there are no mitigating circumstances and the sentence does not constitute an intolerably severe sentence. The Court points out the difference between the proportionality test of the EAW (by the issuing authority) and the proportionality test of the German extradition arrest (by the executing authority). The German extradition arrest remains a sovereign act by a state authority and thus needs to comply with German constitutional law. The Court states that a proportionality test of a German extradition arrest warrant must minimally include an assessment of the requested person's right to liberty and safety, the cost and effort of a formal extradition proceeding including an extradition arrest, the significance of the charge, and the severity of the possible penalty.

Extradition arrests can, in particular, be disproportionate when they concern petty offences and the expected sanctions are out of proportion with the arrest and the extradition of the person involved. In the case at hand, the Court ruled that the extradition arrest was not disproportionate. The alleged offence is not a petty offence and the extradition arrest would not constitute a major burden for Mr. C. as the Court and the General Public Prosecutor will quickly decide on the merits of the extradition. (EDB)

➤eucrim ID=1001045

Draft "Standard Form on EAW Decision"

Following up the recommendation to develop a standard form providing information, in particular on the final – enforceable – decision (Recommendation 16 of the Fourth Round of Mutual Evaluations, see eucrim 3/2009, pp. 77-78; eucrim 4/2009, p. 143), the Spanish Presidency developed a draft "Standard Form on EAW Decision".

Such a standard form was recommended because the evaluation revealed the tendency of certain executing authorities to request excessive or overly detailed additional information from issuing authorities, concerning even the legal classification of the acts, and sometimes going so far as to request that documents (judgments, etc.) be sent. Such a practice, however, runs contrary to the principle of mutual recognition but is linked to the previous extradition procedure that has been replaced by the EAW procedure.

The proposed form consists of standard paragraphs on the identification of the EAW, the final decision of the EAW using boxes to tick reasons for refusal (e.g., minor, amnesty, no double criminality, etc.) or granting (e.g., consent), boxes to tick for surrender arrangements as well as a small paragraph for comments.

The use of the form, once adopted, would not be mandatory but recommended. The proposal has been sent to the Council's Working Party on Co-operation in Criminal Matters. (CR)

➤eucrim ID=1001046

Law Enforcement Cooperation

Updated JIT Model Agreement

On 19 March 2010, an updated Model Agreement for setting up a Joint Investigation Team (JIT) in accordance with Article 13 of the Convention of 29 May 2000 on Mutual Assistance in Criminal Matters and the Council Framework Decision of 13 June 2002 on Joint Investigation Teams was published in the Official Journal of the EU.

While the first Model Agreement of 2003 could not be based on best practices derived from actual experience, as there had been only few JITs in operation so far, the updated Model Agreement is now based on best practices regarding the establishment of JITs. The use of the Model Agreement is, as before, not obligatory but encouraged when setting up the modalities for a JIT.

When comparing both Model Agreements, the following similarities and differences can be observed:

- The first paragraph on the parties to the agreement remains the same.

25 Years Without Borders: Challenges for the Schengen Area Today

Trier, 16 – 17 September 2010

Twenty-five years ago, five EU Member States signed the Schengen Agreement removing systematic border controls between their countries. Today, the Schengen area consists of 25 European countries, the latest entrant being Switzerland.

This seminar will look at the development of the Schengen acquis and discuss its implementation today with representatives of the respective EU agencies, national police officers, and border guards.

The enlarged Schengen area has given rise to numerous new challenges for the protection of the EU's internal and external borders, including:

- The setting-up of a second generation for the Schengen Information System (SIS II);
- The establishment of common centres of police and customs cooperation to assist with cross-border surveillance, hot pursuit, joint patrols, and other joint operations under the Schengen Convention;
- The strengthening of FRONTEX operational capacities by introducing regional offices, Joint Support Teams, joint operations, return cooperation, etc.;
- Measures for a "European Integrated Border Management," such as an entry/exit system, a European Border Patrols Network, and a European Border Surveillance System (EUROSUR);
- New electronic technologies to ensure border control;
- A diverse pattern of opt-ins and opt-outs.

The seminar includes a visit to the village of Schengen and its Schengen documentation centre.

The seminar language is English.

For further information, please contact Mrs. Annette Geibel, Assistant Section for European Public and Criminal Law, ERA. E-mail: ageibel@era.int

■ When describing the purpose of the JIT, it is now recommended to include the circumstances of the crime(s) being investigated (date, place, and nature).

■ A new paragraph entitled "Approach" has been added, offering the parties agreement on an operational action plan (OAP), a flexible document setting out the practical agreements on a common strategy and on how to achieve the purpose of the JIT as well as the practical arrangements not otherwise covered by the agreement. In light of the relevant national legislation and its disclosure requirements, such an OAP can be included in the JIT agreement, or as an appendix to the agreement, or treated as a separate confidential document. A checklist regarding the points related to the possible content of the OAP is set out in Appendix IV to the draft Model Agreement. Issues on the check list include the operational procedure, role of members and/or participants of the JIT, information exchange and communication, intelligence assessment and tasking, evidence gathering, prosecution, testimony, disclosure, and administration and logistics.

■ For those cases where the expiry date set for a JIT needs to be extended, the updated Model Agreement now offers an additional appendix (Appendix II) setting out a standard agreement for the extension of a JIT.

■ Concerning JIT leaders, their replacement shall be designated without delay by mutual consent of the parties in an appendix to the agreement (instead of a decision by his superior, which was sufficient under the previous model agreement). For urgent cases, the updated agreement adds that notification by letter shall be sufficient, but it should be subsequently confirmed by the said appendix.

■ The table describing JIT Members now includes a column for the role of the member. It is clarified which persons can be JIT members. This may include representatives of judicial, police, or other competent authorities with investigative functions as well as the National Members of Eurojust, their deputies and assistants, and other persons who, in line with their national legislation, are also members of the national office, e.g., seconded national experts. Police authorities may comprise members of the Europol national units of the Member States and liaison officers of the Member States at Europol. Eventual replacements of such members should be designated without delay in an appendix to this agreement or by a written notification sent by the competent leader of the JIT. Finally, members of a JIT whose identity must be protected (e.g. in covert investigations, cases of terrorism, etc) may receive identification numbers that can be included in a confidential document. If no identification number can be assigned, the Model Agreement suggests agreeing that the identity of the members is set out in a confidential document, which is attached to the agreement and made available to all parties thereto.

■ Looking at participants to a JIT, i.e., representatives of third countries, Eurojust, Europol, the Commission (OLAF), bodies competent by virtue of provisions adopted within the framework of the Treaties, and international organisations which participate in the activities of the JIT, the updated Model Agreement provides for a separate appendix (Appendix I). This detailed appendix includes an additional agreement laying down the participating parties; the participants name, role, rank; regulations concerning their replacement; specific arrangements regarding the condition and purpose of their participation (e.g., reconferred rights, costs, data protection rules). Furthermore, the appendix foresees detailed provisions regarding the participation of Europol outlining principles for Europol's participation (e.g., no involvement in the taking of any coercive measures), types of assistance Europol can provide for (e.g., operational and strategic analytical support via the Analysis Work Files, technical support such as the Europol "mobile office", forensic support), access to Europol information processing systems, costs and equipment.

■ A new section of the updated Model Agreement deals with evidence. Accord-

ing to the new provision, parties shall entrust the leader or a member(s) of the JIT with the task of giving advice on the obtaining of evidence. His role shall include providing guidance to members of the JIT on aspects and procedures to be taken into account in the taking of evidence. The person(s) who carry out this function should be indicated in the agreement. In the OAP, parties may inform each other about testimony given by members of the JIT.

■ For amendments to the agreement – such as the incorporation of new members of the JIT, changes to the purpose and additions or changes to the current articles –, wording has been suggested in the form of the new Appendix III.

■ Another new item of the Model Agreement is a paragraph on internal evaluation asking the JIT leader(s) to evaluate the progress achieved, at least every six months, as regards the general purpose of the JIT. Furthermore, a final meeting to evaluate the performance of the JIT and the drawing up of a report on the operation is suggested.

■ Finally, the former paragraphs on specific and organisational arrangements have been merged and now include new provisions concerning the media, the confidentiality of this agreement, expenditure (e.g., insurance, translation and interpretation, expenses or income arising from seized assets), and the confidentiality and use of existing and/or obtained information. (CR)

➤eucrim ID=1001047

Model Agreement for Joint Cooperation Teams

In March 2010, the Spanish Presidency launched a proposal on a Model Agreement for setting up Joint Cooperation Teams under the so-called "Prüm Decision" (Council Decision 2008/615/JHA).

According to the "Prüm Decision", joint cooperation teams may be set up together with designated officials (officers) from other EU Member States for the purpose of conducting joint patrols and other joint operations in cases of disasters, serious accidents, mass gatherings and other major events, and other measures at a law enforcement authority station. Therefore, the scope is different from that of a Joint Investigation Team. Under its implementing Decision (Council Decision 2008/616/JHA), the development of such joint cooperation is conditional upon the conclusion of written or verbal arrangements between the competent authorities of the participating Member States.

Thus, in order to facilitate the work of the Member States when setting up a joint cooperation team, the Spanish Presidency seized the opportunity to propose a model agreement. The draft model agreement (which is very similar to but not to be confused with the Model Agreement on Joint Investigation Teams, see above) foresees standard provisions regarding the parties to the agreement, its purpose, place and period of the operation, responsible officers, other participating officers, specialists, advisers, executive powers of the officers seconded to the joint cooperation team, etc.

