eucrim
2013 / 1
THE EUROPEAN CRIMINAL LAW ASSOCIATIONS' FORUM

Focus: Information and Data Protection
Dossier particulier: Information et protection des données
Schwerpunktthema: Information und Datenschutz

2013/1 ISSUE / ÉDITION / AUSGABE

Contents

News*

European Union

Council of Europe

Articles

Information and Data Protection

* 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.

Guest Editorial

Dear Readers,

If the protection of personal data was ever regarded as a somewhat strange subject for specialists only, this is no longer the case for three main reasons. The growing impact of information technology in all fields of life has had the effect that not only citizens but also all kinds of professionals are confronted with issues of personal data protection, whether they like it or not. At the same time, these issues are becoming increasingly global, either linked to the growing use of services available on the Internet by individuals, companies, or governments and becoming increasingly personal, as mobile devices enable or sometimes even require us to always be online and connected, whether we like it or not.

This explains why Art. 8 of the Charter of Fundamental Rights contains a separate provision on the protection of personal data. It is also the reason why the Lisbon Treaty not only made the Charter binding for EU institutions and bodies, and for the Member States acting within the scope of Union law, but also introduced a general provision in Art. 16 TFEU mandating the European Parliament and the Council to adopt rules on the protection of personal data. In this way, it was ensured that EU legal frameworks would be fully up to date and up to speed in order to face the challenges of our modern world.

The impact of this new legal environment can now be seen on different levels. First, the European Parliament and the Council are in the midst of intense deliberations on the Commission proposals for a General Data Protection Regulation and a Directive on data protection in the area of criminal law enforcement. It is possible that – as intended – this will lead to a modernised legal framework by the spring of 2014, with legal effect from 2016. It is desirable that these rules are indeed adopted with the widest possible coverage and horizontal consistency in order to fully reflect the spirit of the Charter in all EU policy areas. At this stage, there is still some work ahead but a good result can be delivered in time if all stakeholders continue to work as hard as they are working now.

However, another impact is also visible. Both in the supervisory tasks of the EDPS and in our consultation on new legislation in different policy areas, we see similar influences at work. The article in this issue on data protection at OLAF illustrates the considerable attention paid to data protection in the area of anti-fraud and anti-corruption, but also how this can be practiced as a strategic tool to ensure a fair and lawful process in an area where far-reaching consequences are at stake on both sides of the matter. In fact, although OLAF developed within the scope of Community law, it has also operated at an interface with criminal law and in cooperation with EU bodies active in this field. Both the need for and feasibility of horizontal consistency will therefore find useful evidence in OLAF's handling of data protection.

Peter Hustinx

Since 2005, about 40 percent of Commission proposals analysed in EDPS opinions on new legislation were closely connected to the Area of freedom, security and justice. This continues to be an important source of input for our task of helping to ensure that the right to personal data protection is adequately reflected in all EU policies, but other areas are also becoming more prominent. One of them is the financial sector, where a series of reform proposals has highlighted issues of personal data protection, either for financial institutions from a "know your customer" perspective, or for regulators when ensuring compliance with stricter rules in a dynamic marketplace increasingly built on sensitive data concerning clients and operators alike.

This is the new reality and the context of the other articles in this issue. They all serve to underscore why the new legal framework for data protection is about ensuring greater effectiveness and more horizontal consistency.

Peter Hustinx
European Data Protection Supervisor

European Union*

Reported by Dr. Els De Busser (EDB), and Cornelia Riehle (CR)

Foundations

EU's Accession to the ECHR

At the JHA Council of 6-7 December 2012, the Cyprus Presidency reported on progress regarding the EU's accession to the ECHR. The Commission is the EU's negotiator while the Council's Working Party on Fundamental Rights, Citizens' Rights and Free Movement of Persons was appointed as a special committee to be involved in the debates.

Parallel to the accession negotiations, more technical rules are discussed in the report covering specific aspects of the accession. The Presidency examined elements of the internal rules, which the EU will have to adopt as a consequence of this accession in order to regulate its participation in proceedings before the ECtHR. The exact formulation and choice of a legal instrument for the issues that need to be set out will be discussed once the Commission comes forward with a formal proposal. (EDB)

➤eucrim ID=1301001

* If not stated otherwise, the news reported in the following sections cover the period December 2012 – March 2013.

Enlargement of the EU

Progress for Several Countries

At the General Affairs Council of 11 December 2012, Commissioner for Enlargement and Neighbourhood Policy Štefan Füle made positive conclusions as to the recent enlargement progress of several countries.

The launch of the new agenda for the accession talks with Turkey (see eucrim 2/2012, p. 50) resulted in progress regarding, for instance, visa policy. Issues of fundamental rights and the relations with Cyprus still remain open, but the accession process could get back on track this way.

Also, discussions with the Former Yugoslavian Republic of Macedonia are moving in a positive direction. Progress was achieved with assistance from the High Level Accession Dialogue on the legislative framework for elections, freedom of expression, and public administration. After the Council adopted conclusions on this progress, the Commission also announced making €56 million available to support reforms in the former Yugoslav Republic of Macedonia that are key to its EU accession process: in the justice system, the economy, the agricultural sector, and the environment. The Commission plans to open the accession negotiations in the summer of 2013.

Serbia is developing a new strategy on judicial reform and adopting a new anti-corruption strategy and action plan. This progress is welcomed by the Council and the Commission, but one of the main unresolved points is still Serbia's relations with Kosovo. If the Commission presents a positive assessment on this progress in spring 2013, accession negotiations could be opened soon.

For Kosovo's part, the Council also urges the normalisation of relations with Serbia. Furthermore, Kosovo has a prospect to open negotiations on a Stabilisation and Association Agreement in 2013 once it has met the short-term priorities identified in a planned feasibility study.

Albania's status of candidate country is still subject to completion of key measures in the areas of judicial and public administration reform as well as revision of the parliamentary rules of procedure. Particular attention should be paid *inter alia* to the following:

- Conducting elections in line with European and international standards;
- Strengthening the independence, efficiency, and accountability of judicial institutions;
- Determined efforts in the fight against corruption and organised crime, including proactive investigations and prosecution in view of developing a solid track record.

With regard to Bosnia and Herzegovina, a key priority for the country's accession to the EU is to bring its Constitution in line with the ECHR. The Stabilisation

and Association Agreement will not enter into force before this has been completed.

Montenegro had its second Accession Conference on 18 December 2012. The first negotiation chapter on science and research was opened and provisionally closed on 11 January 2013. The analytical examination has started for two key chapters: judiciary and fundamental rights as well as justice, freedom and security.

Negotiations with Iceland are entering a decisive phase. On 11 January 2013, 27 negotiation chapters had been opened, of which 11 chapters have already been provisionally closed. This is out of a total of 35 chapters for negotiation. (EDB)
➤eucrim ID=1301002

Institutions

Council of the EU

JHA Priorities of the Irish Presidency

From January till June 2013, Ireland holds the Presidency of the Council of the EU. Its priorities in several areas were presented to the EP committees in the week of 21-25 January.

In the area of justice and home affairs, the Irish Presidency will focus on making progress in a few key areas such as data protection reform, the asylum package, and the Schengen accession of Bulgaria and Romania. In addition, the pending legal instruments on passenger name records, the confiscation of proceeds of crime, seasonal workers, intra-corporate transferees, and the right of access to a lawyer are topics where the Irish Presidency wants to make significant headway during the coming months. (EDB)
➤eucrim ID=1301003

Commission

Commission Should Give Access to Documents on UK's Opt-Out from Charter

On 17 December 2012, the European Ombudsman decided on a complaint that was lodged in 2008 by the NGO European Citizen Action Service (ECAS). ECAS had requested access to documents drafted by the Commission concerning the opt-out that the UK made from the Charter of Fundamental Rights. The request related to five documents, two of which ECAS was granted partial access to but three of which remained undisclosed. The Commission had based the decision to grant only partial access on the exception to public access concerning the protection of legal advice and on the exception concerning the protection of the decision-making process.

Upon inspection of all documents, the European Ombudsman concluded that these arguments were not convincing and recommended that the Commission consider granting public access to the documents in question as this is "key to winning the trust of European citizens."

The Commission argued that only parts of the documents were relevant for the complainant's request, which made the Commission grant access to specific parts of two of the previously undisclosed documents. ECAS then requested a definitive decision from the Ombudsman on the matter. This led to the final assessment of the Ombudsman and the conclusion that by wrongfully refusing to provide public access to documents concerning the UK opt-out from the Charter of Fundamental Rights and by failing to give valid reasons for doing so, the Commission breached the Charter. In view of the importance of the documents for the rights of EU citizens, and the fact that the Commission failed to react constructively to the Ombudsman's detailed analysis, he concluded that this constitutes a serious instance of maladministration. (EDB)
➤eucrim ID=1301004

Commission Issues New Guidelines on Staff Whistle-Blowing

On 6 December 2012, the Commission presented new guidelines on whistle-blowing obligations that elaborate on the existing guidelines adopted in 2004. Even though it is considered a key tool in the fight against irregularities, OLAF statistics show there are only about five cases per year on average. Nonetheless, irregularities are reported without reference to the whistle-blowing rules.

The guidelines contain new provisions, e.g., the possibility for staff to choose from several reporting channels, as a last resort even reporting to another EU institution; no tolerance of retaliation against whistle-blowers; and disciplinary consequences for malicious whistle-blowing. (EDB)
➤eucrim ID=1301005

OLAF

Council Approves OLAF Reform

On 4 December 2012, the Council approved the agreement reached with the EP on the reform of OLAF aimed at strengthening its capacity to combat fraud.

The reform includes improvements to make OLAF more efficient, e.g., extending the right to immediate and unannounced access to information held by institutions, bodies, offices, or agencies in the stages prior to the investigation in order to assess whether there are reasons to start it. Cooperation possibilities with Eurojust, Europol, and third state's authorities are improved as well as the exchange of views with the EP, Council, and Commission. Finally, accountability is enhanced by focusing on the procedural rights of persons affected by an OLAF investigation.

Now that political agreement has been reached, the next step in the procedure is for the Council to adopt its position before the text goes back to the EP for a second reading. (EDB)
➤eucrim ID=1301006

OLAF Signs Memorandum of Understanding with European Communities Trade Mark Association

On 7 December 2012, OLAF Director General Giovanni Kessler and President of the European Communities Trade

Mark Association (ECTA) Domenico De Simone signed a memorandum of understanding. This document constitutes a framework of cooperation on combating trade in counterfeit goods.

This is the first memorandum of understanding that OLAF has signed with a private entity since the expansion of OLAF's investigative capacities to combat fraud related to counterfeit goods. (EDB)
➤eucrim ID=1301007

Europol

Football Match-Fixing Network Uncovered

From July 2011 until January 2013, Europol, together with Germany, Finland, Hungary, Austria, and Slovenia, formed a Joint Investigation Team (JIT) codenamed "Operation VETO" to uncover an extensive criminal network involved in widespread football match-fixing. The team was supported by Eurojust, Interpol, and investigators from eight other European countries.

Operation VETO discovered a total of 425 match officials, club officials, players, and serious criminals from more than 15 countries who were suspected of being involved in attempts to fix more than 380 professional football matches, including qualification matches of the World Cup and European Championship as well as two matches of the UEFA Champions League. In addition, another 300 suspicious matches were identified mainly in Africa, Asia, South America, and Central America.

Operation VETO revealed a sophisticated organised criminal operation, which generated over €8 million in betting profits and involved over €2 million in corrupt payments to those involved in the matches. (CR)
➤eucrim ID=1301008

Smuggling and Illegal Immigration – Organised Criminal Network Dismantled

On 6 February 2013, a joint operation conducted between judicial and law enforcement authorities from Belgium, France, and the UK, supported and coordinated by Eurojust and Europol, dismantled an organised criminal network involved in smuggling and illegal immigration. The network illegally transported Middle Eastern nationals via Turkey, Greece, France, and Belgium into the UK. Europol deployed a mobile office to France for on-the-spot intelligence analysis. Furthermore, an Operational Coordination Centre (OCC) was set up at Eurojust and run by Eurojust's French, Belgian, and UK desks with the assistance of the Eurojust Case Analysis Unit. (CR)
➤eucrim ID=1301009

Global Seizures of Fake and Substandard Food

From 3-9 December 2012, the joint Interpol-Europol "Operation Opson II" that was conducted by customs, police, and national food regulatory bodies and partners from the private sector of 29 countries worldwide resulted in the seizure of more than 135 tonnes of potentially harmful goods. The goods ranged from everyday products, such as coffee, soup cubes, and olive oil to luxury goods such as truffles and caviar. Another 100 tones of misdeclared and/or potentially hazardous food was confiscated during investigations linked to Operation Opson II. (CR)
➤eucrim ID=1301010

People Smuggling Dismantled

On 29 January 2013, Europol supported and coordinated a joint action against persons smuggling between 10 Euro-

Common abbreviations

CBRN	Chemical, Biological, Radiological, and Nuclear
CCJE	Consultative Council of European Judges
CDPC	European Committee on Crime Problems
CEPEJ	European Commission on the Efficiency of Justice
CEPOL	European Police College
CFT	Combating the Financing of Terrorism
CJEU	Court of Justice of the European Union
CONT	Committee on Budgetary Control
COREPER	Committee of Permanent Representatives
DG	Directorate General
EAW	European Arrest Warrant
ECHR	European Convention of Human Rights
ECJ	European Court of Justice (one of the 3 courts of the CJEU)
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EIO	European Investigation Order
(M)EP	(Members of the) European Parliament
EPO	European Protection Order
EPPO	European Public Prosecutor Office
FATF	Financial Action Task Force
FT	Financing of Terror
GRECO	Group of States against Corruption
GRETA	Group of Experts on Action against Trafficking in Human Beings
JHA	Justice and Home Affairs
JIT	Joint Investigation Team
JSB	Joint Supervisory Body
LIBE Committee	Committee on Civil Liberties, Justice and Home Affairs
(A)ML	Anti-Money Laundering
MONEYVAL	Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism
OSCE	Organisation for Security and Cooperation in Europe
SIS	Schengen Information System
SitCen	Joint Situation Centre
TFEU	Treaty on the Functioning of the European Union

pean countries and EULEX (European Union Rule of Law Mission in Kosovo).