The proposal is currently being discussed in COREPER. (CR)

➤eucrim ID=1001048

Council of Europe*

Reported by Dr. András Csúri

Foundations

European Court of Human Rights

ECHR Launches Information on Case-Law in Non-Official Languages

The European Court of Human Rights (ECtHR) HUDOC database has recently made available translations of its key judgments in over ten non-official languages. Additionally, the HUDOC search portal also provides links to third-party collections of case-law in different languages. With this step, the Court aimed to make access to its case-law more open for website users who turn to its website for guidance, but are not well-served in either English or French. HUDOC currently features some 500 translations commissioned in the past by the CoE, with further translations to be added soon. Further progress is the possibility to single out judgments adopted by a Grand Chamber, a Chamber, or a Committee. The interface also provides answers to frequently asked questions on how to perform searches in HUDOC. In order to facilitate such searches, a list of keywords by Convention provision is also being made available. Extra RSS news feeds were also launched, in addition to those added in September (see also eucrim 3/2009, p. 83).

Access to a special page on the ECtHR's Internet site allows users to subscribe to the news feeds for judgments and decisions by a Grand Chamber, to weekly lists of important communicated cases, as well as to the facts,

* If not stated otherwise, the news reported in the following sections cover the period February 2010–April 2010.

complaints, and the Court's questions in such cases. In the near future, the ECtHR plans to publish new and more comprehensive case-law pages on its website with a cumulative index of cases published in its official series.
➤eucrim ID=1001049

New Italian Judge Elected

Mr. Guido Raimondi was elected as a judge to the ECtHR for Italy, replacing Vladimiro Zagrebelsky, who reached the age limit of 70 for the Court's judges.
➤eucrim ID=1001050

Specific Areas of Crime

Corruption

GRECO: Third Round Evaluation Report on Turkey

On 20 April 2010, the Council of Europe's Group of States against Corruption (GRECO) published its Third Round Evaluation Report on Turkey, focusing as always on two distinct matters: criminalisation of corruption and transparency of party funding.

Regarding the criminalisation of corruption, GRECO identified the country's legal framework as rather complex and stated that it contains several deficiencies in relation to the requirements of the CoE's Criminal Law Convention on Corruption (hereinafter: the Convention). The report suggests a thorough review of the legislation to clearly indicate what kind of conduct constitutes bribery. The most important shortcomings were found in the narrow definition of bribery offences. It excludes corrupt behaviour without an agreement between the parties or without a breach of duty by the public official. Moreover, the Turkish legislation does not fully address bribery of foreign and international officials, foreign jurors and arbitrators (all defined by the Additional Protocol to the Convention) as well as bribery in the private sector and trading in influence. GRECO furthermore found a high misuse-potential in the defence of "effective regret" (Section 254 Turkish Penal Code), as it leads to exemption from punishment in a very wide range of cases if the offender reports a crime after its commission and prior to commencement of an investigation. Therefore, GRECO recommends that Turkey revise the existing law in order to provide clear definitions of bribery offences. In addition, promises, offers, and requests for a bribe − irrespective of whether or not the parties agreed upon the bribe − have to be criminalised unambiguously. This also applies to all acts/omissions in the exercise of the functions of a public official, irregardless of whether he acted in breach of duty or whether he lied about the scope of his competence. In addition to this, the legislation should cover cases of bribery committed through intermediaries as well as cases where the advantage is intended for a third party. GRECO also suggests resolving deficiencies related to regulations on bribery in the context of international actors and activities. Regarding the defence of "effective regret," the report suggests revising the automatic and mandatory exemption from punishment and abolishing the restitution of the bribe to the bribe-giver in such cases.

Concerning the transparency of party funding, GRECO describes the existing legislation as being of a good standard and in many respects in line with the principles set out in Recommendation (2003)4 of the Committee of Ministers of the Council of Europe on Common Rules against Corruption in the Funding of Political Parties and Electoral Campaigns (hereinafter: Recommendation (2003)4). However, individuals (such as party candidates, independent candidates for election, and elected representatives) are not subject to transparency regulations that apply to political parties. The most obvious shortcoming of the current system is the lack of specific legislation and monitoring of campaign financing for parliamentary, presidential, and local elections.

GRECO stresses that party accounts tend to be incomplete, uncertified by independent auditors, and that comparisons are difficult if not impossible. As most parties do not even publish their accounts, the supervision of party finances certainly warrants further improvement. In view of the above, GRECO suggests that Turkey broaden the data content of the annual accounts of political parties with the above-mentioned missing aspects and that the political parties should provide more detailed and comprehensive information on their income and expenditure. These annual accounts and the corresponding monitoring reports should be made more easily accessible to the public, within timeframes to be specified by law. GRECO furthermore recommends finding ways to make the contributions of third parties more transparent. All of the above requires independent auditing of party accounts by certified experts, a matter which needs introducing.
➤eucrim ID=1001051

GRECO: Third Round Evaluation Report on Lithuania

On 17 February 2010, GRECO published its report on Lithuania within the Third Evaluation Round.

Regarding incriminations of corruption, the consistent regulations of the Lithuanian Penal Code limit legal loopholes in the existing bribery law and, with the exception of trading in influence, reflect most of the main requirements of the Convention. Besides this, Lithuania still has to sign and ratify the Additional Protocol of the Convention, which applies to arbitrators (in commercial, civil, and other matters) and jurors, as soon as possible. A clear indication of whether the beneficiary of a bribe is the bribe-taker himself or a third party is also missing.

The highlight of the first part of the report is the need to lower the level of proof required to convict a person for

corruption. As a consequence of the high level of proof, many possibly corrupt acts are presently not prosecuted.

In view of the above, GRECO suggests that Lithuania take additional measures (such as training or awareness-raising) to encourage the use of objective factual circumstances to substantiate bribery and trading-in-influence offences. To extend the concept of a bribe so as to clearly cover any form of benefit (material or immaterial, having identifiable market value or not), it should be in line with the concept of "any (undue) advantage" used in the Convention. Making clear that the advantages are not intended for the bribe-taker but for a third party is also covered by provisions on active bribery. The report further suggests analysing the regulation and use of the defence of effective regret in order to ascertain the misuse potential of this defence. GRECO states that Lithuania should increase the flexibility of the statute of limitation for the prosecution of offences and abolish the dual criminality requirement for the prosecution of bribery and trading in influence committed abroad by its nationals. Finally, the report suggests that the prosecution of corruption-related offences would benefit from an increased use of evidence based on objective factual circumstances.

Concerning the transparency of party funding, Lithuania's Law on the Financing and Financial Control of Political Parties and Political Campaigns of August 2004 is largely in line with the principles contained in Recommendation (2003)4.

GRECO suggests improvements in the following fields: The scope of the parties' consolidated accounts should systematically take into consideration their various components and structures. The valuation of in-kind donations must be clarified and the role of campaign treasurers strengthened. The highlight of the second part of the report is the need for more clarity in the supervision of party financing. Responsibility in this area is currently split between two institutions and their ability to exert control is more of a formalistic nature at present.

This is the case despite the common knowledge that parties and candidates handle more money than that which is officially declared.

In view of the above, GRECO stresses the need to rapidly strengthen the implementation of the law of 2004, supported by awareness raising and training initiatives. Furthermore, rules should be introduced that address the activity of third parties and it should be ensured that unused campaign funds transferred to charity organisations are not recycled to the parties.

The report recommends the limitation of unregistered donations (and their use) to the largest possible extent as well as the centralisation of campaign expenditure payments under the campaign treasurer's responsibility. It would be also reasonable to make it mandatory for political parties to open special campaign accounts. Regarding the system of sanctions applicable in the case of violation of the law of 2004, the report suggests a review to ensure that all possible infringements lead to sanctions. Furthermore, the report recommends increasing the level of administrative fines for infringements in the area of transparency of party and campaign funding as well as providing for the possibility to bar persons found guilty of such infringements from holding an elected office. Regarding the implementation of the law of 2004, GRECO suggests the constitution of a leading supervisory body which should function in an independent and impartial manner and would refer cases of suspected violations of the law of 2004 to the prosecutor. Ultimately, GRECO suggests extending the statute of limitation applicable to violations of the law of 2004.

➤eucrim ID=1001052

GRECO: Third Round Evaluation Report on Denmark

On 25 February 2010, GRECO published its Third Round Evaluation Report on Denmark in which it addressed 14 recommendations to the country. The most important recommendation is the introduction of more severe penal sanctions for corruption offences.

Regarding the criminalisation of corruption, GRECO found that the Danish criminal legislation complies overall with the standards of the Convention and its Additional Protocol. Nevertheless, the regulations are missing the offence of trading in influence, and the bribery provisions are not always as explicit as required by the Convention. Furthermore, the penal sanctions for corruption offences generally seem to be generally and need to be increased.

Denmark should also improve its possibilities to prosecute corruption abroad, and the introduction of criminal legislation against corruption should also be given high priority in Greenland and the Faroe Islands. Ultimately, the report recommends the abolishment of the requirement of dual criminality in respect of bribery offences when committed abroad.

Regarding the transparency of party funding, GRECO acknowledges that the electoral system in Denmark is dominated by a few political parties and that political funding is, to a large degree, funded by public means. Furthermore, GRECO welcomes the fact that the existing legal framework has been amended and now provides for more transparency, for instance by publishing party accounts. However, transparency could reach an even higher level through more precise reporting of donations exceeding a certain amount and by abolishing anonymous donations as well as restricting donations from abroad or from private companies. Finally, GRECO recommend developing the existing monitoring mechanism and moving away from the current rather formalistic method of checking to ensure more independent and substantial monitoring in respect of the funding of political parties and electoral campaigns.

➤eucrim ID=1001053

Money Laundering

MONEYVAL: 32nd Plenary Meeting

MONEYVAL's 32nd plenary meeting from 15-18 March 2010 achieved several significant results. At the plenary, MONEYVAL revised its rules of procedure regarding the examination of follow up reports, the application of compliance enhancing procedures, and decision-making processes. MONEYVAL further adopted its 2009 Annual Report and – in the context of the typologies project on money laundering through private pension funds and the insurance sector – also adopted a report on red flags and indicators. The next plenary meeting is scheduled from 27 September to 1 October 2010.

➤eucrim ID=1001054

MONEYVAL: Third Round Evaluation Report on Serbia

On 12 February 2010, the CoE's Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL) published its Third Round Evaluation report on Serbia.

As per its usual practice, the report analyses the implementation of international and European standards to combat money laundering (ML) and terrorist financing (TF), assesses the level of compliance with the Financial Action Task Force (FATF) 40+9 Recommendations, and recommends an action plan to improve Serbia's anti-money laundering (AML) efforts and those to combat the financing of terrorism (CFT).

The main findings of the evaluation report are the following:

The report acknowledged that, since the last evaluation (2005), Serbia has reviewed the efficiency of its AML/CFT system and made several changes that improved the legal framework and AML/CFT requirements. Criminal legislation was amended substantially and new legislation on the liability of legal entities was passed. In accordance with the adoption of an AML/CFT strategy, the country recently also adopted a new AML/CFT law.

MONEYVAL greeted the fact that Serbia's approach to the offence of ML is largely in line with international standards and has also been tested in practice, with several convictions being achieved. Nevertheless, implementation needs to be tackled by the authorities through a firm prosecution policy of money laundering offences, in particular for offences that generate major proceeds. Regarding the TF offence, the report found several legal shortcomings that need to be addressed.

MONEYVAL is concerned about the fact that the current system for investigation, prosecution, and adjudication of different types of ML/TF offences does not, in practice, provide optimal opportunities in respect of cooperation and communication between the competent authorities. Further specific concerns arise with regard to the independence of the prosecution service as well as the excessive workload and understaffing of the judiciary, specialized law enforcement services, and supervisory bodies.

The report found that the current regime needs to be reviewed in order to ensure that the competent authorities receive the necessary tools to clarify the application of the relevant provisions and thus ensure that they can make full use of the existing legal framework. MONEYVAL believes that the complex legal framework does not enable authorities to take the necessary preventive and punitive measures without delay, in accordance with the relevant United Nations Resolutions. The Serbian financial intelligence unit (FIU), the Administration for the Prevention of ML – though strengthened and seeming generally effective – is understaffed in the light of the tasks and duties set out in the new AML/CFT law. The report questions whether the detection of cross-border movement of currency is adequately pursued. Customer due diligence and record-keeping requirements were found to be broadly in line with the international standards. Regarding the reporting of suspicious transactions, there has been a constant increase in the number of reports by banks. However, there is a low level of understanding and implementation of the reporting requirement by non-banking financial institutions as well as a lack of AML/CFT supervision of designated non-financial businesses and professions (DNFBPs). Therefore DNFBPs need further guidance and feedback in implementing their AML/CFT obligations.

➤eucrim ID=1001055

MONEYVAL: Report on Fourth Assessment Visit to Slovenia

On 23 April 2010, MONEYVAL published its Report on the Fourth Assessment Visit to Slovenia. The 4th cycle of assessments is, in general, a follow-up round in which important FATF Recommendations are reassessed, as well as all those for which the state concerned received non-compliant or partially compliant ratings in its third round report. The on-site visit to Slovenia took place in October 2009, and the report mainly summarises, describes, and analyses the major AML/CTF measures in place in Slovenia at the time. Further, the report offers recommendations on how to strengthen certain aspects of the system.

The risk of the small country being used as a base for terrorism or the financing of terrorism is estimated as low, also due to the fact that Slovenia is not considered a major international financial centre. Despite introducing a number of measures in recent years to strengthen its AML/CFT regime, the levels of prosecutions for ML and orders to confiscate assets are very low. This fact notably undermines the effectiveness of the regime.

The designated FIU of Slovenia (Office for Money Laundering Prevention, hereinafter: OMLP) is well structured and professional. It operates effectively and has a good working relationship with the police and other relevant state agencies.

The basic elements of the Slovenian AML/CFT regime are contained in the Slovenian Criminal Code, which regulates the relevant offenses, in the Act on the Prevention of Money Laundering and Financing of Terrorism (APMLTF) as well as in the sector-specific laws.

This ensures a broad and sound legal structure with major preventive standards. No major deficiencies were detected in the key preventive standards. MONEYVAL expressed its concerns that weak supervision of and lack of guidance to certain non-banking sectors could have an impact on the effectiveness of the AML/CFT regime.

Slovenia has systems and procedures working well in practice in order to facilitate national and international cooperation. However, the report states that the lack of statistics in some areas made it difficult to gauge effectiveness.

➤eucrim ID=1001056

Russia: MOLI-RU 2

Further developments took place within the follow-up project MOLI-RU 2, which aims at further developing Russia's AML/CTF system in view of both practice and legislation (see also eucrim 1-2/2007, p. 45; eucrim 1-2/2009, p. 33; eucrim 3/2009, p. 85 and eucrim 4/2009, pp. 153-154). From 21-22 April 2010, MOLI-RU 2 organised an international seminar on AML in cooperation with the Nizhny Novgorod Academy of the Ministry of the Interior for detective officers specialized in AML and disruption of the economic basis of terrorism. The seminar aimed to raise awareness of the key elements of the AML/CFT regime and expose AML/CFT specialists to European standards within the sector. Investigation methods and case studies were also discussed during the course.

From 15-16 April 2010, MOLI-RU 2 held an international conference in Kazan adjusted to regional needs and focusing on the prevention of corruption and the laundering of corruption proceeds.

The MOLI-RU 2 project also supported the participation of five officials from the Russian Federation at the annual international conference on cooperation against cybercrime, which took place at the CoE from 23-25 March 2010 in Strasbourg. A report on this conference can be read in the following news section.

In cooperation with the Siberian Law Institute of the Ministry of the Interior, the MOLI-RU2 Project also supported the 13th conference on current issues of fighting crime in the Siberian region. The conference took place from 18-19 February 2010 in Krasnoyarsk. The conference participants primarily discussed the issues of the criminal situation in Siberia, research and prevention of crime in the region, the prevention of organised, group, and repeated crime as well as juvenile delinquency. The MOLI-RU2 project facilitated the participation of three foreign experts from the UK, Italy, and Sweden, who presented their international experience in combating corruption and, in particular, criminal law confiscation and the correlation between corruption and gifts.

➤eucrim ID=1001057

Cybercrime

Octopus Interface Conference

From 23-25 March 2010, over 300 cybercrime experts met at the Octopus Interface Conference in Strasbourg to enhance their cooperation in the fight against cybercrime. Prior to and during the conference, representatives from Azerbaijan, Montenegro, and Portugal ratified the Budapest Convention on Cybercrime (hereinafter: the Budapest Convention). Acknowledging that the growing threat of cybercrime worldwide comprises a wide range of initiatives, the participants adopted inter alia the following key messages, which were submitted to the United Nations Crime Congress in Salvador, Brazil (12-19 April 2010) for consideration:

- Measures against cybercrime must comply with human rights and the rule of law;
- The broadest possible implementation of existing tools and instruments is essential;
- Decision makers have to be made aware of the risks of cybercrime in order to encourage them to exercise their responsibility;
- The broadest possible implementation of the Budapest Convention worldwide;
- Strengthening of the Cybercrime Convention Committee (T-CY) as a

Advocacy Training for Criminal Defence Lawyers – Focus on the ICC and International Criminal Tribunals

Rome, 24–25 September 2010

The aim of this course is to provide criminal defence lawyers with the advocacy skills necessary to appear before the International Criminal Court (ICC) and other ad hoc international criminal tribunals.

The course will include:

- Explanation and demonstration of examination-in-chief/direct examination and cross¬examination;
- Practical exercise in examination-in-chief;
- Practical exercise in cross-examination;
- Mock trial.

The exercises will use case studies especially constructed for the course and designed to reflect the type of cases which participants will be dealing with in practice. The course will take account of the particular circumstances that prevail in the ICC and in international criminal tribunals. The trainers are familiar with different European trial systems and will therefore be able to contrast and compare the "adversarial" and "inquisitorial" systems. They will provide advice on how to improve both written content and style.

The training language is English.

For further information, please contact Mrs. Ute Beissel, Assistant Section for European Public and Criminal Law, ERA. E-mail: ubeissel@era.int

forum for information-sharing, policy-making, and as a standard-setting network;

- Encouragement of the T-CY to address issues not regulated in the Convention, such as electronic evidence, jurisdiction, and the liability of Internet Service Providers.

Stronger networking among existing networks in the global battle against cybercrime to allow synergies to flow and reduce duplication of work.

➤eucrim ID=1001058

12th UN Congress on Crime Prevention and Criminal Justice

The Congress took place in Salvador from 12-19 April 2010 and also reflected on the key messages submitted by the Octopus Interface Conference. It strengthened the idea of technical assistance and capacity building. The Congress also underlined that the latter should happen on the basis of existing instruments. This also includes existing legal instruments (like the Budapest Convention) as there was no agreement on a suggestion for preparation of a new treaty.

➤eucrim ID=1001059

Procedural Criminal Law

Recommendation CM/Rec(2010)3 to Member States on Effective Remedies for Excessive Length of Proceedings

On 24 February 2010, the Committee of Ministers adopted a Recommendation on effective remedies for excessive length of proceedings. The case law of the ECtHR and notably its pilot judgements provide guidance to the Member States. Excessive delays in the administration of justice constitute grave danger in respect of the rule of law and are often caused by systematic problems. Therefore, the Committee of Ministers recommends to the governments of the Member States:

- That all stages of domestic proceedings are determined within a reasonable time;
- To ensure that mechanisms exist to identify proceedings that risk becoming excessively lengthy;
- To address systematic problems if they are responsible for the excessive length of a proceeding;
- To ensure effective remedies at the domestic level for all arguable claims of violation of the right to trial within a reasonable time;
- To ensure compensation, including consideration of non-pecuniary damages;
- To consider specific forms of non-monetary redress, such as the reduction of sanctions.

➤eucrim ID=1001060

Network of Pilot Courts: 5th Plenary Meeting

The Network of Pilot Courts (NPC) held its fifth plenary meeting in Geneva on 13 April 2010 (see also eucrim 3/2009, p. 85). The NPC was established to foster a better understanding of the day-to-day work of the courts in Europe and to highlight best practices in order to improve the efficiency of judicial systems. Together with members of the European Commission for the Efficiency of Justice (CEPEJ) and other experts, meeting participants assessed the collection of statistical data on judicial time management and the implementation of satisfaction surveys for court users.