With the support of more than 1200 police officers, 103 persons suspected of being involved in the smuggling of illegal migrants from, into, and within the European Union, mainly via Turkey and the Western Balkan region, were arrested. The illegal migrants were mainly from Afghanistan, Iraq, Pakistan, Syria, and Turkey. (CR)

➤eucrim ID=1301011

Cross-border Action at 28 European Airports

At the beginning of December 2012, Europol and Airpol supported a joint cross-border action carried out by law enforcement authorities from 15 countries and covering 28 European airports. The action resulted in the arrest of 10 suspected couriers and the seizure of illicit cash shipments worth €1.25 million as well as cannabis and 4 kg of synthetic drugs.

Airpol is a permanent and multidisciplinary cooperation network of police services, border guards, and other relevant law enforcement services active in and around airports with the mission of contributing substantially to increasing security in the airports of the EU Member States and the Schengen-associated States. Airpol was set up by a Council Resolution of 2-3 December 2010. (CR)

➤eucrim ID=1301012

European Financial Coalition against Commercial Sexual Exploitation of Children (EFC) Launched

On 26 November 2012, EU Commissioner for Home Affairs, Cecilia Malmström, and Director of Europol, Rob Wainwright, announced the launch of a new European Financial Coalition against Commercial Sexual Exploitation of Children Online (EFC). This 36-month project, which is co-financed by the European Commission, takes action via the payment and ICT systems that are used to run these illegal operations. The EFC has the following five main objectives:

- To support international law enforcement investigations, wherever possible through cooperation with private stakeholders;
- To assess and study commercial child sexual exploitation on the Internet carried out through all kinds of Internet environments, e.g., hosting services, newsgroups, etc.
- To help protect legitimate private business interests from possible misuse of their services by criminals with the aim of distributing child sexual abuse content through various information and communication technologies;
- To empower law enforcement and private companies to counteract the problem through the delivery of training and sharing of resources;
- To inform decision makers and raise awareness among the public about the EFC's activities.

The chair of the new EFC is held by Europol. The EFC's Secretariat is hosted by Missing Children Europe and led by a Steering Committee composed of representatives of Inhope, MasterCard, Visa Europe, PayPal, Microsoft, Google, Eurojust, the KLPD (Dutch national police force), and the International Center for Missing and Exploited Children (ICMEC).

Missing Children Europe is a European Federation for Missing and Sexually Exploited Children based in Brussels, representing 28 NGOs active in 19 EU Member States and Switzerland. (CR)

➤eucrim ID=1301013

Eurojust

New National Member for Romania

On 13 December 2012, Daniela Buruiană was appointed new National Member for Romania at Eurojust.

Before joining Eurojust, Ms. Buruiană worked as a prosecutor at different levels within the Romanian Prosecution Service for 14 years. During the past eight years, she has worked within the Prosecutor's Office attached to the High Court of Cassation and Justice-Directorate for Investigating Organised Crime and Terrorism.

Ms. Buruiană succeeds Ms. Elena Dinu, Eurojust's first National Member for Romania, who left Eurojust in December 2012. (CR)

➤eucrim ID=1301014

New National Member for Spain

On 4 December 2012, Mr. Francisco Jiménez-Villarejo was appointed National Member for Spain at Eurojust.

Mr. Jiménez-Villarejo has 13 years of experience in the Spanish prosecution service, his last position being in the General Prosecution Offices of Malaga, specialising in international cooperation and corruption cases. Furthermore, he was a professor of criminal and procedural law at the police academies of Andalusia and Majorca and in the Public Law Department of the Universidad de las Islas Baleares. (CR)

➤eucrim ID=1301015

Specific Areas of Crime / Substantive Criminal Law

Tax Fraud

Directive on Mutual Assistance in the Field of Direct Taxation Enters into Force

On 1 January 2013, Directive 2011/16/EU on administrative cooperation in the field of taxation entered into force (see also eucrim 1/2011, p. 7). This directive repeals Directive 77/799/EEC and introduces new rules on cooperation between Member States on collecting taxes that are due.

A key feature of these new rules is the end of the traditional bank secrecy. Member States' authorities can no longer refuse to deliver information to another Member State based on the fact that it is information held by a bank. The directive covers all forms of taxes except

those that fall within the scope of more specific EU legal instruments, e.g., VAT. (EDB)
➤eucrim ID=1301016

New Action Plan and Recommendations on Tax Evasion and Avoidance

On 6 December 2012, the Commission presented an action plan for a more effective EU response to tax evasion and avoidance. It was accompanied by two recommendations on specific issues.

The action plan contains measures on the short, medium and long terms. Among the measures put forward are an EU tax identification number and common guidelines to trace money flows. The first recommendation focuses on tax havens or third states that do not meet minimum standards of good governance in tax matters. The second recommendation deals with aggressive tax planning or an artificial arrangement or series of arrangements put into place for the essential purpose of avoiding taxation and leading to a tax benefit.

In order to monitor the implementation of the action plan, scoreboards and other new monitoring tools will be set up. To foster implementation of the recommendations, a Platform for Tax Good Governance will report on Member States' efforts. (EDB)
➤eucrim ID=1301017

Protection of Financial Interests

Proposed Directive on Protection of Financial Interests by Criminal Law – State of Play

The JHA Council of 6-7 December 2012 was informed of the discussions on the Commission proposal for a directive on the fight against fraud to the EU's financial interests by means of criminal law (see eucrim 3/2012, p. 98). The proposal aims to improve the prosecution and sanctioning of crimes against the EU budget by developing common definitions and by facilitating the recovery of misused funds.

During the discussions, a question was raised by some Member States regarding the legal basis of the proposal. The majority of Member States claimed that it should be Article 83(2) TFEU instead of Article 325(4) TFEU as proposed by the Commission. The Council therefore requested its preparatory bodies to clarify this issue before continuing the debate. (EDB)
➤eucrim ID=1301018

Money Laundering

Fourth Anti-Money Laundering Directive Released

On 5 February 2013, Commissioner for Internal Market and Services Michel Barnier presented two proposals adopted by the Commission to reinforce the EU's existing rules on anti-money laundering and fund transfers:

- A directive on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing;
- A regulation on information accompanying transfers of funds to secure "due traceability" of these transfers.

Both proposals are seen as providing for a more targeted and focused risk-based approach as well as reinforcing the sanctioning powers of the competent authorities.

The aforementioned directive is the long-awaited fourth money laundering directive. This proposed directive improves the rules on customer due diligence, aiming for companies to have a better knowledge of their customers and their customer's businesses. The provisions dealing with politically exposed persons now also include persons such as heads of state or government members residing in EU Member States. Cooperation between the Financial Intelligence Units is also strengthened in the proposed text.

An important new feature of the proposed directive is its widened scope. The directive will apply to natural and legal persons trading in goods to the extent that payments are made or received in cash for an amount of €7,500 or more. This is a lower threshold than the one included in the third money laundering directive, which is currently still applicable. The third directive used the €15,000 threshold required by the Financial Action Task Force.

The proposed regulation is a revision of the provisions of Regulation (EC) No. 1781/2006 regarding information on the payer accompanying transfers of funds, and it will replace this regulation after its adoption. The new proposal lays down rules for payment service providers to send information on the payer throughout the payment chain for the purposes of prevention, investigation, and detection of money laundering and terrorist financing. Enhancing the traceability of payments is carried out *inter alia* by requiring information on the payee and by requiring verification of the identity of the beneficiary with regard to payments originating outside the EU for any amount higher than €1000. Additionally, effective mechanisms should be established in accordance with the regulation in order to encourage reporting of breaches of its provisions.

Both proposals will be dealt with by the ordinary legislative procedure. (EDB)
➤eucrim ID=1301019

Implementation of Anti-Money Laundering and Counter-Terrorism Financing Rules for Electronic Money

On 7 December 2012, the Joint Committee of the European Supervisory Authorities (European Banking Authority, European Securities and Markets Authority, and European Insurance and Occupational Pensions Authority) published a report on the implementation of AML/CTF requirements for e-money issuers, agents, and distributors in Europe.

The report gives an overview of the implementation efforts by the Member States and highlights where differences

in national legislation could affect the integrity of the EU legal framework on AML/CTF.

The Joint Committee also formulates recommendations for the Commission to take action towards improving the current legal framework. (EDB)

➤eucrim ID=1301020

Anti-Money Laundering Reporting Obligations for Lawyers Not Disproportionate

On 6 December 2012, the ECtHR ruled in the case of *Michaud v. France* on the obligation for French lawyers to report suspicious transactions of their clients. The central question is whether this obligation disproportionately interferes with confidential lawyer-client relations and thus breaches Art. 8 ECHR.

Several directives have been adopted in the fight against money laundering. Among these is Directive 2005/60/EC or the "third money laundering directive," which introduces reporting obligations for several professions regarding suspicious money transfers. The French implementation legislation required lawyers to report their suspicions to the president of the Bar of the Conseil d'Etat and the Court of Cassation or to the president of the Bar of which they are members. The report is then transmitted to the national financial intelligence unit Tracfin. When the National Bar Council decided that lawyers must put in place internal procedures in view of possible declarations of suspicion, the complainant took to the Conseil d'Etat, arguing an infringement of professional privilege and the confidentiality of lawyer-client relations as protected by Art. 8 ECHR. His request to have the case transferred to the ECJ for a preliminary ruling was rejected and his complaint was dismissed. The Conseil d'Etat did not see a disproportionate infringement of Art. 8 given the public interest in the fight against money laundering and the fact that the information received by lawyers does not fall within the scope of the reporting obligation.

The complainant brought the case before the ECtHR, relying in particular on Art. 8. The Court focused on the proportionality of the privacy infringement and ruled that there was no violation of Art. 8 for two reasons. First, in accordance with the applicable French legislation, lawyers are only obliged to report their suspicions when they take part in transactions for, or on behalf of their clients or act as trustees and when they assist in preparing or carrying out certain transactions. Second, lawyers do not have to report their suspicions directly to Tracfin but to the president of the Bar of the Conseil d'Etat and the Court of Cassation or to the president of the Bar of which they are members. The ECtHR decided on these grounds that there was no disproportionate infringement of Art. 8 ECHR. (EDB)

➤eucrim ID=1301021

Report

Towards the European Public Prosecutor's Office (EPPO)

Institutional and Practical Aspects

ERA, Trier, 17-18 January 2013

This seminar, organised by the ERA with the financial support of the European Commission, OLAF (under the Hercule II Programme), was dedicated to the topic of the European Public Prosecutor's Office (EPPO).

It analysed the institutional and practical aspects of establishing the EPPO. Issues of substantive and procedural criminal law were examined, together with the legal status and possible internal organisation of the new office. It also debated the future relations of the EPPO with all the other relevant bodies involved in cooperation in criminal matters in the EU such as Eurojust, OLAF, and Europol.

After an introductory session (European Commission, Eurojust, and OLAF), the first morning session was dedicated to an overview of prosecution experiences in Member States where the financial interests of the European Union are at stake. In the afternoon, the EPPO was presented from a much wider perspective. Panellists discussed democratic control of the acts of the EPPO, the use of evidence in the EPPO's proceedings, procedural safeguards and the human rights dimension, the status of the EPPO in prosecution services in EU Member States, judicial control of the acts of the EPPO and its powers.

The seminar was designed as a "discussion forum," in which EU policy-makers could consult EU legal practitioners on their real needs and views. To this end, at least 45 minutes were dedicated to the discussion with the audience after each session.

The audience consisted mainly of EU lawyers, prosecutors, judges, and anti-fraud investigators. All in all, the conference brought together approximately 110 legal practitioners and experts, some of them from the national associations for the protection of the financial interests of the European Union.

Different views, various national needs, and quite a lot of concerns were expressed regarding the establishment of the EPPO. The European Commission said that these opinions will be taken into account, also in light of the "EPPO impact assessment" to be published in Spring 2013 (the impact assessment had not yet been published at the time the ERA seminar was held).

The seminar was held in English, German, and French.

Laviero Buono, Head of European Criminal Law Section, ERA

Counterfeiting & Piracy

Stronger Criminal Law Protection of Euro Currency

On 5 February 2013, the Commission presented a proposal for a directive on the protection of the euro and other currencies against counterfeiting by criminal law. After its adoption, this directive shall replace Framework Decision 2000/383/JHA. The proposal is a joint initiative of Vice-President Viviane Reding, Vice-President Olli Rehn, and Commissioner Algirdas Šemeta, and it aims to strengthen cross-border investigations. It also introduces minimum penalties, including imprisonment of up to eight years for the most serious counterfeiting offences.

A new feature in the proposal is the obligation for judicial authorities

Making the Fight against Corruption in the EU More Effective

Towards the Development of New Evaluation Mechanisms

St. Julians (Malta), 16-17 May 2013

In 2011, the European Commission adopted the so-called "anti-corruption package," a set of measures to more vigorously address the serious harm generated by corruption at economic, social, and political levels. One year later, in March 2012, the new proposal for a directive on freezing and confiscation was published.

The conference will discuss these recent EU policy developments and legislative reforms. It will also present the results of a study commissioned by OLAF (to be published in March-April 2013) that is aimed at collecting information and developing methodologies to assist both the Commission and Member States' authorities with the implementation of the new EU anti-corruption policies.

The study is intended to provide tools, which may feed into the general anti-corruption review mechanism, improve the application of public procurement rules, and promote implementation of the Commission's anti-fraud strategy in the Member States.

Presentations will be made by national, European, and international experts. The role and contribution of OLAF will be outlined and concrete international and European cases presented.

Key topics are

- Recent European initiatives and major challenges in the fight against corruption;
- Assisting Member States' authorities with the implementation of the new EU anti-corruption policies;
- Developing a comprehensive methodology to measure the real costs of corruption in selected sectors of the economy;
- Criminalising active and passive corruption carried out in the course of business activities.

Who should attend? Judges, prosecutors, national government officials, lawyers in private practice, and policy-makers.

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

to transmit to laboratories samples of seized counterfeit currency for technical analysis, also during criminal proceedings, for the purpose of detecting further counterfeits in circulation. (EDB)

➤eucrim ID=1301022

Organised Crime

Annual Report on Implementation of Counter-Terrorism Strategy

During the JHA Council of 6-7 December 2012, the EU counter-terrorism coordinator presented his annual implementation report on the EU counter-terrorism strategy. This report gives an overview of the results for the four components of the strategy (prevent, protect, pursue, and respond) and lists the areas in which measures should be taken.

With regard to the element of prevention, the counter-terrorism coordinator points out that the Cyprus Presidency revised the EU Strategy on Radicalisation and Recruitment, which had been approved by the Council in October 2012. Part of this strategy is the Check the Web programme, which is supported by Europol. In the context of this programme, a web portal was set up with wide access to Member States' experts in Islamist propaganda on the Internet. The report also pays attention to several national initiatives, especially in the field of training to deal with lone actor terrorism and radicalisation.

The protection component can be served by continuing improving border management, protecting critical infrastructures, enhancing aviation and transport security as well as making budgets available for security-related research.

As regards the element of pursuit, passenger name records and financial messaging data continue to be important tools in the prevention of terrorist attacks.

Ultimately, with regard to response, the new Crisis Coordination Arrangements defining rules for interactions between EU institutions and affected states in cases of internal or external crisis are under preparation. The counter-terrorism coordinator also lists other important steps taken in counter-terrorism work outside the EU, e.g., the Global Counter-Terrorism Forum that has working groups focusing on the Horn of Africa and on the Sahel. The EU Counter-Terrorism Strategy was adopted by the Council in December 2005 and provides the framework for EU activity in this field. (EDB)

➤eucrim ID=1301023

Market Abuse Directive – General Approach Approved by Council

During the JHA Council of 6-7 December 2012, a general approach towards the proposal for a directive on criminal sanctions for insider dealing and market manipulation was agreed upon (see also eucrim 4/2012, p. 148).

Ireland has decided to take part in the adoption of the directive. The UK and Denmark will not participate. The text will be discussed in the EP plenary in June 2013. (EDB)

➤eucrim ID=1301024

New Project Fights Trafficking in Human Beings at EU Borders

On 18 February 2013, the Commission presented the launch of a new project to fight organised crime and trafficking in human beings at the external borders of the EU. The project is part of the EU Strategy towards the Eradication of Trafficking in Human Beings 2012-2016, which was adopted by the Commission 19 June 2012 (see eucrim 3/2012, pp. 100-101).

The €1.5 million project focuses on trafficking in Azerbaijan, Bosnia-Herzegovina, Moldova, and Turkey. It in-

volves data sharing as well as training law enforcement authorities to deal with this type of crime more effectively. It also promotes regional cooperation and coordination with regard to human trafficking.

The first phase of the project was launched at the beginning of 2013. A second phase is expected in mid-2014 in order to consolidate project results. In addition, the scope will be broadened by adding more countries and addressing not only law enforcement but also assistance and protection of victims. (EDB)
➤eucrim ID=1301025

Report on EU Drug Markets

On 31 January 2013, the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) and Europol released their first joint EU drug markets report. The two EU agencies have joined forces to provide the first strategic analysis of the entire illicit drug market in Europe.

The report concludes that the contemporary illicit drug market is dynamic, innovative, and quickly adapts to new circumstances. Thus, the approach towards combating this market should be equally dynamic and innovative.

Globalisation and the use of more countries for production, storage, and transit of drugs, together with the prominent role that the Internet plays, are important factors.

The report contains case studies as well as action points dealing with intelligence gathering and analysis, tracing money flows and partnerships within the legitimate markets. (EDB)
➤eucrim ID=1301026

Cybercrime

EU Cyber Security Strategy Released

On 7 February 2013, the European Commission and the High Representative of the EU for Foreign Affairs and Security Policy presented a joint communication on the EU Cyber Security Strategy. This was accompanied by a proposed directive on network and information security.

Prevention and response to cyber disruptions and attacks is the core objective of the strategy. The EU's perspective on the strategy falls into five priorities:

- Achieving cyber resilience;
- Drastically reducing cybercrime;
- Developing cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP);
- Developing the industrial and technological resources for cyber-security;
- Establishing a coherent international cyberspace policy and promoting core EU values.

The proposed directive is a key element of the strategy requiring Member States, Internet providers, social networks, and all other relevant operators, e.g., health care services and banks, to ensure a secure and trustworthy digital environment. (EDB)
➤eucrim ID=1301027

ENISA Publishes Critical Cloud Computing Report and Threat Landscape Report

On 14 February 2013, the European Network and Information Security Agency (ENISA) released a report that analyzes cloud computing from a Critical Information Infrastructure Protection (CIIP) perspective. Based on a survey of public sources, a number of scenarios involving cloud computing, large cyber attacks, and disruptions of cloud computing services, were studied. This study resulted in a list of recommendations on cyber security governance at a national level, including risk assessment, security measures, and incident reporting.

In the Threat Landscape Report, published on 8 January 2013, ENISA analyzed over 120 recent reports from public sources to identify the current top cyber threats. Cyber threats were also compared with information from the past few years in order to identify emerging threats in the areas of mobile computing, social technology, critical infrastructures, trust infrastructures, cloud computing, and big data. (EDB)
➤eucrim ID=1301028

ENISA's Mandate Extended

On 1 February 2013, the Council and the EP reached agreement on extending the mandate of ENISA seven years. The proposed regulation that provides for this extension dates from 2010 and also includes other items.

ENISA was set up in 2004 with the task of ensuring a high level of network and information security across the EU. Since then, challenges with respect to information security have changed a lot and the threat of large-scale cyber attacks has increased. Therefore, it was considered necessary to revise and extend ENISA's mandate.

ENISA's tasks have been outlined in more detail, another branch was established in Athens besides the head office in Heraklion/Greece, and an executive board will be installed to prepare administrative and budgetary decisions to be taken by the management board. Furthermore, the proposed regulation has been brought in line with the common approach to decentralised EU agencies of 12 June 2012 (see eucrim 3/2012, p. 90). (EDB)
➤eucrim ID=1301029

Sexual Violence

EU-US Global Alliance against Child Sexual Abuse Online

On 5 December 2012, the Global Alliance against Child Sexual Abuse Online was launched. This is a joint EU-US initiative and part of the EU-US Working Group on cyber security and cybercrime, where the fight against child online abuse has been identified as a key priority.

At the time of the launch, 48 states had already expressed their willingness to participate. Government leaders of these states will be requested to commit to a set of policy targets and operational goals. hey would then decide on the specific actions to take to achieve these goals. A monitoring mechanism will be set up to follow up on their implementation. (EDB)
➤eucrim ID=1301030

Procedural Criminal Law

Data Protection

Data Protection Reform – State of Play

The JHA Council of 6-7 December 2012 discussed the progress made on reform of the data protection legal framework by the Cyprus Presidency (see eucrim 4/2012, pp. 150-151). The debate has been increasingly focusing on issues in the proposed general data protection regulation than the proposed directive on data protection in criminal matters. The Cyprus Presidency shared the Member States' opinion that more clarity should be achieved on the proposed general data protection regulation before deciding upon new data protection rules for the law enforcement sector in the proposed directive. Nevertheless, the Presidency continued with the examination of the proposed directive.

With regard to the proposed regulation, three issues are considered particularly important. First, at several points in the proposed regulation, the Commission is given the power to adopt delegated and implementing acts. This means that the Commission can adopt new rules regarding non-essential elements of a legislative instrument. This could, for instance, concern technical details. A majority of the Member States is opposed to this. Thus, the Commission clarified that these acts should only be understood as a tool of last resort, in case all other tools for a harmonised approach fail. Alternatives were introduced into the debate, such as guidelines or best practices formulated by the proposed European Data Protection Board. In order not to speculate on parts of the proposed regulation that still need to be discussed, the alternatives were not further dealt with before the first complete reading of the text is finalised.

Second, the administrative burdens and costs of compliance with the proposed regulation were included in the Commission's Impact Assessment, but several Member States do not agree with this assessment. There is, however, consensus among Member States that making an exception to data protection rules that have expensive consequences for small and medium enterprises is not an optimal solution in all cases. An approach based on the risk inherent in specific data processing operations met with general agreement.

Third, a number of Member States supports the opinion that the proposed regulation needs to provide more flexibility in the public sector, in order to allow adequate leeway for domestic processing by national authorities. Since this question is connected to the legal form of the instrument, it was agreed that this matter also needs to be discussed after a complete discussion on the text has been finalised.

The Council agreed to these three points of discussion. (EDB)

➤eucrim ID=1301031

EDPS Work Programme 2013

The EDPS presented his 2013 work programme on 18 January 2013. Besides the current debate on the reform of the data protection legal framework of the EU, four other key priorities dominate the EDPS' consultation agenda for 2013:

- Technological developments and the Digital Agenda;
- Further developing the Area of Freedom, Security and Justice;
- Financial sector reform;
- eHealth.

Additionally, consultations could be considered regarding data protection in other policy areas, e.g., competition and trade. (EDB)

➤eucrim ID=1301032

EDPS Strategy 2013–2014 for Excellence in Data Protection

On 22 January 2013, the EDPS presented its Strategy 2013-2014 for Excellence in Data Protection.

Following a strategic review launched by the EDPS in July 2011 and after consulting their stakeholders, priorities were identified and an action plan was developed in response to the increasing workload and broader scope of activities that the EDPS will face in the coming years. The current reform of the EU data protection legal framework, the Lisbon Treaty, and the expanding exchange of information as well as the increased sophistication of the technology used pose new challenges for data protection as such. With a set of objectives and key performance indicators, the EDPS has a clear strategy for maximising his resources as well as his efficiency. (EDB)

➤eucrim ID=1301033

Second Joint Review of the TFTP Agreement

The EU-US Agreement on the exchange of financial messaging data for the Terrorist Finance Tracking Programme (TFTP Agreement) entered into force on 1 August 2010 (see eucrim 3/2010, p. 94) and has already been the subject of a first joint EU-US review of its implementation (see eucrim 2/2011, pp. 63-64).

The second joint review was carried out for the period from 1 February 2011 to 30 September 2012. The overall conclusion was that the TFTP respects the safeguards included in the agreement and that the recommendations of the first review have been followed up to a large extent. One issue that was highlighted and requires further monitoring is the requirement to delete data older than five years.

The report also mentioned examples of cases in which the TFTP and the data gathered for it have proven their added value. The next joint review is planned for 2014. (EDB)

➤eucrim ID=1301034

Freezing of Assets

General Approach on Proposed Directive on Freezing and Confiscation of Proceeds of Crime

The Council endorsed the general approach on the proposed directive on freezing and confiscating proceeds of

crime (see also eucrim 4/2012, p. 151). An introductory note demonstrates that the text is the result of a compromise and should be seen as a package. For instance, the non-conviction based confiscation, which is new for several Member States, was limited to two specific circumstances. Flexibility was also introduced regarding the national procedures used to achieve confiscation objectives in those circumstances, be it through *in absentia* or non-conviction based proceedings.

Ireland notified the Council that it wishes to take part in the adoption and application of the proposed directive. The UK and Denmark decided not to participate.