➤eucrim ID=1001061

The European Observatory of Judicial Timeframes: 7th Meeting

The Pilot Group of the CEPEJ SATURN Centre for judicial time management held its seventh meeting in Geneva from 12 to 14 April 2010. On this occasion, the Group analysed statistical data on the length of procedures and case flows provided by the Pilot Courts on the basis of the EUGMONT Guidelines (European Uniform Guidelines for Monitoring Judicial Timeframes), with the view towards setting up a European observatory of judicial timeframes. An experimental protocol of the tools and measures defined by the CEPEJ in the field of judicial time management will be proposed to Pilot Courts.

➤eucrim ID=1001062

Legislation

GRETA: The Netherlands Ratifies the CoE Convention on Action against Trafficking in Human Beings

The Netherlands is the 27th state to become Party to the Council of Europe Convention on Action against Trafficking in Human Beings.The Convention entered into force on 1 February 2008. The Netherlands accepted the Convention on 22 April 2010 and it will enter into force for this state on 1 August 2010.

➤eucrim ID=1001063

Data Protection in the EU – Challenges Ahead

Viviane Reding

I. Introduction

The processing of personal data has become an inherent part of the daily life of Europeans, for example when booking a flight ticket, transferring money, applying for a job, or just using the Internet for private purposes. Nobody wants to miss out on the advantages of modern technologies. Sometimes individuals provide their personal data simply because they choose to do so. But sometimes data is collected without consent and often without the knowledge of the individuals concerned. The protection of personal data is becoming more and more relevant as technology develops and the possibilities increase to use and misuse information more efficiently. Processing personal data also plays an increasing role in police and judicial cooperation: the lawful storage, exchange, and evaluation of information about a person can be an important instrument in ensuring public security.

The entry into force of the Lisbon Treaty[1] provides a much needed opportunity to reflect on the main challenges for the protection of personal data and on how the European Commission intends to address these challenges in the future.

II. The Protection of Personal Data at the European Level

The protection of personal data is one of the basic values in Europe, for the Member States of the EU and for the EU institutions. The current protection of personal data in the Union is governed by Article 8 of the Charter of Fundamental Rights of the European Union ("EU Charter")[2] and specified in the general Data Protection Directive 95/46/EC[3] as well as complemented by Directive 2002/58/EC on privacy and electronic communications.[4] The processing by EU institutions and bodies is covered by Data Protection Regulation (EC) No 45/2001.[5] Since 2008, the EU general framework for the protection of personal data in police and judicial cooperation in criminal matters is Framework Decision 2008/977/JHA.[6]

1. The protection of personal data as a fundamental right

Article 8 of the EU Charter of Fundamental Rights enshrines the fundamental right of every individual to the protection of his/her personal data. Equally, Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms[7] guarantees the right to respect private and family life, which includes the right to protection of personal data.

Article 8 of the EU Charter defines the basic principles for data protection in an exemplary way. It reads as follows:

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

Unlike other countries, notably the US, EU legal rules on data protection do not discriminate between EU citizens and foreigners – the fundamental right to personal data protection is guaranteed to "every person" in Europe, citizens and non-citizens alike.

2. The *acquis* for the protection of personal data

In secondary law, data protection in the EU has been regulated since 1995. This EU legal framework for data protection – primarily Directive 95/46/EC on the protection of personal data – has also served as a much admired standard for third countries when regulating data protection. Its effect and impact, within and outside the EU, have been of utmost importance.

Directive 95/46/EC is the central piece of legislation on the protection of personal data in Europe. It set a milestone in the history of the protection of personal data as a fundamental right. The principles of the protection of the rights and freedoms of individuals, which are contained in this Directive, notably the right to privacy, give substance to and amplify those principles contained in Council of Europe Convention 108 of 28 January 1981 (and its additional protocol on transborder data flows and independent supervisory authorities, added in 2001 after implementation of the Directive).[8]

Directive 95/46/EC enshrines two of the oldest aims of the European integration project: the achievement of an Internal Market (in this case, the free movement of personal data) and the protection of fundamental rights and freedoms of individu-

als. In the Directive, both objectives are equally important. Legislation at the EU level was justified because differences in the way that Member States approached this issue impeded the free flow of personal data between the Member States.

The Directive applies to and has been implemented by all 27 EU Member States as well as by the three EEA/EFTA States: Iceland, Liechtenstein, and Norway. Switzerland has also implemented the Directive for the Schengen area. In line with the Copenhagen criteria, all candidate countries are committed to transposing Directive 95/46/EC by the time of accession.

The Directive applies to both the public and private sectors. It develops and specifies data protection principles in order to achieve harmonisation throughout the EU. The Directive stipulates general rules on the lawfulness of personal data processing and the rights of the people whose data are processed ("data subjects"). The Directive also sets out that at least one independent supervisory authority in each Member State shall be responsible for monitoring its implementation. In particular, the Directive regulates transfers of personal data to third countries: in general, personal data cannot be exchanged with a third country unless the latter provides guarantees for an adequate level of protection.

In the area of police and judicial cooperation in criminal matters, the current data protection framework in the EU can only be described as a patchwork, as several instruments exist with specific data protection regimes or with data protection clauses. The legal provisions on Europol,[9] Eurojust,[10] the Schengen Information System,[11] and those contained in the "Prüm" Council decision[12] are just examples of such sector-specific regimes, the creation of different rights and obligations for Member States and individuals, and the setting up of several data protection supervisory authorities.[13]

Since 2008, Framework Decision 2008/977/JHA has aimed at creating an EU general legislative framework for the protection of personal data in police and judicial cooperation in criminal matters. Implementation of Framework Decision 2008/977/JHA is due for November 2010. It fully applies to the UK and Ireland, as well as Iceland, Norway, and Switzerland, as it is a development of the Schengen acquis. It does not, however, replace the rules applicable to Europol, Eurojust, Schengen, and the Customs Information System and also does not create a single independent supervisory authority.

Critics, such as the European Data Protection Supervisor (EDPS), point out that, in direct comparison with Directive 95/46/EC, this particular Framework Decision provides *inter alia* only for minimum standards and has a scope limited to the processing of personal data transmitted or made available between Member States.[14] In view of such shortcomings, the European Parliament explicitly called for a timely revision of Council Framework Decision 2008/977/JHA in its Resolution on the Stockholm programme.[15]

3. The Treaty of Lisbon

The Lisbon Treaty led to a fundamental change in the system for the protection of personal data in the EU:

- First, with the entry into force of the Lisbon Treaty on 1 December 2009, by virtue of the first subparagraph of Article 6(1) of the Treaty on European Union (TEU), the EU Charter of Fundamental Rights has the same legal value as the Treaties.

- Second, the Lisbon Treaty newly introduced Article 16 Treaty on the Functioning of the European Union (TFEU) to become the sole legal basis for the protection of personal data in the EU. On this basis, the European Parliament and the Council will – as co-legislators – be able to adopt rules with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law as well as rules relating to the free movement of such data. This is without prejudice to the specific rules for the protection of personal data laid down in Article 39 TEU for Common Foreign and Security Policy (CFSP) by Member States.

Article 16 paragraph 2 TFEU applies to all forms of data processing in the private and in the public sector and particularly includes the area of police and judicial cooperation in criminal matters, which was previously not the case. However, Declaration 21, attached to the Lisbon Treaty, states that specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 TFEU "may prove necessary because of the specific nature of these fields."

III. Challenges for the Protection of Personal Data

The main findings of the Eurobarometer Survey of 2008[16] show that a majority of EU citizens have concerns about data protection issues: two-thirds of survey participants said they were concerned as to whether organisations in possession of their personal data handled this data appropriately (64%). Most European Internet users feel uneasy when transmitting their personal data over the Internet: 82% of Internet users believe that data transmission over the Web is not sufficiently secure.

In very general terms, the main causes for this uneasiness result from three trends, which certainly pose a challenge for the protection of personal data in the future: the astounding capabilities of modern technologies, the increased globalisation of data flows, and access to personal data by law enforcement authorities that is greater than ever.

1. Modern technologies

The growth in new technologies, mobile Internet devices, and web-user generated content is increasingly pushing individuals to the fore when it comes to the "management" of their personal data, requiring a shift in focus on the part of policy makers. Social networking sites, like Facebook, MySpace, StudiVZ or Twitter, to name but a few, have become extremely popular on a global scale, particularly among young people. Millions of people use these sites everyday to keep in touch with friends, upload an unlimited number of photos, share links and videos, and learn more about the people they meet. All of this is based on personal data processing. And important revenue is being generated by tracking users on the Internet with "behavioural advertising."

2. Globalised data flows

Globalisation has seen an increasing role of third countries relating to data protection and has also led to a steady increase in the processing of the personal data of Europeans by companies and public authorities outside the European Union. For example, in a recent move, ten privacy commissioners from the national data protection authorities of Canada, France, Germany, Ireland, Israel, Italy, New Zealand, the Netherlands, Spain, and the UK addressed a joint letter to Google's CEO Eric Schmidt complaining that the company was overlooking privacy values and legislation when rolling out products. These regulators rightly want Mountain View[17] to adopt a set of data protection principles that include collecting and processing only the minimum amount of personal data needed for a Google product or service, providing better disclosure to its users, and creating privacy-protective default settings.

3. Access to personal data by law enforcement authorities

In addition to the increasing technical possibilities, the growing appetite for personal data for reasons of public interest, in particular for public security matters, is also an important challenge for data protection. The collection and processing of personal information can be very valuable in order to secure important and legitimate public and private interests – if done in a lawful way. A practical example is the use of body scanners for passenger screening at airports: before a new technology can be accepted as a regular and standardised method for passenger screening in all European airports, a careful assessment in regard to privacy and the protection of personal data is necessary. The assessment is complex, but the determinant criteria are clear: the use of body scanners must be lawful, their use and purposes laid down by law, the collected data must be necessary for passenger screening in order to improve security, no less intrusive alternatives regarding the privacy of passengers should be available that could achieve the same results, and there must be a sound relationship between the necessity and effectiveness of body scanners on the one hand and their impact on privacy on the other.