The EU Fundamental Rights Agency (FRA) published its opinion on the proposed directive on 4 December 2012. In its opinion, the FRA evaluates the provisions of the text in the light of the EU Charter of Fundamental Rights and that of international human rights standards. (EDB)

➤eucrim ID=1301035

Cooperation

Police Cooperation

Commission Communication on EU Information Exchange

Under the Stockholm Programme, the European Commission was asked to assess the need for a European Information Exchange Model based on an evaluation of existing instruments. To meet this request, on 12 December 2012, the European Commission published a Communication to the European Parliament and Council, taking stock of how cross-border information exchange in the EU works today and making recommendations on how to improve it.

The instruments and main channels used in cross-border cooperation exchange as analysed by the Communication include, amongst others, the Swedish Initiative, the Prüm Decisions, Europol, the Schengen Information System, the European Border Surveillance System (EUROSUR), and information exchange via SIRENE, Interpol, and between Europol and its National Units.

In its conclusions, the Communication found that, at this stage, no new law enforcement databases or information exchange instruments were needed at the EU level, since current problems result instead from insufficient implementation of existing instruments and the inconsistent organisation of exchange. Hence, the Communication makes the following recommendations;

- Improving the use of existing instruments, streamlining and managing the channels, in order to ensure data quality, security, and protection;
- Improving training and awareness;
- Introducing new funding possibilities

as well as more comprehensive statistics. (CR)

➤eucrim ID=1301036

Implementation of the Prüm Decisions

On 26 November 2012, the Irish Presidency sent a report on the state of implementation of the provisions of the Prüm Decisions to the Working Group on Information Exchange and Data Protection (DAPIX). Member States had to comply with all provisions by 26 August 2011. In detail, the report lists those Member States that have made declarations to the Council regarding the following:

Report

Choice of Forum in Cooperation Against EU Financial Crime

Freedom, Security and Justice & the Protection of Specific EU Interests

Utrecht, the Netherlands, 19 and 20 April 2012

The conference addressed the central question of whether or not a revised conceptual framework is needed for choice of forum. The current system does not adequately prevent positive and negative conflicts of jurisdiction. The conference aimed to define the interests at stake and to establish the legal parameters within which choice of forum should take place. It dealt with three issues:

- To what extent are discretionary powers of the Member States, prosecuting authorities in particular, a problem in choice of forum?
- If discretionary powers are indeed a problem, who is to take action?
- If action is to be taken, what direction should it take?

Renowned speakers discussed the institutional framework for choice of forum and current daily practice. They also explored the potential of new concepts like European territoriality and European citizenship. The conference was attended by 67 experts from 17 countries, including representatives of 14 associations.

Conference results are:

a) The adverse consequences of the current system were widely recognized. There is a need to categorically include the interests of the EU and EU citizens into the debate;

b) The foundations for and limits to different models of forum choice were explored in light of the specifics of the European legal order, including fundamental rights;

c) From there on, various speakers offered the European legislator new perspectives for a new model for choice of forum.

The conference was organized by the Utrecht University, together with DASEC (the Dutch law association for the study of the protection of the financial interests of the EU) and co-financed by the European Commission (OLAF) under the Hercule II Programme and the Netherlands Organisation for Scientific Research (NWO) under the Innovational Research Incentives Scheme.

For further information, see: M. Luchtman (ed.), Choice of forum in cooperation against EU financial crime: freedom, security and justice & the protection of specific EU-interests, The Hague: Boom/Lemma 2013.

Dr. Michiel Luchtman, Utrecht University, m.luchtman@uu.nl

- Contact points for the automated searching of DNA profiles, dactyloscopic data, and vehicle registration data (VRD);
- Contact points for the exchange of information on major events and to prevent terrorist offences;
- Data protection authorities.

Furthermore, the report indicates which Member States have declared their national DNA analysis files and maximum search capacities for dactyloscopic data and which ones have notified the Council of their readiness to apply the decisions and of their compliance with data protection requirements.

Additionally, on 7 December 2012, the Commission published a report on the implementation of the Prüm Decision (Council Decision 2008/615/JHA) and reflecting on the main difficulties in the operation of this instrument. The report finds that, as of 12 October 2012, only 18 Member States were ready for the automated search of DNA data. 14 Member States were ready for searches in their automated fingerprint identification systems by other Member States, and 13 Member States were operational in the area of VRD. According to the report, the reasons for the delay include technical difficulties and problems with financing. Hence, the Commission recommends that Member States experiencing serious delays to make better use of existing possibilities such as funding under the Commission programmes, the Mobile Competence Team (MCT), and the helpdesk at Europol. With regard to running the instrument and possible improvements short of legal amendments, the Commission also recommends taking the work of the MCT and the Europol helpdesk into consideration. As meaningful statistics are seen as the best way to assess the added value of the Prüm Decisions, Member States are invited to consider options to improve the current models for statistics. Finally, the establishment of procedures to follow up matches between data sets (also called hits) should be enforced. (CR)

➤eucrim ID=1301037

Joint Customs and Police Operation "Athena III"

Between 16 and 22 October 2012, 26 EU Member States, together with Croatia, the Former Yugoslav Republic of Macedonia, Iceland, Montenegro, Serbia, Norway, Morocco, and Switzerland, as well as OLAF, TAXUD, Europol, INTERPOL and the World Customs Organization (WCO), participated in the joint customs and police operation "Athena III." The operation was targeted at cash couriering and the violation of EU and Member States' laws on the declaration and transportation of large amounts of cash. Operation Athena III revealed more than €9 million that had not been declared, and more than €120 million were declared in the course of the operation. Furthermore, over 196 other goods, such as semiprecious stones and jewels, were seized during the operation. (CR)

➤eucrim ID=1301038

Council of Europe*

Reported by Dr. András Csúri

Foundations

Reform of the European Court of Human Rights

Court Issues Annual Table of Violations and Survey of Activities

At the annual press conference of the ECtHR on 24 January 2013, President Spielmann looked back at 2012 in a positive manner. The review underlined that, for the first time since 1998, the Court reduced the backlog of its pending cases, largely due to the adoption of new working methods and the optimum exploitation of the single judge procedure introduced by Protocol No. 14 (see eucrim 3/2012, p. 106; 3/2011, p. 116; 4/2009, pp. 147-148 and 1/2009, pp. 25-26). At the same time, the number of applications disposed of had increased, which opened up the perspective to bring the inflow and backlog of inadmissible cases under control within two to three years.

The president stressed again the importance of the effective implementation of Convention standards at the national level and the full implementation of the ECtHR judgements emphasised at the high-level conference on the future of the Court held in Brighton in 2012 (see also eucrim 3/2012, p. 106)

The courts annual activity report and the statistics for 2012 were issued at the press conference and revealed that the states with the highest number of judgements having at least one violation of the Convention delivered against them were Russia, Turkey, and Romania.

In further news, some of the factsheets of the ECtHR were translated into Turkish and published on 15 February 2013, with further translations to follow. (For news on factsheets, see also eucrim

* If not stated otherwise, the news reported in the following sections cover the period December 2012 – March 2013.

4/2011, p. 151; 1/2011, p. 19 and 4/2010, p. 148. For translation-related news, see eucrim 3/2012, p. 106, 2/2012, p. 61 and 4/2012, p. 152).
➤eucrim ID=1301039

Specific Areas of Crime

Corruption

GRECO : Fourth Round Evaluation Report on Estonia

On 8 January 2013, GRECO published its fourth round evaluation report on Estonia, which focuses on the prevention of corruption of Members of Parliament, judges, and prosecutors. The report strengthened Estonia's position as one of today's least corrupt countries in Europe. The legal framework in the field is satisfactory. Deficiencies were stressed as to the absence of insufficient definition of ethical principles, the lack of practical guidance regarding the acceptance of gifts, and the weak supervision of rules for conflicts of interest. GRECO made a total of 19 recommendations; amongst others calling for the extension of the regulations on conflicts of interest to Members of Parliament and to consider introducing a periodical assessment of the professional performance of judges.
➤eucrim ID=1301040

GRECO: Fourth Round Evaluation Report on Poland

On 26 January 2013, GRECO published its fourth round evaluation report on Poland.

The report acknowledges Poland's solid legal framework in the field, especially the quite strict regulations regarding incompatibilities, accessory activities, and mandatory asset declarations. The reports states, however, that professionals often lack a clear understanding what conduct is expected of them and what is meant by conflict of interest. Further, the ethical principles seemed too general to provide guidance in certain specific situations. Therefore, GRECO made a total of 16 recommendations; inter alia the need to refine the ethical standards and to offer special trainings and confidential counselling for professionals in the field.
➤eucrim ID=1301041

Legislation

GRETA First Assessment Reports on Malta, France, Latvia, and Portugal

In January and February 2013, GRETA published first assessment reports in regard to Malta, France, Latvia, and Portugal. These reports assess the extent to which the CoE Convention on Action against Trafficking in Human Beings' provisions have been put into practice by the respective authorities. The common weak spots identified in these reports were the often underestimated figures of THB and the lack of focus on labour exploitation. The possibly erroneous figures were explained by the lack of formal procedures to identify victims and the linking of identification with the participation in investigation.

The report on Malta was published on 24 January 2013. It commended the progress made in developing legal and institutional frameworks for combating THB, including the adoption of a national action plan and the setting up of a Human Trafficking Monitoring Committee. However, GRETA believes that the figures do not show the real situation in the field and criticised that most of the cases launched since 2006 are still pending. Therefore, GRETA urges improving identification procedures and ensuring prompt and effective investigations and prosecution.

The report on France was published on 28 January 2013. It called upon the authorities to launch a coordinated national anti-trafficking action plan and to set up a nationwide referral mechanism to identify victims of trafficking. Both the need to focus on labour exploitation and the necessary dissociation of the victims' access to support and their willingness to cooperate were stressed by the report.

The report on Latvia was published on 31 January 2013. Latvia is a country of origin for THB, primarily for sexual exploitation and is in need of a better system for identifying victims. The report praised the national anti-trafficking programmes, the creation of national coordinator and inter-institutional working groups as well as the allocation of resources to help victims. However, as the majority of the investigations do not lead to successful trials, the report emphasised the need to strengthen investigation and prosecution procedures.

The report on Portugal was published on 12 February 2013. It highlighted the need to improve the identification of victims and the prosecution of traffickers. The report welcomed the setting up of a multi-disciplinary team for the identification of victims of THB but stressed that it lacks the capacity to intervene. GRETA recommended not to let the access to support depend on the victims' willingness to cooperate and to increase the detection of trafficking for the purpose of labour exploitation.
➤eucrim ID=1301042

Data Protection at OLAF

Laraine Laudati*

The European Anti-Fraud Office (OLAF) is charged with protecting the EU's financial interests by investigating fraud, corruption, and other illegal activities. OLAF's daily work involves the processing of large amounts of sensitive[1] personal data. As a service of the European Commission, OLAF is subject to Regulation (EC) 45/2001 on the protection of individuals with regard to the processing of personal data by Community institutions and bodies (data protection regulation) and is thus under the supervisory powers of the European Data Protection Supervisor (EDPS). OLAF conducts administrative investigations in full independence, both internally – concerning the EU institutions and bodies – and externally – concerning economic operators located in the Member States and third countries. In order to help protect its independence when conducting investigations, OLAF is the only service of the European Commission that has appointed its own Data Protection Officer (DPO); the Commission has appointed one DPO for all of the other services combined.

Investigations are handled by approximately 130 OLAF investigators and other case handlers who have widely different backgrounds and whose home Member States have varying traditions with respect to the processing of personal data. OLAF, with the help of its partner authorities, must gather evidence that may be located in Member States and third countries and it must thus exchange personal data with those authorities in the course of its investigations. Its final reports and recommendations, which contain personal data, are often sent to prosecutors and judicial authorities in the Member States who pursue criminal charges for the fraud that is the subject of the OLAF investigation. Accordingly, OLAF operates in a highly complex environment in which the demands of the data protection regulation touch the work of its investigators on a daily basis. OLAF is fully committed to fulfilling these demands.

The key players in an OLAF investigation (persons concerned, informants, whistle-blowers, and witnesses) are "data subjects" who have rights under the data protection regulation, which OLAF must respect. These include the rights of information about their data being processed and of access to such data. If they believe the processing of their data is illegal, they also have the right to object as well as rights of rectification, blocking, and erasure of their data.

This article shall describe how OLAF complies with data protection requirements in performing its investigative function. It begins by explaining OLAF's notification of its personal data processing operations to its DPO and its "prior checking" of the sensitive processing operations with the EDPS. The elements of the OLAF data protection "toolbox" which has been created to assist OLAF investigators ensure that they perform their daily tasks in full compliance with the requirements are next described. The challenges OLAF has faced in relation to transferring personal data to its partner Member State authorities and third country authorities are then considered. It will be shown that, through the continuous efforts of OLAF and the practical approach of the EDPS geared towards finding workable solutions, Regulation (EC) 45/2001 has proven sufficiently flexible in allowing OLAF to achieve compliance without undue administrative burden.