Due to the increase in transborder and transatlantic data processing as a means of preventing, detecting, investigating, and prosecuting criminal and terrorist acts, an effective protection of personal data is required, in particular, in the field of police and judicial cooperation, both within the European Union and when cooperating with international partners. The controversial discussions about these information exchanges have fuelled several specific agreements in the past between the USA and the EU, thus leading to the inclusion of provisions on the protection of personal data.[18]

IV. The European Commission Is Acting

The question has thus legitimately arisen whether today's legal framework at the EU level is still fully equipped to deal with all these new challenges – a question coming first and foremost from within the Commission itself.

1. Listening to stakeholders

In order to hear from the various stakeholders, the European Commission held a public consultation on the future of privacy, which featured – as part of a broader initiative – a review of the current European data protection framework in its entirety. This public consultation was intended to reach a broad sampling of stakeholders, based on three very open questions, leaving them as much leeway as possible in identifying new challenges, signalling out areas that would need improvement, and making suggestions on how a future legal framework could better tackle certain problems.

The preliminary results have shown that the current legal framework – in particular Directive 95/46/EC – is generally rooted in very strong data protection principles, still regarded as sound, and aptly equipped to regulate data protection

throughout the European Union. The technological neutrality of the Directive has also been widely celebrated and there is consensus on not stepping away from this paradigm. It is mainly the application of these principles in practice that causes problems and where action is needed.

The main challenges identified in the submitted contributions of the above-mentioned public consultation are the divergences between Member States' legislations implementing the Directive – which potentially disrupt the Internal Market –, the need for administrative simplification in dealing with Data Protection Authorities (e.g., regarding notification requirements), the need to update definitions and concepts in light of new technologies, and the need to better regulate international data transfers with third countries.

We also obtained confirmation that our citizens are increasingly worrying about what they perceive as a growing demand by public authorities to gather and request personal data, both inside and outside the EU, either directly or via private actors. Citizens are also concerned with whether they are still able to exercise their data protection rights once their data leaves the European Union.

The joint opinion of the Working Party established by Article 29 of the Directive together with the Working Party on Police and Judicial Cooperation[19] has made a notable contribution. The national data protection authorities identified key issues that have to be addressed in order to modernise and streamline the data protection framework, suggesting ways to better tackle these issues in the future. They see a further need to include the fundamental principles of data protection into one comprehensive legal framework at the EU level, which also applies to police and judicial cooperation in criminal matters.

2. An Action Plan for the next five years

With the entry into force of the Lisbon Treaty on 1 December 2009, the EU now has the tools to bring a new balance to policies in order to strengthen the rights and freedoms of Europeans. The protection of the fundamental right to data protection has been set as one important strategic initiative in the work programme of the Commission for 2010.[20]

In December 2009, European leaders endorsed the Stockholm Programme.[21] It sets out objectives aiming at creating a genuine European area of freedom, security and justice in the next five years. In April 2010, the European Commission turned these political objectives into an Action Plan for 2010–2014.[22] In the justice, fundamental rights and citizenship area, the plan includes proposals to improve data protection for data subjects in all EU policies – including law enforcement and crime prevention – and in relations with international partners. The Commission will tackle the challenges for the protection of personal data by means of two concrete actions:

a) Modernising Data Protection Directive 95/46/EC

Firstly, by the end of 2010, Data Protection Directive 95/46/EC will be modernised in response to the latest technological developments, so that the EU acquis continues to guarantee a high level of protection of individuals with regard to the processing of personal data. Also, the Commission aims at achieving a consistent, coherent, and effective legal implementation and application of the fundamental right to protection of personal data in all areas of the Union's activities.

This is likely to result in an increased harmonisation of data protection legislation in Member States by clarifying the application of some key rules and principles of data protection (such as applicable law, consent, and transparency), introducing some additional principles (such as "privacy by design"), strengthening the effectiveness of the system by modernising existing arrangements (e.g., limiting bureaucratic burdens), and – most importantly – by extending the fundamental principles of data protection into one comprehensive EU legal framework, which also applies to police and judicial cooperation in criminal matters.

Therefore, the rules of Framework Decision 2008/977/JHA should be improved and integrated into a new coherent legal framework based on Directive 95/46/EC, while taking into account the specificities of police cooperation and judicial cooperation in criminal matters where necessary. Where appropriate, this will also mean adapting and/or repealing existing data protection clauses or provisions in other former third pillar legislation. This exercise will, in the long term, also affect the current regimes for Europol and Eurojust. It will also affect other instruments devised in the former third pillar. Particular attention will have to be paid as regards the independent supervision of data protection processing where there are currently different supervisory authorities.

b) A data protection agreement between the EU and the US

Secondly, the Commission will present a negotiation text by summer 2010 for an "umbrella" data protection agreement between the EU and the US. As stated by the European Council in the Stockholm Programme, the EU must be a driving force behind the development and promotion of international standards for the protection of personal data. This data protection agreement should ensure a high level of protection of the fundamental rights and freedoms of natural persons, in par-

ticular the right to protection of personal data, and be fully in line with the EU Charter of Fundamental Rights as well as the Lisbon Treaty. It should only apply when personal data is transferred and processed by competent public authorities of the EU and its Member States and the US exclusively for the purpose of preventing, investigating, detecting, or prosecuting crime, including terrorism, within the framework of police cooperation and judicial cooperation in criminal matters, as these are the areas which have sparked controversy in the past.

The agreement should provide legal certainty and fill the current "protection gap" with a set of clearly defined data protection rights for European data subjects, such as the possibility to file complaints about unlawful processing of personal data. Data protection complaints by European citizens should be handled in the same manner as those filed by American citizens in US courts, which is not the case today.

V. Conclusion

There are many challenges ahead for the protection of personal data. Our citizens will now expect action and concrete results from Europe. The Lisbon Treaty and the adoption of the Stockholm action plan are ideally timed to turn our policies into practical results.

I have repeatedly stressed that I intend to use all of the powers given by the Lisbon Treaty to effectively improve the European rules on the protection of personal data, so that it may fully reflect the status of fundamental rights contained therein in daily life.

European personal data should be protected according to European data protection standards. This also means that, for any processing of personal data, there must be strong and effective supervision of these standards by independent supervisory authorities and, ultimately, the courts of justice. European data subjects must enjoy the protection of the same data protection principles from the North Cape to the tip of Malta Island, from the shores of the Atlantic to the Eastern Mediterranean Sea, and wherever their data are processed across other parts of the globe.

I am determined to work in this direction. I also have no doubt that the European Union will continue to fulfil its role as a key player in setting the standards for personal data protection, as it has done for the past 15 years.

Viviane Reding
Vice-President of the European Commission,
EU Commissioner responsible for Justice,
Fundamental Rights and Citizenship

1 For the consolidated versions of the Treaty on European Union and of the Treaty on the Functioning of the European Union, together with the annexes and protocols thereto, as they result from the amendments introduced by the Treaty of Lisbon, see OJ 2010 C 83/1.
2 Charter of Fundamental Rights of the European Union, OJ 2010 C 83/389.
3 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; OJ 1995 L 281/31.
4 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201 , 31/07/2002 pp. 0037–0047.
5 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data; OJ 2001 L 8/1.
6 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ 2008 L 350/60.
7 Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No. 11, Rome, 4.11.1950 (European Treaty Series – No. 5; http://conventions.coe.int).
8 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No.: 108; regarding supervisory authorities and transborder data flows, see also Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data CETS No.: 181, available at: www.coe.int.
9 Europol Council Decision of 6 April 2009 establishing the European Police Office (Europol) (2009/371/JHA), OJ 2009 L 121/37.
10 Eurojust Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime, OJ 2009 L 138/14.
11 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 2000 L 239/19.
12 Council Decision 2008/615/JHA, of 23 June 2008, on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, OJ 2008 L 210/1.
13 See for data protection authorities at the national level, the EDPS and the Joint Supervisory Board for Europol, Customs, Schengen (with a common secretariat), in addition to Eurojust and its Supervisory Body.
14 Cf. second and third opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters; OJ 2007 C 91/2; OJ 2007 C 139/01.
15 P7_TA-PROV(2009)0090.
16 Data Protection in the European Union-Citizens' perceptions- Analytical report,

Flash Eurobarometer Series 225, January 2008, http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf; http://ec.europa.eu/public_opinion/flash/fl_225_sum_en.pdf.
17 Mountain View is the seat of the headquarter of Google Inc. (1600 Amphitheatre Parkway, Mountain View, CA 94043, United States).
18 See, for example, the US-Europol cooperation agreement: http://www.europol.europa.eu/legal/agreements/Agreements/16268-2.pdf; US-Eurojust agreement: http://www.eurojust.europa.eu/official_documents/Agreements/061106_EJ-US_co-operation_agreement.pdf; 2007 Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS), OJ 2007 L 204 /16.
19 Joint contribution of Article 29 Data Protection Working Party and the Working Party on Police and Justice to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, adopted on 01 December 2009 (02356/09/EN WP). http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm.
20 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions; Commission Work Programme 2010 (COM (2010) 135, http://ec.europa.eu/atwork/programmes/index_en.htm.)
21 "The Stockholm Programme – An open and secure Europe serving and protecting the citizens", Council document 17024/09.
22 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions; Delivering an area of freedom, security and justice for Europe's citizens; Action Plan Implementing the Stockholm Programme COM(2010)171 final.