I. OLAF's Notifications and Prior Checks

The data protection regulation requires that the controller (defined as the organizational entity that determines the purposes and means of a processing operation) give prior notice to the DPO of any personal data processing operation for which it is responsible. The DPO is charged with maintaining a public register of all such notifications. OLAF's register is available on its "Europa" website.[2] It contains approximately seventy notifications of processing operations currently underway at OLAF.

The regulation requires that processing operations "likely to present specific risks," as defined therein, are subject to prior checking by the EDPS. Approximately half of OLAF's processing operations have been subject to prior checking, mainly because they relate to one of the specific risks listed, that is, "to suspected offences, offences, criminal convictions or security measures" and/or that they are "intended to evaluate personal aspects relating to the data subject, including his or her ability, efficiency and conduct." The EDPS has issued prior checking opinions for these processing operations, all of which may be seen at the OLAF Europa website.[3] These opinions all contain recommendations that OLAF has implemented or, for a few of them, that are still in the process of being implemented. OLAF reports back to the EDPS on which steps it has taken to im-

plement the recommendations, and once the EDPS is satisfied with the implementation, he closes the prior checking case.

The recommendations of the EDPS in his prior checking opinions have had an important influence on how OLAF observes data protection requirements. Through exchanges and discussions with the EDPS, OLAF has resolved key issues of how to apply the data protection regulation in the context of its investigations. For instance, OLAF initially had difficulty interpreting the "information" requirement, that is, the requirement that all data subjects receive certain information specified in the regulation. Given that case files contain the names of many persons, a large number of whom may have no relevance to the investigation, it would be an excessive burden for OLAF personally to inform all such persons, with no benefit to them. A practical solution was found with the EDPS: to provide a personalized privacy statement only to the key players in an investigation (persons concerned, informants, whistle-blowers, and witnesses). The non-relevant data subjects could access OLAF's privacy statements on the OLAF Europa website. This application of the information requirement to data subjects whose data is in OLAF case files has allowed OLAF to implement the requirement in a practical and feasible manner.

II. The OLAF Investigator's Data Protection Toolbox

Three elements have been developed to help OLAF's investigators comply with data protection requirements in their daily work: OLAF Instructions to Staff on Data Protection, OLAF workforms, and the OLAF Data Protection Module.

1. OLAF Instructions to Staff on Data Protection

The OLAF Instructions to Staff on Data Protection for Investigative Activities (ISDP) were adopted by the Director General in April 2013, replacing data protection guidelines that had originally been adopted in 2006.[4] The new instructions specify in practical terms what the investigator must do to satisfy data protection requirements in all aspects of his/her work. The main sections of the ISDP are: Definitions, Data Quality, Information to the Data Subject, Other Rights of the Data Subject, Transfers and Complaints. The ISDP implements many of the recommendations of the EDPS included in his prior checking opinions on OLAF investigations, his inspection reports, and his decisions on complaints made by data subjects against OLAF. The data quality requirements specify that any personal data gathered must be adequate, relevant, and not excessive in relation to the purpose of the processing concerned, which must be analyzed on a case-by-case basis.

The ISDP defines "relevant data subjects" in an OLAF investigation as "natural persons who have relevance for an OLAF case, including: persons concerned, informants, whistleblowers and witnesses, as well as natural persons who are, exceptionally, named in a recommendation of an OLAF coordination case to a national judicial authority." As stated above, any data subject fitting this definition must receive a personalized privacy statement in the course of the investigation.

The requirements for making transfers of personal data to other EU institutions/bodies, Member State authorities, and third country authorities and international organizations are specified. The instructions set forth the procedures to be followed at OLAF when handling requests from data subjects in exercise of their rights under the regulation – the rights of access, rectification, blocking, erasure, and objection – as well as complaints by data subjects. Procedures for deferring observance of data subjects' rights, when necessary and in the observance of the legal requirements of the regulation, are also set forth.

Finally, the instructions spell out exactly what the investigator must record in the Data Protection Module.

2. OLAF Workforms

OLAF workform templates have been developed, which investigators must use in carrying out the various steps of an investigation. OLAF has incorporated the concept of "privacy by design" in these workforms by including in the template any necessary data protection paragraphs. More specifically, any workform designed to be sent or otherwise provided to a relevant data subject contains a "privacy statement," including all of the information which the data protection regulation obliges the controller to provide to the data subject. Any workform designed to be sent outside of OLAF to any recipient other than a data subject, and which may contain personal data, includes a "transfer clause," specifying what use the recipient can make of the data and indicating how the data should be handled. Different transfer clauses are required, depending on the type of recipient – an EU institution or body, a Member State authority, or a third country authority or international organization – which reflect the differing requirements for each of them under the data protection regulation. Accordingly, by using the official OLAF workform to prepare case-related documents, the investigator automatically meets the requirements of providing a privacy statement to relevant data subjects and of including a transfer clause in its correspondence that contains personal data.

3. OLAF Data Protection Module

The electronic case files for all OLAF cases are stored in the Case Management System (CMS). A Data Protection Module (DPM) has been created within the CMS and is used to store information about compliance with all data protection requirements for each relevant data subject in each OLAF case. Investigators must list the names of all relevant data subjects when a case is open. As soon as a privacy statement has been provided to a relevant data subject, this must be recorded in the module. If a data subject submits a request for access, rectification, blocking or erasure, or an objection, the request and all OLAF responses must be recorded in the DPM. If OLAF must defer provision of a privacy statement or a reply to a request, the deferral must be recorded in the DPM, thereby making it easy to monitor deferrals and ensuring that the privacy statement or other information or responses are eventually provided once the reason for the deferral no longer exists. Complaints from data subjects and their replies are also stored in the DPM. OLAF's management, its DPO, and the EDPS can also use the DPM to gain an overview of the state of OLAF's compliance with data protection requirements in its case files.

III. OLAF's Transfers of Personal Data

OLAF may transfer personal data to EU institutions/bodies, Member State authorities, third country authorities and international organizations during the course of an investigation or upon its completion. During the investigation, it may be necessary to transfer a name and other personal information in order to request assistance from a partner authority or to reply to a request for assistance or otherwise assist a partner by, for example, sending interview records or mission reports. After an investigation is closed, it may be necessary to transfer personal data included in a final report when OLAF issues recommendations to be implemented by the recipient authority. The categories of data that may be transferred include identification data, professional data, and case involvement data (data relating to the allegations and/or facts concerning matters under investigation by OLAF).

Articles 7, 8, and 9 of Regulation (EC) 45/2001 govern transfers of personal data to EU institutions/bodies, Member State authorities, and third country authorities/international organizations, respectively. Under Article 7, a transfer within or between EU institutions/bodies can be made, if necessary, for the performance of a task covered by the competence of the recipient. Under Article 8, a transfer to a Member State authority can be made, *inter alia*, if the data are necessary for the performance of a task carried out in the public interest or subject to the exercise of public authority. Under Article 9, a transfer to a third country authority or international organization is possible if an "adequate level of protection" is ensured in the country of the recipient or within the recipient international organization and if the data are transferred solely to allow tasks covered by the competence of the recipient to be carried out. If the recipient does not have an adequate level of protection, then it would be possible, exceptionally, to make a transfer by way of derogation if, *inter alia*, the transfer is necessary or legally required on important public interest grounds or for the establishment, exercise, or defense of legal claims. However, if systematic transfers are to be made to a third country authority or international organization that does not have an adequate level of protection, then the EDPS may authorize a set of transfers where the controller adduces adequate safeguards, e.g. through data protection clauses, for protection of the data subject's rights.

EDPS prior checking opinions relating to OLAF investigations have emphasized that, for transfers under Articles 7 and 8 of Regulation (EC) 45/2001, notice has to be given to the recipient in order to inform him/her that personal data can only be processed for the purposes for which they were transmitted. He also emphasized that even if a transfer of information is foreseen in other relevant legislation, the transfer is only lawful if it also meets the requirements established in the data protection regulation. Further, he recommended that an analysis of the necessity of the transfer has to be carried out *in concreto* on a case-by-case basis, that the proportionality factor must be taken into account, and that a note to the file should be made specifying the need for the transfer.

For transfers under Article 9, Article 25(6) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995[5] provides that the Commission may find that a third country ensures an adequate level of protection by means of domestic law or international commitments as regards protection of private lives, basic freedoms, and individual rights.[6] However, OLAF must transfer data to authorities in a number of countries where the Commission has not yet concluded that an adequate level of protection exists. Thus, in 2005, it initiated a consultation with the EDPS on how it could make such third country transfers while respecting data protection requirements. The EDPS concluded, in a 2006 decision, that OLAF would need adequate safeguards in a specific legal framework for "repeated, mass or structural" transfers, which could be included in memoranda of understanding with OLAF's partners. For occasional transfers, OLAF could rely on the exception mentioned above, but this could not be relied upon for systematic use because it would not ensure that the rights of the data subject are protected.

OLAF thereafter developed a first model Administrative Cooperation Arrangement (ACA), with an annex containing data protection clauses designed to provide adequate safeguards.

In December 2006, the EDPS indicated that the data protection clauses provided a good basis for moving forward in addressing the need for adequate safeguards. In 2010, OLAF undertook the simplification of the data protection clauses and submitted a revised version to the EDPS. The revised data protection clauses include definitions, joint obligations, OLAF obligations, partner obligations, resolution of disputes, and suspension and termination clauses. Following extensive discussions with the EDPS on the revised clauses, the EDPS made recommendations in letters dated 3 April 2012[7] and 16 July 2012[8] and OLAF has implemented those recommendations. The EDPS is expected to react on the final version of the model data protection clauses in the near future. On the basis of these clauses, several new ACAs have been concluded.[9]

Conclusion

This article has presented an overview of how OLAF has implemented data protection requirements in the context of its investigations. Notwithstanding the enormity of the task of ensuring that each relevant data subject's rights are observed in the course of each OLAF investigation – by the approximately 130 investigators and other case handlers from all EU Member States – OLAF has, through good collaboration with the EDPS, found practical solutions. Through its use of "privacy by design" in its workform templates, its DPM, and its ISDP as well as the data protection training of its staff, OLAF has developed a system which ensures observance of the rights of the many data subjects whose personal data it processes during its investigations.

* The views expressed are purely those of the author and may not under any circumstances be regarded as stating an official position of the European Commission.

1 The data is sensitive because it may include allegations and facts concerning the possible involvement of individuals in matters under investigation by OLAF. This is to be distinguished from "special categories of data" within the meaning of Article 10 of Regulation (EC) 45/2001, which is sometimes referred to as sensitive data.

2 "Europa" is the public website of the European Union. OLAF's register may be viewed at the following URL within the Europa website: http://ec.europa.eu/anti_fraud/dataprotectionofficer//register/index.cfm?TargetURL=D_REGISTER

3 The EDPS' opinions concerning OLAF's prior checks may be viewed at the following URL: http://ec.europa.eu/anti_fraud/about-us/data-protection/processing-operations/prior_checking_en.htm.

4 The ISDP may be viewed at the following URL: http://ec.europa.eu/anti_fraud/about-us/data-protection/index_en.htm.

5 O.J. L 281, 23.11.1995, p. 31.

6 To date, the Commission has made adequacy findings for the following: Andorra, Argentina, Canada, Eastern Republic of Uruguay, Faeroe Islands, Guernsey, Isle of Mann, Israel, Jersey, New Zealand, Switzerland, and the PNR and Safe Harbour provisions for the USA.

7 The letter is published on the EDPS website: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Priorchecks/Opinions/2012/12-04-03%20Model%20Data%20Protection%20Clauses_OLAF_D-746_EN.pdf.

Laraine Laudati
OLAF Data Protection Officer

8 This letter analyses the data protection clauses under Article 9(6) of Regulation 45/2001, and not for an authorisation for massive or structural transfers under Article 9(7). The letter states that OLAF should notify the EDPS in cases where the transfers become massive or structural, to request an authorisation under Article 9(7). See the EDPS website: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Priorchecks/Opinions/2012/12-07-16Model%20Data%20Protection%20Clauses_OLAF_D-1051_EN.pdf.

9 A list of all ACAs that OLAF has entered into can been viewed at: http://ec.europa.eu/anti_fraud/documents/international-cooperation/aca_third_countries_and_dp_annex_en.pdf.

The Data Protection Gap

From Private Databases to Criminal Files

Dr. Els De Busser

Debates on the reform of the EU's data protection legal framework are currently being held in the Council of the EU and the European Parliament.[1] One particular issue has, however, not (yet) been included in these debates: the processing of personal data by law enforcement authorities for the purpose of criminal investigations after these data were originally collected by private companies for the purpose of their commercial activities. This topic has, however, been discussed at several

other negotiation tables. On the EU level, the Cybersecurity Strategy[2] released in February 2013 and the continuing debate on the use of passenger name record (PNR) data for the prevention, detection, investigation, and prosecution of terrorist offences[3] and serious crime as well as the controversy that surrounded the Data Retention Directive[4] demonstrate the difficult balance between the protection of personal data and the need to obtain private sector information for the purpose of investigating and prosecuting criminal offences. This debate has also been held in the context of transatlantic cooperation. The 2010 EU-US Agreement on the processing and transfer of financial messaging data for the purposes of the Terrorist Finance Tracking Programme (TFTP Agreement)[5] is one of the best examples of how private sector information is used to prevent and prosecute serious crime such as terrorism. The second EU-US joint review of the implementation of the TFTP Agreement listed several cases in which the information received from a company called SWIFT[6] – the market leader in the transmission of financial messaging data between banks worldwide – helped in tracing, identifying, and, ultimately, prosecuting persons involved in the preparation or execution of terrorist attacks.