Transatlantic Adequacy and a Certain Degree of Perplexity

Dr. Els De Busser

The very least that one can say or write about the cooperation in criminal matters between the EU and the US is that it has intensified since 2001. The EU and its bodies that deal with criminal matters – Eurojust and Europol – have concluded agreements with US authorities. However, the data protection provisions in several of these agreements have raised eyebrows. The exchange of personal data is a crucial tool in judicial and law enforcement cooperation in criminal matters. The EU as an entity, but also Eurojust and Europol, entered into negotiations with the US in order to regulate the exchange of personal data that were deemed necessary for the purpose of prevention, investigation, and prosecution of criminal offences. A key requirement for the transfer of personal data from within the EU to a non-EU state (a third state) is the evaluation of whether this third state endorses a level of data protection that is adequate in comparison to the EU rules on data protection. This adequacy assessment should ensure the protection of personal data transferred to another legal system that applies different data protection rules.

When the US and the Council of the EU signed – on 30 November 2009 – a new Interim Agreement on the processing and transfer of financial messaging data for the purposes of the Terrorist Finance Tracking Program (TFTP), the European Parliament's Committee on Civil Liberties, Justice and Home Affairs examined the Agreement in order to recommend approval of the Agreement to the Parliament. The Committee asked the Article 29 Working Party (the independent EU Advisory Body on Data Protection and Privacy) and the Working Party on Police and Justice (a specific working group of the Conference of Data Protection Authorities) to evaluate this Interim Agreement. When dealing with the question of whether the US endorses an adequate level of data protection, a prerequisite for the EU for the exchange of personal data with the US, the following statement was made by the chairmen of both working parties: "Furthermore, the wording of Article 6 of the Interim Agreement, according to which the 'U.S. Treasury Department is deemed to ensure an adequate level of data protection', has brought about a certain degree of perplexity amongst the Working Parties' members." Thus far, a thorough examination has not been carried out in order to conclude on the adequacy of the US data protection system. The observation made by the two Working Parties regarding the lack of a genuine assessment of the American data protection rules is, in fact, not an isolated case. No assessment was made before signing the Interim Agreement and no assessment had been made prior to the conclusion of other agreements in the past.

In this article, examples of cooperation agreements with the US are examined, where, undoubtedly, members of data protection authorities and other data protection experts have experienced a similar "degree of perplexity" due to the lack of an adequacy assessment. First, the requirement for an adequate level of data protection will be clarified, followed by the challenges in applying this requirement. Subsequently, the agreements between the EU, Europol, and Eurojust, on the one

hand, and the US, on the other, will be scrutinised with regard to their compliance with the adequacy requirement.

I. Umbrella Legislation

The EU is known for utilizing "umbrella legislation" on the protection of personal data. This term refers to the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Data Protection Convention)[1] as the comprehensive legal instrument that covers all types of automatically processed personal data regardless of the purpose for which they are processed. It is referred to as "umbrella legislation" due to this wide scope. Because all EU Member States have ratified the Data Protection Convention, the data protection principles laid down therein are also the principles governing the EU's legislation on data protection. Therefore, when personal data are exchanged between authorities within one Member State or between authorities located in different Member States, they are transferred to a legal system that is bound by the same basic principles on data protection as the legal system they originated from.

Alternately, in a situation where the personal data are located in an EU Member State and transferred to a non-EU state (a third state), there are two possibilities. On the one hand, the receiving state could be bound by the Data Protection Convention[2] and thus by the same basic principles governing the EU's data protection regime. On the other hand, the receiving state could be a state that has a different view on data protection. This would mean that personal data could enter a legal framework that offers lower data protection safeguards than the EU Member State from which the data originated. The opposite case – stricter data protection rules in the receiving state – is equally possible, but would not give rise to many difficulties unless the smooth international exchange of data is hindered by applying stricter rules.

In order to protect the personal data transferred from a state bound by the Data Protection Convention to a state that is not bound by it, the Convention itself did not lay down any rules. However, one requirement was introduced[3] in the 2001 Additional Protocol to this Convention.[4] The Protocol obliges the states bound by it to assess the level of data protection of the receiving state. If the level of data protection endorsed by the receiving state is adequate, the transferring state can send the requested data. This is called the adequacy requirement.

The Additional Protocol is not the only instrument that lays down the adequacy requirement,[5] but it is the only one with an all-embracing – umbrella – scope including all personal data that are automatically processed. The adequacy requirement has also been copied in legal instruments that cover a more specific part of personal data processing.[6] This underlines the fact that the requirement of an adequate level of data protection has become known as a basic prerequisite for cross-border flows of personal data.[7]

II. The Paradox of the Adequacy Requirement

As appealing as it may sound in theory, the adequacy requirement causes many questions to arise regarding the assessment of the level of data protection and regarding whether the Member State is bound by the requirement or not. It is a prerequisite that has been laid down with the purpose of guaranteeing the EU's level of data protection and having the objective of ensuring that personal data of EU citizens are not subject to misuse in third states. A prerequisite of such a significant objective should at least be clear in its meaning, and it should be made a uniform requirement for all transfers of personal data to third states. However, this is not the case. Especially with regard to the sensitive area of criminal investigations and prosecutions, it would be logical to establish a strong data protection regime. This is the paradox concerning the adequacy requirement. The question as to exactly what an assessment of a state's level of data protection should minimally include has not yet been solved. In addition, this assessment is not a prerequisite for all Member States or all data transfers to third states. *A fortiori*, even when the assessment of the adequacy of the data protection regime in the third state is laid down as a requirement, it is not always applied as such.

1. How to assess adequacy?

The Additional Protocol to the Data Protection Convention specifies the necessity of an assessment of the level of data protection offered by the receiving third state, but does not specify how to carry out the assessment. According to the Explanatory Report to the Additional Protocol, the provisions of Chapter II (basic principles of data protection) of the Data Protection Convention should be taken into account when assessing the adequacy of the third state's legal framework on data processing. Nonetheless, this clarification is only valid as far as the Convention's principles are relevant for the specific case of transfer.[8] Thus, the basic principles of data protection do not necessarily have to be considered.

As a consequence, each judicial and law enforcement authority of each Member State could come up with its own concept for assessment of the level of data protection of the receiving third state. Differences in evaluation tools and methods as well as in the items evaluated can result in divergent outcomes, de-

pending on the authority or the Member State carrying out the assessment. From the point of view of the third state requesting personal data from two states that have ratified the Additional Protocol, this can lead to a different reply from each state and exacerbate the risk of *data-shopping*.

The development of a uniform checklist of the minimum provisions necessary for an adequate level of data protection would be an important step. In fact, the groundwork has already been laid. The Article 29 Working Party reflected on the matter and published a discussion document on the central question of adequacy. The document focused on the adequacy requirement in Directive 95/46/EC and was already published in 1997.[9] Even though it is not applicable to the field of criminal matters, the document provides good guidelines on what an adequacy assessment should include. These guidelines have been formulated in a general manner and could have easily been adjusted to fit adequacy assessment in criminal matters.

To allow for some flexibility on the part of the states exchanging data, the Additional Protocol allows for derogations from the adequacy requirement that should be interpreted restrictively.[10] Similar to the derogations from the provisions on human rights in the European Convention for Human Rights and Fundamental Freedoms (ECHR), they should at least be laid down by (national) law and be necessary for the protection of legitimate prevailing interests. Corresponding to the ECHR, the explanatory report to the Additional Protocol also refers to the same interests, based on which the right to privacy and data quality principles can be lawfully derogated from as follows: to protect an important public interest, the exercise or defence of a legal claim, or the extraction of personal data from a public register. Exceptions can also be made for the specific interest of the person whose data are transferred for the fulfilment of a contract with this person or in his interest, to protect his vital interests or if he has given his informed consent.[11]

In case an adequate level of data protection cannot be assured, another possibility for exchange still exists if the receiving state provides sufficient safeguards that are deemed adequate by the requested state. The safeguards can be limited, however, to include only the relevant elements of data protection and are only applicable to a specific transfer of data.[12]

2. Mandatory nature or the lack thereof

The adequacy requirement is not a requirement for all transfers of personal data from a Member State to a third state that is not bound by the Data Protection Convention. Three arguments motivate this statement.

Firstly, the Additional Protocol has so far been ratified by only 16 EU Member States.[13] Even though the Protocol has a general scope and is applicable to all automatically processed personal data, its partial ratification means that the adequacy requirement is not a uniform requirement for all data transfers from the EU to third states.

Secondly, the EU legal instruments including the adequacy requirement are only applicable to a specific group of data transfers. Directive 95/46/EC – which is implemented in every Member State – includes the same adequacy requirement, but is only applicable to data transfers that fall within the scope of Community law. Similarly, Regulation 45/2001[14] – which is also implemented in every Member State – has included a provision on the adequacy requirement, but is only applicable to the transfers of personal data made by Community institutions and bodies. The newest legal instrument in the field of data protection, the Framework Decision on Data Protection in Criminal Matters[15] – which needs to be implemented by all Member States by 27 November 2010 – is equally limited in scope. It is only applicable to the personal data that have been transmitted or made available by another Member State and excludes the data gathered by the requested Member State itself. The Framework Decision states that, in future agreements, the adequacy assessment should be ensured. Still, in accordance with the Framework Decision, Member States can derogate from the adequacy requirement for the protection of specific legitimate interests of the data subject, legitimate prevailing interests – especially important public interests –, or when sufficient safeguards are provided by the receiving state.

Thirdly, the data protection rules that the EU agencies Eurojust and Europol have laid down for themselves, and which govern transfers to third states, are very different from one another. Europol has introduced a four-step approach for reaching a decision on the adequate level of data protection of a third state.[16] With the exception of urgent circumstances,[17] the Management Board consults the Joint Supervisory Board (JSB) regarding the processing of data by Europol. Then, the Council of the EU conducts a second check and, in a third step, the Director initiates negotiations, after which the Management Board and the JSB need to give their approval to conclude the agreement in a final step. This four-step filtering system has no counterpart in Eurojust data protection rules. In accordance with the rules governing data transfers by Eurojust, an adequacy assessment by its data protection officer is sufficient. Eurojust does not involve the Council and only turns to the JSB when the data protection officer meets difficulties in making his assessment. The recent decision on strengthening Eurojust does not add to Eurojust's data protection provisions in order to improve the assessment.