Since the above-mentioned cases indicate that the exchange of personal data between private companies and law enforcement authorities has significant added value, it is all the more surprising to see that this form of cooperation is neither dealt with on the EU level in the proposed data protection directive nor in the proposed data protection regulation. In fact, the transfer of personal data from a private company to a law enforcement authority for the purpose of a criminal investigation or prosecution falls in the gap between both proposed legal instruments. Whereas data processing by private companies is governed by the proposed regulation, data processing by law enforcement authorities for the purposes of prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties is dealt with by the proposed directive. The question of which legal instrument should contain provisions on safeguarding data protection in this type of transfer should thus be part of the ongoing discussions in the Council and the Parliament.

This contribution will attempt to address that particular question. It is only by analysing the effect of the data transfer from private companies to law enforcement authorities on data protection principles that the question can be answered as to what the applicable legal instrument should be. For this reason, the quality and security of the personal data that are the subject of this transfer are examined here. Logically, the currently applicable legal instruments on data protection will be considered as well as the pending reform proposals.

The proposed directive will not be applicable to Europol. However, Europol plays a key role in the EU's law enforcement cooperation and has experience in dealing with data transfers from private companies. Its rules on data processing can function as an inspiration for the proposed EU legal instruments on data protection. For this reason, this contribution will also include the analysis of data transfers involving Europol.

I. Data Processing Standards

Directive 95/46/EC is applicable to the processing of personal data wholly or partly by automated means. It is equally applicable to the processing of personal data other than by automated means which are part of a filing system or are intended to become part of a filing system in the course of an activity that falls within the scope of Union law. Processing of personal data for the purpose of commercial activities is thus included in the scope of Directive 95/46/EC. The proposed regulation does not change this scope. Framework Decision 2008/977/JHA is applicable to the transmitting of personal data that a Member State receives from another Member State for the purpose of the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties. The proposed directive expands its scope to include also domestically gathered personal data.

No legal instrument adopted on the EU level lays down standards on personal data transfers from private companies to law enforcement authorities in general, although for specific types of companies legal instruments exist.[7] With two applicable legal instruments in the area of data protection at the moment and two new and revised legal instruments pending, the question is where to include provisions on these transfers. For answering this question, the precise nature of this transfer should be defined. The currently applicable legal instruments do not contain a definition of transfers from private companies to law enforcement authorities. It is certainly not "processing under the authority of the controller and processor"[8] since there is no reporting or supervision between both parties. It can also not be qualified as "processing on behalf of a controller"[9] because that would mean that the law enforcement authority would be processing the data for a commercial purpose or vice versa. It is also not a transfer to a third state or international organisation. Obviously, it could constitute a transfer to a third state's law enforcement authority but it can also be a transfer within the EU or even within one Member State.

Because both the company and the law enforcement authority are data controllers but both process the data for the performance of different activities unrelated to each other, the transfer of personal data from a company to a law enforcement authority should be defined as a transfer from a data controller to another data controller where the purpose of the data process-

ing changes from a commercial purpose to that of a criminal investigation or prosecution.

The data protection principles that are the basis of the aforementioned legal instruments are enshrined in the 1981 CoE Data Protection Convention. Even though this convention is also being modernized at present, the basic principles of data protection still remain the same. Nonetheless, it should be analysed how these principles are or could be affected when a transfer of data from private companies to law enforcement authorities is concerned.

1. Degrees of Accuracy and Reliability

Directive 95/46/EC and Framework Decision 2008/977/JHA both state that the data controller must ensure that personal data are accurate and, where necessary, kept up to date. The proposed directive made this provision more precise by explicitly making it the competent authority's responsibility as a data controller to adopt policies and implement appropriate measures to ensure that the processing of personal data is performed in compliance with the provisions adopted pursuant to the directive. This includes the right to rectification of inaccurate or incomplete data and the right to deletion. More importantly, in accordance with the proposed directive, law enforcement authorities are also obliged to indicate the degree of accuracy and reliability of the personal data they process. When personal data are transferred from a private company that is a data controller to a law enforcement authority, which then becomes the data controller, the accuracy of the data should be safeguarded. The personal data as such can be accurate but that does not make the assessments or conclusions drawn from them accurate. When a person buys several litres of artificial fertiliser needed for his vegetable farm and, shortly after, buys a timer for a sprinkler system in his backyard, the data regarding these purchases may be correct, but one of the conclusions that can be drawn from these purchases could be that this person is producing explosives in his home. A "new"[10] provision in the proposed directive obliges law enforcement authorities to distinguish different degrees of accuracy and reliability when processing different categories of personal data: in particular, the distinction between personal data based on facts, on the one hand, and personal data based on personal assessments, on the other hand. The provision is not entirely new as it is a copy of principle 3 of CoE Recommendation (87)15 regulating the use of personal data in the police sector.

In its own rules on analysis work files, Europol has included the stipulation that data stored in these files for analysis purposes shall be distinguished according to the assessment grading of the source and the degree of accuracy or reliability of the information. This means that data based on facts are distinguished from data based on opinions or personal assessments.[11] Information is evaluated by Europol using a 4x4 system that awards a code to the source of the information and a code to the information itself. Based on these codes, decisions are made regarding the accuracy of the information or the reliability of the source.[12] The responsibility for data processed at Europol, particularly as regards transmission to Europol and the input of data, as well as their accuracy and their up-to-date nature, lies with the Member State that has communicated the data. However, with respect to data communicated to Europol by third parties, including data communicated by private parties, this responsibility lies with Europol.[13]

Where the quality of personal data that law enforcement authorities (including Europol) have received from private entities is concerned, the currently applicable rules do not provide for the necessary safeguards. However, as long as the provision on distinguishing degrees of accuracy and reliability survives the negotiations on the proposed directive, it is not necessary to provide for further rules on ensuring the quality of data transferred from private entities to law enforcement authorities.

2. Processing for Compatible Purpose and Necessity

Personal data can be processed for legitimate purposes only and should not be processed for purposes incompatible with the purpose they were collected for. Processing for a compatible purpose is allowed but a definition of a compatible purpose has not been developed yet. The concept could be defined as having "functional equivalence" or similarity to the original purpose. Additionally, the data subject should be able to reasonably foresee[14] the processing of his data for that purpose.[15] Functional equivalence means that both purposes have a large degree of similarity, e.g., a pharmacist's database contains personal data on patients' purchases of specific medication as well as their contact data. Using these data to advise the patient on the dosage of his medication would be a functionally equivalent and foreseeable, and thus compatible, purpose. Giving access to this database to labour inspectors visiting pharmacies in order to verify that all their employees are registered would not be a compatible purpose. In order to process personal data for incompatible purposes the legality and necessity requirement should be fulfilled. This includes the cases where personal data are collected for commercial purposes and afterwards processed for the purpose of a criminal investigation or prosecution.

The traditional purpose limitation principle is included in Directive 95/46/EC as well as in the proposed regulation. Derogating from the principle is allowed when this is necessary to safeguard the prevention, investigation, detection, and prosecution of criminal offences. What it really means is that

no mass transfer of personal data is allowed. It is essential to maintain the nexus between the data that are transferred by a law enforcement authority and the criminal investigation or prosecution that they should be processed for. For example, when the pharmacist in the aforementioned example is under investigation for selling a counterfeit cancer drug, searching his database for all patients who had bought this particular cancer drug during a specific period of time would be an allowed derogation from the purpose limitation principle, because there is a clear nexus between the personal data and the ongoing investigation. If a pharmacist would be requested to give a law enforcement authority access to his database to "comb" through it, however, such a nexus would not exist.

Mass transfers of data were one of the problems with respect to first version of the 2010 TFTP Agreement that was rejected by the European Parliament. The second version included a new role for Europol. Article 4 of the agreement gives Europol the power to give binding force to the requests from the UST. Europol was thus put in the unexpected position as the authority that decides upon the legitimacy of the requests to obtain data from a private company. Since the entry into force of the agreement Europol verifies the requests formulated by the UST on three aspects. The request should identify as clearly as possible the categories of data requested, the necessity of the data should be demonstrated and the request should be tailored as narrowly as possible. The company in question, SWIFT, must wait for Europol's authorisation before carrying out the request.[16] At the moment of the first joint review of the TFTP Agreement in 2011, an inspection report by the Europol Joint Supervisory Body (JSB) concluded that the requests that had been sent made a proper verification by Europol within the terms of the agreement, impossible. The second joint review report highlighted that Europol's verification role is based on an operational assessment of the validity of the request. The reviewers concluded that Europol is best placed for deciding on the requirement of tailoring the requests as narrow as possible while enjoying a certain margin of discretion.[17] Nonetheless, the Europol JSB still has concerns regarding the amount of data being transferred since subsequent requests – that have all been positively verified by Europol – with an average of one per month essentially cover an uninterrupted time-period. Another concern expressed by the JSB is the continuing role that oral information provided by the UST to Europol plays in the verification process.[18] Therefore, in practice mass transfers of personal data are not entirely ruled out.

The proposed directive will not be applicable to Europol; yet, for transfers from private companies to the Member States' law enforcement authorities, the necessity requirement included in the proposed directive should be strengthened. The same goes for the proposed regulation. A provision should be added stipulating that the necessity requirement means that a nexus should be present between the personal data requested and the criminal investigation or prosecution for which their transfer and processing will be carried out.

II. Data Security

Data controllers are responsible for implementing appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and against all other forms of unlawful processing. The level of security should be appropriate for the risks presented by the processing and the nature of the data in question.[19] Companies that transfer personal data to law enforcement authorities should thus secure the data until the moment of transfer. Law enforcement authorities have a similar obligation of ensuring data security under Framework Decision 2008/977/JHA. The provisions are more specific, also including equipment access control, data media control, storage control, communication control, transport control, etc.

The proposed directive and the proposed regulation both introduce the obligation for the data controller to notify the supervisory authority of a personal data breach.[20] The provision states that the controller needs to document any personal data breaches, comprising the facts surrounding the breach, its effects, and the remedial action taken. If personal data are sent to law enforcement authorities that were the subject of a data breach when under the control of a company as data controller, the above-mentioned documentation should also be transferred to the law enforcement authority in question. This is not included in any of the proposed legal instruments. The purpose of this notification is not to verify compliance with the regulation but to be informed of possible manipulation of personal data that can be used in a criminal investigation or prosecution at a later stage. In view of the accuracy and reliability of personal data processed by law enforcement authorities, the fact that a security breach may have affected or disclosed these data at an earlier stage could be vital information.

Europol itself takes the necessary technical and organisational steps to ensure data security. Each Member State and Europol implement measures to ensure controls regarding data access, data media, etc. In accordance with the Europol Decision, direct contact with private companies however is not allowed. Europol may only process personal data transmitted by companies via the National Unit of the Member State under whose law the company was established, and the transfer should be in accordance with the national law of that Member State.[21] Thus, for the security of the personal data in the hands of the private company, the national law, which

needs to comply with Directive 95/46/EC and, in the future, with the proposed regulation, will be applicable.

The introduction of data breach notifications in the proposed data protection legal framework of the EU is highly important to data processing for commercial purposes and data processing for the purposes of a criminal investigation or prosecution. In view of distinguishing different degrees of accuracy and reliability, a transmission of the notification by the private company to the receiving law enforcement authority should be made mandatory.

III. Data Protection Reform Package

Now that the EU institutions are discussing the reform of the data protection legal framework, the timing is appropriate to also include clear provisions on how to organise transfers of personal data from private companies to law enforcement authorities and ensure that the data protection principles are respected. The question is whether these provisions should be incorporated in the proposed directive or in the proposed regulation. For answering this question, the scope of both legal instruments is significant.

The scope of the proposed directive is limited to the processing of personal data by law enforcement authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. The proposed regulation is defined by the processing of personal data in the course of an activity which falls within the scope of Union law. The focus of this contribution is a transfer from what is covered by the proposed regulation to what is covered by the proposed directive. This means that most of the necessary data protection provisions already exist. Only this particular transfer is not regulated yet. It would be more efficient including the lacking provisions on this type of transfer in one of the existing legal instruments than creating a fully new one.

Considering the ECJ's jurisprudence on the purpose of data processing, the element of safeguarding the internal market that was used in the case on the Data Retention Directive, could not be used in the data transfers that are discussed here.[22] The element of essential objective or the final purpose of the data processing would lead to the conclusion of regulating these transfers in the proposed directive.[23] This would be in accordance with the jurisprudence of the ECJ and it would respect the scope of the proposed directive that is limited to processing of data by law enforcement authorities. Therefore the proposed directive should include the stipulation that its provisions also apply to the personal data a Member State's law enforcement authority receives from a private company.

IV. Closing the Data Gap

No discussion has taken place on whether or not personal data collected by private companies are needed by law enforcement authorities. Without these data, investigations into many criminal offences would be unsuccessful. The question is how data protection can be guaranteed when personal data are transferred from private companies to law enforcement authorities, since both data controllers' processing activities fall within the scope of two different legal instruments. Moreover, these two legal instruments are undergoing a reform process at the present time.

For law enforcement authorities, it is crucial to have clarity on the accuracy and reliability of personal data processed for the purpose of criminal investigations and prosecutions. For this reason, it should be mandatory for the company transferring data, which were the subject of a data security breach, to inform the receiving law enforcement authority of this incident. Besides being accurate, personal data should also be proportionate in relation to the purpose they are processed for. With respect to the transfers discussed here, because the data are processed for a purpose that is incompatible with the purpose they were collected for, the necessity requirement should be fulfilled. Thus, only those data that have a clear nexus with a specific criminal investigation or prosecution should be transferred.

The necessity requirement should be explicitly added to the provisions of the proposed directive. Informing law enforcement authorities of a data breach that occurred before the data were transferred to them by private companies is the private company's obligation and should therefore be included in the proposed regulation. To rule out confusion as to which data protection rules govern the processing of personal data after a transfer from private companies to law enforcement authorities, an explicit provision should be included in the proposed directive declaring the provisions applicable to these data.

Now that the EU's legal framework on data protection is being revised, the momentum should be used to include provisions on the protection of personal data that are the subject of a transfer from a private company to a law enforcement authority.

1 Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 2012/0011(COD), 16.01.2013 and Draft Report on the proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, 2012/0010(COD), 20.12.2012.

Dr. Els De Busser
Max Planck Institute for Foreign and International Criminal Law

2 Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1 final, 07.02.2013.
3 Proposal for a Directive on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM(2011) 32 final, 02.02.2011.
4 Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, O.J. L 105, 13.04.2006, p. 54.
5 Agreement on between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, O.J. L 195, 27.07.2010, p. 5.
6 Society for Worldwide Interbank Financial Telecommunication.
7 Legal instruments such as the aforementioned Data Retention Directive and the TFTP Agreement as well as the 2012 Agreement between the EU and the US on the processing and transfer of passenger name record data (the PNR Agreement), etc.
8 Article 16 of Directive 95/46/EC (Article 27 of the proposed regulation) and Article 22 of the proposed directive.
9 Article 17 of Directive 95/46/EC (Article 26 of the proposed regulation) and Article 21 of the proposed directive.
10 This provision was included in the proposal for Framework Decision 2008/977/JHA but did not make it to the final text.
11 Council Decision on adopting the implementing rules for Europol analysis work files, O.J. L 325, 11.12.2009, p. 14.
12 Europol Information Management Booklet, File no: 2510-271. See also "Europol: '4x4' intelligence handling codes includes 'dodgy data'", Statewatch, accessed January 7, 2013, http://www.statewatch.org/news/2013 /jan/03europol-dodgy-data.htm.
13 Article 28 Europol Decision.
14 ECtHR,*The Sunday Times v. United Kingdom*, 1979, §49; *Malone v. United Kingdom*, 1984, §§67-68; *Rotaru v. Romania*, 2000, §55 and *Amman v. Switzerland*, 2000, §56.
15 *L. Bygrave,* Data protection law. Approaching its rationale, logic and limits, The Hague, Kluwer Law International, 2002, p. 340. See also *E. De Busser,* Data Protection in EU and US Criminal Cooperation, Antwerp, Maklu, 2009, p. 68.
16 Article 4 of the TFTP Agreement.
17 Report on the second joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging data from the European Union to the United States for the purposes of the TFTP, SWD(2012) 454 final, 14.12.2012, pp. 6-7.
18 Ibid., pp. 2-3.
19 Article 17 Directive 95/46/EC.
20 This notification was inspired by the personal data breach notification in Article 4(3) of e-privacy Directive 2002/58/EC.
21 Article 24 Europol Decision.
22 ECJ C-301/06, *Ireland v. Council and Parliament*, 2009.
23 ECJ C-317/04 and C-318/04, *Parliament v. Council*, 2006.

The Directive on the Right to Information

Genesis and Short Description

Steven Cras/Luca De Matteis*

On 22 May 2012, the European Parliament and the Council adopted Directive 2012/13/EU on the right to information in criminal proceedings.[1] The directive is the second measure ("measure B") in application of the Roadmap on procedural rights, which was adopted by the Council in 2009.[2]

The directive is evidence that Member States are in favour of measures enhancing the procedural rights of suspects and accused persons in criminal proceedings, contrary to what is sometimes said. Indeed, the directive provides a good example of legislation where the Council, together with the European Parliament, has taken a very much "pro-rights" approach, by establishing even more extensive and protective rights than those proposed by the European Commission.

This article describes the genesis of the directive and provides a short description of its contents.

I. Genesis

1. Roadmap, Commission Proposal, and the "Cross-Border" Issue

Following an initiative launched by the Swedish Presidency in 2009, the work in the European Union on strengthening procedural rights for suspects and accused persons in criminal proceedings has been carried out on the basis of the roadmap, which was adopted by the Council on 30 November 2009. The roadmap provides a step-by-step approach – one measure at a time – towards establishing a full catalogue of procedural rights for suspects and accused persons in criminal proceedings. After successful negotiations and adoption of the directive on measure A, concerning the right to interpretation and translation in criminal proceedings,[3] a positive mood reigned among the Member States to continue working on the roll-out of the roadmap. The Belgian Presidency, which took office in the

second semester of 2010, was very eager to begin working on measure B, concerning a directive on the right to information in criminal proceedings.

Although its services had prepared a proposal for measure B in good time, the Commission hesitated in submitting this proposal to the Council and to the European Parliament. At a certain point, the Belgian Presidency had to insist that Commissioner Reding table the proposal, in order to be able to start work on the new measure in the Council so as to allow the Presidency to achieve concrete results during its term in office.

The Commission's hesitation in submitting the proposal for measure B was apparently due to the fact that lawyers within that institution were considering whether the proposal should be limited to cross-border cases. It is recalled that Art. 82 (2) of the Treaty on the Functioning of the European Union (TFEU[4]) states that legislation should only be proposed "to the extent necessary to facilitate mutual recognition of judgments and judicial decisions and police and judicial cooperation in criminal matters *having a cross-border dimension.*" Whereas it was not an issue whether the condition of a "cross-border dimension" was fulfilled in relation to measure A, which covered the more "international" issue of interpretation and translation,[5] the issue seemed more problematic in relation to measure B. In the end, however, the Commission concluded that this measure should cover all criminal proceedings, not simply those with a cross-border dimension, and put its proposal forward on 20 July 2010.

This was certainly a correct conclusion, since it is impossible in practice to make a distinction between (purely) domestic cases and cross-border cases: in practice, it often happens that a case that starts off as a domestic case subsequently turns out to have a cross-border dimension. If in such a case, assuming that it was a purely domestic case, certain procedural rights would not have been given and it would subsequently turn out, in view of the newly "discovered" cross-border dimension of the case, that such rights should have been given from the outset, a legal minefield would be opened. It is therefore necessary to set minimum rules on procedural rights that apply without distinction in criminal proceedings in the Member States, independently of the cross-border nature of the case. It is now hoped that the issue of the cross-border dimension of procedural rights, which had also caused substantial problems during the discussion on the 2004 Commission proposal,[6] will have been definitively settled.

2. Work in the Council on the General Approach

After the Commission had submitted its proposal the Belgian Presidency immediately started work in the Council, making it a high priority for its term in office. The work was carried out by representatives of the 27 Member States in all meeting formats that are available in the Council in the field of criminal justice: by Brussels-based legal representatives meeting as JHA (Justice and Home Affairs) counsellors, by senior officials meeting in CATS,[7] by ambassadors meeting in COREPER,[8] and by the Ministers of Justice meeting in the JHA Council.

Most of the work, however, was carried out by national experts, both in the Working Party for Substantive Criminal Law ("Droipen"[9]) and in meetings of the "Friends of the Presidency". Droipen meetings are the official meetings for experts in substantive criminal law. They usually include full interpretation, which means that approximately 20 languages are available. Such meetings must be organised well in advance, and the interpretation requirement makes them rather costly. The Friends of the Presidency is a hybrid group that adapts its composition in relation to the subject matter. It is composed of at least one representative per Member State, and Member States are free to send to the meeting whomever they want.[10] The advantage of this latter group is that advice by experts is often available and that it can be convened much more flexibly than the Droipen group, since all business is conducted in English and no interpretation is required. The fact that all attendees in the Friends of the Presidency speak the same language also makes it a more informal group, which often facilitates reaching an agreement.

The experts in the Droipen and Friends of the Presidency meetings, who knew each other well from the work on measure A, successfully addressed the difficulties in the Commission proposal. In fact, while the proposal was not very extensive – it only contained 13 articles – it dealt with three particular complexities:

- First, the directive on measure B had to "predict the future" to a certain degree, since it would contain a catalogue of rights in respect of which there would be a right to information. Apart from the right to interpretation and translation (measure A), the precise contents of these rights was not yet known when measure B was discussed, since they would be decided at a later stage (e.g., measure C relating to the right of access to a lawyer and measure D relating to the right to communicate with a third person and with consular authorities). It was often said during the work in the Council, and even more so during the negotiations with the European Parliament, that it would have been much better, or at least easier, to decide on measure B when all the other measures of the roadmap had been agreed upon.
- Second, compared to measure A, measure B was mostly concerned with early information that was to be given to suspects or accused persons and thus mostly with situations typically occurring in the pre-trial phase. Given that the procedural rules of the Member States regarding the pre-trial phase differ much more from each other than the rules regarding the trial phase, it was necessary to develop more fine-tuned, tailor-made solutions.

- Third, a problem was posed by the interaction between, on the one hand, the objective of ensuring efficient conduct of criminal prosecutions (which has lead Member States to establish systems for carrying out investigations without the suspect or accused person, or any third person, being made aware thereof) and, on the other hand, the objective of providing "equality of arms" to the defence (through the proposed provisions on the right to information about the accusation and the right of access to the materials of the case).

Notwithstanding these particular complexities, on 3 December 2010, the Council reached a general approach on the text of the draft directive and agreed that negotiations with the European Parliament could be initiated on that basis.[11] If one compares the text of the Council's general approach with the text of the Commission proposal, one can see that the Council substantially improved the text on several points by clarifying the wording and by establishing more extensive and protective rights than those proposed by the Commission. This is actually quite remarkable, given that difficult compromises sometimes had to be found between the positions of the various Member States.

3. Negotiations with the European Parliament

The negotiations with the European Parliament started after its Committee on Civil Liberties, Justice and Home Affairs (LIBE) held its orientation vote on 17 March 2011. This orientation vote provided the representatives of the European Parliament with a mandate for negotiations with the Council, which were organised in "trilogue" meetings in the presence of representatives of the Commission, the latter institution acting as "honest broker."

On behalf of the European Parliament, the negotiations were led by Birgit Sippel of the S&D Group,[12] who was the rapporteur on this file. From the Council's side, the negotiations were led by the Hungarian Presidency, which held office in the first semester of 2011, and by the Polish Presidency, which held office in the second semester of 2011.

The negotiations between the Council and the European Parliament on measure B were more complicated than the negotiations on measure A. This seems to have had various reasons:

- First, the subject matter of measure B is more difficult than the subject matter of measure A. This came as no surprise, since the order of the measures in the roadmap had been decided in view of their estimated difficulty in reaching an agreement: whereas the "easier" measure (interpretation and translation) was taken care of first, the more difficult measures were put lower down the list. Measure B was therefore considered to be more difficult than measure A from the outset.
- Second, while the orientation vote of the European Parliament was clearly inspired by the text of the Council general approach on several points, it significantly departed from that text and even from the original Commission proposal on other points. The orientation vote notably contained some completely new elements as to when the rights foreseen in the draft directive would kick in, and proposed a new "internal logic" of the text. This caused noticeable difficulties in the negotiations.
- Third, during the trilogues, the rapporteur of the European Parliament often indicated that, before continuing the negotiations on a certain topic, she wished to discuss that specific topic with the shadow rapporteurs (Members of the European Parliament that follow a specific co-decision file on behalf of political groups other than that of the rapporteur). It was therefore not so easy to do "business on the spot."[13]
- Fourth and finally, the work in the Council during the negotiations with the European Parliament – e.g., on which concessions could be made to the European Parliament – was mostly carried out in meetings of the JHA counsellors. It is understandable that the Presidency decided to choose this format, because the JHA counsellors are more politically driven. However, since experts are not invited to JHA counsellors' meetings, contrary to meetings of Droipen and of the Friends of the Presidency, the specific know-how of the experts who had negotiated the Council's general approach was not available at those meetings. Some Member States felt that this made the negotiations more complicated.

Despite the complexity of the negotiations, which took up nine trilogues[14] (measure A: three trilogues), the European Parliament and the Council were able to reach a provisional agreement on the text in November 2011. After legal-linguistic revision of the text and the necessary internal arrangements in the Council and in the European Parliament, the directive was finally adopted on 22 May 2012. It was subsequently published in the Official Journal on 1 June 2012; it is to be transposed into the national legal orders by 2 June 2014.