Therefore, the mandatory nature of the adequacy requirement is diverse and depends on which Member State or EU agency is transferring data, whether the state has ratified the Additional Protocol or not, and on the data that are transferred. Obviously, this conclusion is only based on the EU's legal instruments and not on Member States' national law. Member States can – on their own initiative – incorporate an adequacy requirement for outgoing data transfers in their national law.
Only two cases exist in which all EU Member States are obliged to assess the adequacy of the level of data protection in a third state requesting personal data: that in which the processing of data falls within the scope of Community law and that in which the data are processed for the purpose of a criminal investigation, as long as it concerns data that the transferring Member State has received from another Member State. There is thus no general adequacy requirement for data processed for the purpose of prevention, investigation, and prosecution of criminal offences.

3. A "forgotten" requirement

Even when there is a clear obligation to make an adequacy assessment, there are cases in which it has been "forgotten". Obviously, the word "forgotten" is meant in an ironic sense here, as it is difficult to imagine mandatory rules accidentally not being applied. It is more likely that a conscious – politically more opportune – choice was made to disregard them. This is especially visible in transatlantic cooperation. The agreements made between the EU and its agencies mandated to deal with cooperation in criminal matters (Eurojust and Europol), on the one hand, and the US on the other, have one particular thing in common. They all ignore the adequacy requirement. As mentioned earlier, both Eurojust and Europol are bound by the adequacy requirement. They are not parties to the Additional Protocol to the Data Protection Convention, but have included the requirement in their own set of rules governing their data transfers to third states.

In the Europol Decision,[18] two possibilities are regulated by which Europol can transfer personal data to third states.[19] The general rule is the conclusion of an agreement, after authorisation of the Council and supported by a prior opinion of the JSB. As an exception, the Director of Europol can enter into negotiations without authorisation of the Council and without prior consultation with the JSB. Exceptional circumstances are defined – at the discretion of the Director – by the absolute necessity to transmit personal data in order to safeguard the essential interests of the Member States concerned, within the scope of Europol's objectives, or in the interest of preventing imminent danger associated with crime.[20] The Director must in these circumstances consider the level of data protection applicable for the receiving authority in the third state and weigh this against the essential interests. The parameters for making this assessment are laid down in Article 23 of the Europol Decision. In comparison to the Europol Convention, the Europol Decision adds a new parameter: "whether or not the entity has agreed to specific conditions required by Europol concerning the data."[21] This is a useful and necessary guideline for the Director. However, the provision of parameters to judge the adequacy of the level of data protection of a third state could have been developed into a more detailed checklist. Also, in the case of Europol, the question of what should be minimally included in an adequacy assessment has been left open.

The exceptional way for Europol to negotiate data transfers to third states – through the Director, without authorisation of the Council – was used to conclude two agreements with the US after the 2001 terrorist attacks.[22] The first of these agreements was, however, inserted into the conventional procedure at the Council meeting on Justice, Home Affairs and Civil Protection.[23] The Director of Europol was then authorised to conclude a cooperation agreement on the exchange of strategic information, not including personal data, the negotiations on which had already begun.[24]

During this same Council meeting, Europol received the authorisation to start negotiations on another agreement that would focus on the exchange of personal data. This would mean that the level of data protection of the US should be assessed in accordance with Article 18, §1, 2) of the Europol Convention (which was applicable at the time) and in accordance with the rules governing the transmission of personal data by Europol to third States and third bodies.[25] The Council noted during this meeting that a data protection report concerning the US had been drawn up by Europol.[26] Nonetheless, the JSB stated that Europol did not provide a report on the data protection law and practice in the US and that the JSB was therefore unable to make a conclusion on the level of data protection in the US.[27] On 3 October 2002, the JSB issued another opinion based on practical experiences with the US system and on presentations made during the negotiations.[28] The JSB stated that the Council was in the position to allow the Director of Europol to conclude the agreement, but expressed concerns about the purposes for which personal data would be used after their exchange to the US. Data should not be used for purposes outside the objectives of Europol. These concerns are not unreasonable since the purposes for which the data can be used in accordance with the Agreement have been widened by the parties in documents called "exchange of notes". These notes are not formally part of the Agreement, but are intended to assist its implementation.[29] Nonetheless, they explicitly state that the data that are exchanged in accordance with the Agreement can also be used for "inter alia, exchange

of information pertaining to immigration investigations and proceedings, and to those relating to in rem or in personam seizure or restraint and confiscation of assets that finance terrorism or form the instrumentalities or proceeds of crime, even where such seizure, restraint or confiscation is not based on a criminal conviction."[30] Immigration investigations and confiscation not based on a criminal conviction clearly go further than the objectives of Europol.

Still, the 2002 Supplemental Europol-US Agreement on the exchange of personal data and related information (2002 Europol-US Agreement) was signed on 6 November 2002. Proof of the US endorsing a data protection regime that fulfils the conditions of the adequacy requirement has not been produced to date. An informal explanatory note only reflecting Europol's view on the 2002 Europol-US Agreement, states, quite sarcastically, that the Agreement is "generally in line with the major principles incorporated in Europol's legal framework". The adequacy requirement does not seem to be considered a major principle of Europol's legal framework. The text of the note goes even further and states that the provisions of Article 5 of the Agreement on general terms and conditions "would not be used as a legal basis for generic restrictions, but only in specific cases where there was a real necessity."[31] The phrase "generic restrictions" can clearly be understood as the requirement involving an adequate level of data protection. This means that the note calls for the rejection of this requirement in the cooperation with the US.

The exception that has been made for the US could create political strife with other third states. Europol has negotiated agreements with Australia, Canada, Croatia, Iceland, Norway, and Switzerland. All of these agreements were negotiated after an opinion of the JSB was issued and confirmed by the Council that no obstacles exist to include the transmission of personal data in the agreement. The only exception that has been made so far is for the US.

Eurojust only exchanges case-related[32] personal data with third states bound by the Data Protection Convention or third states that support an adequate data protection system. In the latter case, possible additional safeguards can be included in agreements between the data controller and the third state.[33] Switzerland, Iceland, Romania, Norway, and Croatia all have ratified the Data Protection Convention. The US was the first state not bound by the Data Protection Convention to conclude an agreement with Eurojust. In fact, proof of an adequacy assessment of the US rules on data protection was not provided. Instead, the Eurojust JSB – which is responsible for monitoring data protection – remarkably preferred not to be involved directly in the negotiation process, but instead to be closely informed about the important steps and developments made.[34] The JSB expressed concerns regarding the use of data that had been made public regardless of whether the release had occurred lawfully or not.[35] The lack of an assessment on the level of data protection was not mentioned.

With regard to the inclusion of the adequacy requirement in the cooperation agreements, the Agreement concluded between the EU and the US on mutual legal assistance[36] and the Agreement concluded between Eurojust and the US[37] can be analysed together. The requirement has, in fact, been abolished in these instruments even more clearly than in the 2002 Europol-US Agreement. Both Agreements include an article on "limitations on use to protect personal and other data," which explicitly states that generic restrictions with respect to the legal standards of the requesting State or party in the processing of personal data may not be imposed by the requested State or party as a condition for providing evidence or information.[38] Where, in the 2002 Europol-US Agreement, the US was labelled an adequate partner with regard to its data protection regime, even though this was unjustified, in the 2003 EU-US Agreement and the 2006 Europol-US Agreement, the adequacy requirement was thrown overboard.

III. Continuing Along the Same Path

Four years after it was revealed that the Society for Worldwide Interbank Financial Telecommunication (SWIFT) answered to administrative subpoenas issued by the US Department of the Treasury (UST) by sending personal data (financial messaging data) in bulk for the purpose of investigating the financing of terrorism under the Terrorist Finance Tracking Programme (TFTP), the US called for an agreement with the EU on a regular transfer of these data. A change in SWIFT's architecture meant that a large amount of its data was no longer stored in the US, but in the EU. Thus, in 2009, the US and the Council of the EU began negotiating an agreement in order to establish the transfer of SWIFT's financial messaging data for the purpose of the TFTP. First, a temporary agreement of nine months – the Interim Agreement – was to be signed and, after that, a permanent agreement negotiated. However, the entry into force of the Lisbon Treaty made the European Parliament's consent a prerequisite for entry into force of the Interim Agreement. A substantial report written by Parliament Member Jeanine Hennis-Plasschaert[39] brought about the rejection of the Interim Agreement on 11 February 2010.[40] Not mentioned in the report as a reason to vote against the Interim Agreement, but nevertheless important, is Article 6, in which it is stated that the UST is "deemed to ensure an adequate level of data protection". The Article 29 Working Party and the Working Party on Police and Justice rightfully expressed their disapproval of this provision and pointed out that other reports

(that are confidential, such as the report by Judge Bruguière on the compliance of the TFTP with the safeguards offered by the UST) cannot necessarily substitute an adequacy assessment.

IV. Adequate Perplexity

Research has proven that the basic data protection principles applicable in criminal matters in the EU are not fully complied with in the cooperation between the EU Member States.[41] In much the same way as this internal exchange and its lack of duly applied data protection principles, compliance with the adequacy requirement is also problematic. In the external exchange of personal data between EU Member States and third states, the adequacy requirement is not a general requirement and has not been defined in detail. Differences between Member States' views on an adequacy check can thus lead to *data shopping* or the search by a requesting third state for the most "lenient" Member State. Therefore, the meaning of the requirement itself can be put into question. If you do not operate with the same criteria, why do you have the requirement in the first place? The answer should be to protect personal data transferred to third states that might have a different view on data protection than that represented by EU data protection principles. However, the protection that the adequacy assessment should offer is clearly not watertight.

Considering the major importance of the protection of personal data transferred for the purpose of a criminal investigation or prosecution, and also considering the high importance of the protection of personal data transferred to a state that has not ratified the Data Protection Convention, it is all the more surprising to see that the assessment intended to ensure this protection is not mandatory in the EU.

From a political point of view, it is also surprising to see the clear difference in the treatment of third states. The exception that has been made for the US of not carrying out an adequacy assessment has not been made for any other third state so far.

It is therefore understandable that the members of the Article 29 Working Party and the Working Party on Police and Justice reacted to the lack of an adequacy assessment in the Interim Agreement with an appropriate degree of perplexity. This degree of perplexity is equally justified with regard to the agreements that the EU, Europol, and Eurojust concluded with the US authorities.

Looking at the future of the adequacy requirement, the JHA Coucil that announces the mandate that has been adopted to launch negotiations between the Commission and the US authorities on a new agreement for the transfer of financial messaging data indicated that the Agreement shall contain safeguards and controls, which ensure an adequate level of protection of personal data.[42] Even though this is a general statement that is in need of further clarification as to which safeguards and controls will be provided, it is sure to trigger less perplexity on the part data of protection experts.

1 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, ETS no. 108, 28 January 1981.
2 So far, 14 third states have ratified the Data Protection Convention.
3 Chronologically, it was Directive 95/46/EC (O.J. L 281, 23 November 1995, pp. 31-50) that was the first instrument to include the adequacy requirement; however, the scope of the Directive is limited to the processing of personal data for the purpose of activities that fall within the scope of Community law.
4 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, 8 November 2001.
5 See, e.g., Directive 95/46/EC, O.J. L 281, 23 November 1995, pp. 31-50.
6 See, e.g. Article 26, Council of the European Union, Rules of procedure on the processing and protection of personal data at Eurojust, O.J. C 68, 19 March 2005, pp. 1-10 and Article 4, Council of the European Union, Act 12 March 1999 adopting the rules on the transmission of personal data by Europol to third states and third bodies, O.J. C 88, 30 March 1999, pp. 1-3.
7 See also European Data Protection Supervisor, Third opinion 27 April 2007 on the Proposal for a Council Framework Decision on the Protection of Personal Data processed in the Framework of Police and Judicial Cooperation in Criminal Matters, O.J. C 139, 23 June 2007, § 26.
8 Additional Protocol to the Data Protection Convention, ETS no. 181, 8 November 2001, Explanatory Report, § 29.
9 Article 29 Data Protection Working Party, XV D/5020/97-EN final, WP 4, 26 June 1997.
10 Additional Protocol to the Data Protection Convention, ETS no. 181, 8 November 2001, Explanatory Report, ETS no. 181, 8 November 2001, Explanatory report, §31.
11 *Ibid.*, §31.
12 *Ibid.*, § 32-33.
13 The protocol entered into force for Austria, Cyprus, Czech Republic, Estonia, Ireland, Germany, Hungary, Latvia, Lithuania, Luxembourg, Netherlands, Poland, Portugal, Romania, Slovakia, and Sweden.
14 European Parliament and Council, Regulation (EC) no. 45/2001, 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, O.J. L 8, 12 January 2001, pp. 1-22.
15 Council of the European Union, Framework Decision of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, O.J. L 350, 30 December 2008, pp. 60-71.
16 Council of the European Union, Decision of 27 March 2000 authorising the Director of Europol to enter into negotiations on agreements with third States

Dr. Els De Busser
Senior Researcher at the Max Planck Institute for Foreign and International Criminal Law, European Criminal Law Department

and non-EU related bodies, O.J. C 106, 13 April 2000, pp. 1-2.
17 In urgent circumstances, the Europol Director is authorized to transmit personal data to third states.
18 Council Decision establishing the European Police Office, O.J. L 121, 15 May 2009, pp. 37-66.
19 Council of the European Union, Act 12 March 1999 adopting the rules on the transmission of personal data by Europol to third states and third bodies, O.J. C 88, 30 March 1999, p. 1.
20 Article 2, §1, b) Council Act of 12 March 1999 adopting the rules on the transmission of personal data by Europol to third states and third bodies. The inclusion of terrorist offences is a new addition to this provision made by the Europol Decision.
21 Article 23, §9, e) of the Europol Decision.
22 *V. Mitsilegas*, The New EU-USA Cooperation on Extradition, Mutual Legal Assistance and the Exchange of Police Data, EFAR 2003, vol. 8, pp. 516-517.
23 European Council, 14581/01, 6-7 December 2001, p. 11.
24 The first draft, dating from 31 October 2001, is available in the Council of the EU's public documents database. Council of the European Union, 13359/01, Draft agreement between Europol and USA, 31 October 2001.
25 O.J. C 88, 30 March 1999, p. 1.
26 European Council, 14581/01, 6-7 December 2001, p. 11.
27 Europol JSB, Document 01/38, 26 November 2001, p. 2.
28 Europol JSB, Document 02/65, 3 October 2002.
29 Council of the European Union, 13696/1/02, 28 November 2002, p. 2.
30 Council of the European Union, 13996/02, 11 November 2002, p. 3.
31 Council of the European Union, 13696/1/02, 28 November 2002, p. 10.
32 Evidently, with regard to non case-related data exchange, the issue of an adequate level of data protection or adherence to the 1981 CoE Convention is not pressing as, in this respect, use for a wider range of purposes is allowed.
33 Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, O.J. L 63, 6 June 2002, Article 27, §4 and Council, Rules of procedure on the processing and protection of personal data at Eurojust, O.J. C 68, 19 March 2005, Article 28, §§ 2 and 3.
34 Joint Supervisory Body of Eurojust, Activity Report 2006, p. 6, www.eurojust.europa.eu
35 *Ibid*., pp. 6-7.
36 Agreement 25 June 2003 on mutual legal assistance between the European Union and the United States of America, O.J. L 181, 19 July 2003, p. 41.
37 Agreement between Eurojust and the United States of America, 6 November 2006, www.eurojust.europa.eu.
38 Article 9 of the 2003 EU-US Agreement and Article 9 of the 2006 Eurojust-US Agreement.
39 European Parliament Recommendation, A7-0013/2010, 5 February 2010.
40 O.J. L 8, 13 January 2010, p. 9.
41 *E. De Busser*, Data protection in EU-US criminal cooperation, Antwerp-Apeldoorn, Maklu, 2009, pp. 127-183.
42 Council of the European Union, 8920/10, 23 April 2010, p. 6.

Imprint

Impressum

Published by:

Max Planck Society for the Advancement of Science
c/o Max Planck Institute for Foreign and International Criminal Law
represented by Director Prof. Dr. Dr. h.c. Ulrich Sieber
Guenterstalstrasse 73, 79100 Freiburg i.Br./Germany

Tel: +49 (0)761 7081-0,
Fax: +49 (0)761 7081-294
Email: u.sieber@mpicc.de
Internet: http://www.mpicc.de

Official Registration Number:
VR 13378 Nz (Amtsgericht
Berlin Charlottenburg)
VAT Number: DE 129517720
ISSN: 1862-6947

The publication is co-financed by the European Commission, European Anti-Fraud Office (OLAF), Brussels

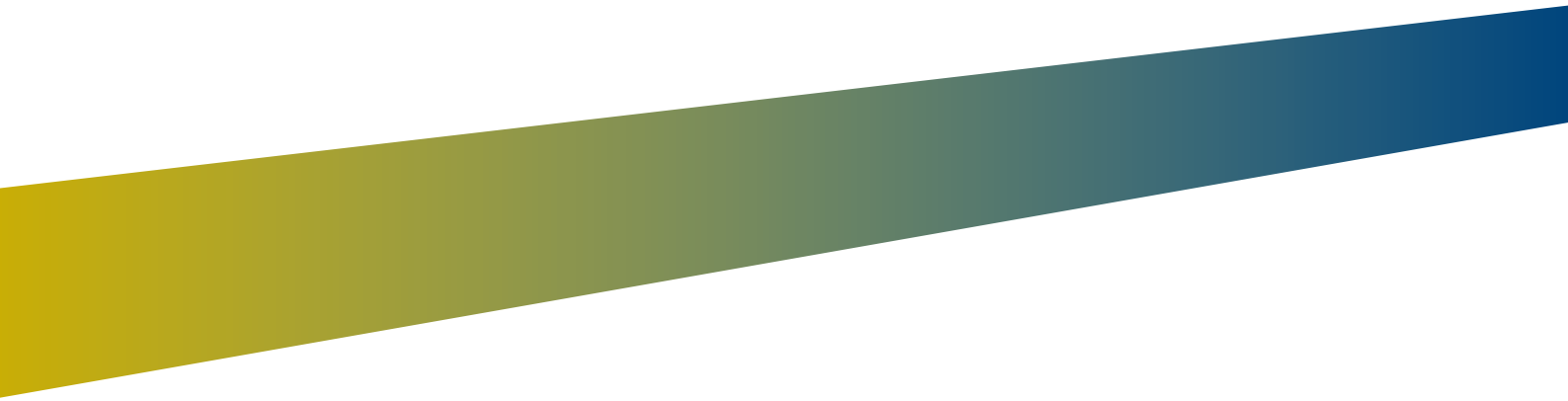
Subscription:
eucrim is published four times per year and distributed electronically for free.
In order to receive issues of the periodical on a regular basis, please write an e-mail to:
eucrim-subscribe@mpicc.de.
For cancellations of the subscription, please write an e-mail to:
eucrim-unsubscribe@mpicc.de.

For further information, please contact:

Dr. Els De Busser
Max Planck Institute for Foreign and International Criminal Law
Guenterstalstrasse 73,
79100 Freiburg i.Br./Germany

Tel: +49(0)761-7081-227 or +49(0)761-7081-0 (central unit)
Fax: +49(0)761-7081-294
E-mail: e.busser@mpicc.de

The European Criminal Law Association is a network of lawyers' associations dealing with European criminal law and the protection of financial interests of the EU. The aim of this cooperation between academics and practitioners is to develop a European criminal law which both respects civil liberties and at the same time protects European citizens and the European institutions effectively. Joint seminars, joint research projects and annual meetings of the associations' presidents are organised to achieve this aim.



Max-Planck-Institut
für ausländisches und
internationales Strafrecht