II. Description of the Directive

1. Introduction

The directive contains two sets of provisions: those on the right to information about rights, on the one hand, and those on the right to information about the accusation and the right of access to the materials of the case, on the other.

The right to information about rights is not foreseen in the European Convention on Human Rights (ECHR). This right can, however, be inferred from the case law of the European Court of Human Rights (ECtHR) on Art. 6 ECHR, according to which the authorities should take a proactive approach towards ensur-

ing that persons facing a criminal charge are informed of their rights.[15] The importance of the right to information about rights can hardly be overestimated: it is not sufficient that suspects or accused persons have procedural rights; they should also be aware of these rights in order to be able to fully exercise them.

The right to information about the accusation ("charge"), which stems from Art. 6(3)(a) ECHR, is fundamental for a person accused of having committed a criminal offence in order to for him to be in a position to prepare his defence. The right of access to the materials of the case ("case file") stems from Art. 5(4) and Art. 6(1) ECHR, as interpreted by the ECtHR. In relation to Art. 6(1), the Court ruled that it is a fundamental aspect of the right to a fair trial that criminal proceedings should be adversarial and that there should be equality of arms between the prosecution and defence. The prosecuting authorities should disclose to the defence all material evidence in their possession for or against the accused.[16] In relation to Art. 5(4), the ECtHR stated that equality of arms is not ensured if the counsel is denied access to those documents in the investigation file that are essential to effectively challenging the lawfulness of his client's detention.[17]

In respect of both sets of provisions, the directive provides considerable added value compared to the ECHR and the case law of the ECtHR, by establishing rights in clear and precise wording in a binding, legislative instrument whose application can be effectively enforced before the European Court of Justice. On several points, the directive gives concrete meaning to the relevant provisions of the ECHR and the case law of the ECtHR; on other points, it goes beyond the ECHR and Strasbourg case law by providing new rights.

2. Art. 1 – Subject Matter

According to Art. 1, "the Directive lays down rules concerning the right to information of suspects or accused persons, relating to their rights in criminal proceedings and to the accusation against them. It also lays down rules concerning the right to information of persons subject to a European Arrest Warrant relating to their rights."

As in measure A, this directive on measure B does not give a definition of "criminal proceedings": it is again understood that this legal notion should be interpreted in the light of the case law of the ECtHR with respect to the scope of application of Art. 6 ECHR.[18] Taking this into account, the addition of the reference to the European Arrest Warrant (EAW) proceedings was necessary in view of the fact that extradition procedures do not fall within the scope of application of this Convention provision.[19]

Art. 1 stresses that the directive only gives to *suspects or accused persons* a right to be informed about the accusation, not to *requested persons* under EAW proceedings. However, when a requested person is arrested in the executing Member State, the executing judicial authorities are obliged to inform that person of the EAW and its contents, in accordance with Art. 11(1) of the Framework Decision on the EAW;[20] this normally entails that the person is informed about the reason for his arrest and hence is, at least summarily, informed about the accusation against him. When the person is subsequently surrendered to the issuing Member State on the basis of an EAW issued for the purpose of conducting a criminal prosecution, he benefits from the right to be informed about the accusation as a suspect or accused person in criminal proceedings.

It is worth noting that the Council, supported by the European Parliament, modified "charge," as used in the Commission proposal, into "accusation." Recital 14 states, however, that the term "accusation" in the directive is meant to describe the same concept as "charge" in Art. 6(1) ECHR. This cryptic modification was made since "charge" is a term that strictly refers to the common law systems and is difficult to translate with an equivalent term in civil law systems. The "charge" in common law systems is a formal act of the police at the onset of investigations; in civil law systems, it does not exist, since the object of the trial (accusation) is defined by a prosecutor (or investigating judge) at a much later stage. Therefore, Member States were afraid that if "charge" were to be interpreted in a "common law" sense (rather than in the sense of "being the subject of an ongoing criminal investigation," as used by ECtHR) the right to information would reach too far back (too early and during police proceedings). Therefore, the neutral word "accusation" was introduced, albeit with reference, in the recitals, to the ECHR and its case law.

3. Art. 2 – Scope

According to Art. 2, "the Directive applies from the time persons are made aware by the competent authorities of a Member State that they are suspected or accused of having committed a criminal offence until the conclusion of the proceedings, which is understood to mean the final determination of the question whether the suspect or accused person has committed the criminal offence, including, where applicable, sentencing and the resolution of any appeal."

It was more difficult to reach agreement on the scope of measure B than on that of measure A. This can be explained by the fact that the right to interpretation and translation, the subject matter of measure A, is normally to be applied in the context of criminal proceedings that have already been ongoing for some time, whereas the right to information, the subject matter of measure B, is often to be applied at the very start of the criminal proceedings.

The final text regarding scope in measure B, set out above, is slightly different from the corresponding text in measure A, which contained, after "made aware," the words "by official notification or otherwise."[21] The deletion of these words was apparently motivated by a desire to tighten the scope of measure B, compared to the scope of measure A. It seems however that this difference in the texts does not change the meaning and that both measures A and B have the same wide scope of application.

In this context, it may be observed that under the case law of the ECtHR, the Art. 6 rights should also apply when the suspect has learned about the investigation from a source other than a (official) communication by the investigating authorities (e.g., through a house search, through a seizure, or through the closure of a business during the investigation[22]). Since the level of protection provided by both directives should never fall below the level of protection under the ECHR,[23] as interpreted in the case law of the ECtHR,[24] they should have the same wide scope of application as the ECHR. For this reason, it may be assumed that the scope of application of measures A and B is the same.

Although all Member States could agree to the scope of the directive as it was finally formulated, one Member State[25] asked that a declaration be made stating that the scope of the directive would not constitute a precedent for future measures to be decided on the basis of the roadmap. The negotiations on this declaration were particularly difficult, since many Member States felt that the scope of the directive as agreed was satisfactory and that there should be consistency between the provisions on scope in the various measures of the roadmap. It is therefore understandable that the declaration as it was finally adopted is a typical Brussels compromise with a high level of "constructive ambiguity."[26] The vague wording of the declaration is certainly one of the reasons why it has never been referred to since its adoption.[27]

The question of whether the directive should apply not only to *natural persons* but also to *legal persons* was also discussed. Although the negotiations had clearly been conducted under the presumption that the directive should only apply to natural persons, in the end nothing in this respect was mentioned in the directive. One could assume that the legal basis of the directive, which is Art. 82 (2) TFEU, rules out that the directive applies to legal persons, since it refers to the right of "individuals" in criminal proceedings. That is, however, the text of the English language version. The other language versions of the same treaty text provide a more confusing image: while the German language version[28] seems to support the meaning of the English text, other language versions, such as the Dutch[29] and the French,[30] seem to leave it entirely open as to whether the directive can apply to legal persons as well. It will therefore probably be up to the European Court of Justice to decide on this matter.[31]

Finally, in line with measure A, some minor offences have been excluded from the scope of this directive on measure B.[32]

4. Art. 3 – Right to Information about Rights

Arts. 3 and 4 set rules regarding the right to information about rights. Art. 3 provides that Member States should ensure that at least information on certain procedural rights has to be provided to suspects or accused persons promptly, orally or in writing. All suspects and accused persons are covered here, whether deprived of liberty or not, thus including suspects or accused persons who are at large. Art. 4 provides that more extensive information has to be provided, through a written letter of rights, to suspects or accused persons who are arrested or detained.

In Art. 3, the Commission in its proposal suggested stating that suspects or accused persons should be provided with information on four rights: the right of access to a lawyer, free of charge where necessary; the right to be informed of the charge and, where appropriate, to be given access to the case-file; the right to interpretation and translation; and, finally, the right to be brought promptly before a court if the suspected or accused person is arrested.

In its general approach, the Council refined the text of the Commission, e.g., by splitting the right of access to a lawyer and the right, if any, to legal aid ("any entitlement to free legal advice and the conditions for obtaining it"). The Council also transferred certain rights from Art. 3, regarding all suspects or accused persons, to Art. 4, regarding suspects or accused persons who are arrested or detained. For example, it was decided that the right of access to the case file (later called the right of access to the materials of the case, see below) should only apply when the person is arrested or detained. The same holds true for the right to be brought promptly before a court if the suspect or accused person is arrested; it was somewhat remarkable that this right had been contained in Art. 3 in the first place.

Most importantly, however, the Council enlarged the catalogue of rights in Art. 3 by inserting the right to remain silent. This right has always been a key right in criminal proceedings in most EU Member States as well as in other parts of the world: it is probably the most important right in the Miranda rights[33] in the United States ("you have the right to remain silent and everything you say or do may be used against you in court"). Moreover, the Commission itself had in 2006 analysed the issue of the right to remain silent in the Green Paper on the presumption of innocence.[34] It is therefore surprising that this right was not contained in Art. 3 of the original Commission proposal for measure B. In any event, it is very appropriate that the Council inserted the right to remain silent in Art. 3. This is also a good example of the Council taking a "pro-rights" approach in this directive.

As a result of these modifications made by the Council and the negotiations with the European Parliament, the final text of Art. 3 states that suspects or accused persons should be provided with information on the following rights: a) the right of access to a lawyer, b) any entitlement to free legal advice and the conditions for obtaining it, c) the right to be informed about the accusation, d) the right to interpretation and translation, and e) the right to remain silent. By establishing this list of rights in respect of which information should be provided, the directive gives concrete meaning to the case law of the ECtHR.[35]

There was a lengthy discussion during the negotiations with the European Parliament about when suspects or accused persons should be informed of their rights. The European Parliament suggested that this should be the case "at the point when those rights become applicable and in any event upon questioning by law enforcement authorities." However, the Council felt that this was rather vague wording and proposed that information should be provided at the latest before the "first official interview" of the suspect or accused person by the police or another competent authority. It turned out to be very difficult, however, to agree on a definition of "official interview," in part because the European Parliament feared, understandably, that the scope of Art. 3 would be substantially reduced by using this concept. In the end, it was therefore decided to retain only the term "promptly," as in the Commission proposal and as used in Art. 6 (3) (a) ECHR; a reference to "official interview" was nevertheless kept in recital 19.

As vague as the term "promptly" may seem, it is important to note that it must be interpreted with respect to the possibility for suspects or accused persons to effectively exercise their procedural rights: the expression, if read in the light of the ECHR standards (which, as mentioned above, sets a minimum level for Member States when implementing the directive), implies that information on procedural rights should be given by the competent authorities as early as necessary (and as early as possible) in order for the subject of the investigation to make adequate choices in the exercise of his defence during the proceedings.

It is furthermore important to note that information regarding procedural rights should be provided "as they apply under national law." This means that the information that has to be provided may differ among the Member States. However, as the roadmap is further rolled out and new directives on procedural rights are adopted and implemented in the Member States, the content of this information will converge little by little. In the short term, for example, the information on the right to interpretation and translation should, to a large extent, be similar in all the Member States in view of the upcoming deadline for the implementation of measure A[36] – although some differences may always exist, since all procedural rights directives based on Art. 82(2) TFEU only provide *minimum* rules.

It can ultimately be observed that, according to Art. 3 (2), the information on rights should be provided "in simple and accessible language, taking into account any particular needs of vulnerable suspects or vulnerable accused persons." Recital 26 makes clear that such vulnerable persons can, for example, be children or persons who have a mental or physical impediment. The Council was not very enthusiastic about making a reference in measure B to vulnerable persons: it held that, from a legal drafting point of view, it would be neither elegant nor appropriate to make such a reference, since it is planned that the rights of vulnerable persons will be the subject matter of a specific measure (E) of the roadmap. But inter-institutional compromises almost never win a beauty contest …

5. Art. 4 – Letter of Rights on Arrest

Art. 4 (1) provides that "Member States shall ensure that suspects or accused persons who are arrested or detained are provided promptly with a written Letter of Rights. They shall be given an opportunity to read the Letter of Rights, and shall be allowed to keep it in their possession throughout the time that they are deprived of liberty."

Surprisingly, there was almost no discussion in the Council about the proposal of the Commission, revolutionary for some Member States,[37] to provide arrested suspects or accused persons with a written letter of rights. On this point, the directive clearly contains a new right, which is not foreseen in the ECHR, nor in the case law of the ECtHR.

During the negotiations with the European Parliament, however, there was substantial discussion about the question of which persons a letter of rights should be provided to. The Commission had proposed that a letter of rights should be given to all *arrested persons*. The European Parliament, however, requested that a letter of rights be provided to all *persons who are deprived of liberty*. Even though, in the light of the scope of the directive, this could only mean that a letter of rights should be provided to all *suspects or accused persons who are deprived of liberty*, fear prevailed in the Council that this might extend the right too far. For instance, in certain Member States, it is possible that suspects or accused persons who are not arrested can, for a limited time, be deprived of liberty in order to attend certain procedural acts (e.g., assistance in an identity parade). Another example is that of foreigners who are suspected or accused of having committed a criminal offence (e.g., drug dealing) and who do not have identification papers: they can be kept in police custody for a brief period of time in order for their identities to be established. Again, this is not

arrest, but deprivation of liberty, and the Council did not want that in those particular situations Member States should be required to provide a letter of rights. In the end, a compromise was found by stating that suspects or accused persons who are arrested or detained should be provided with a letter of rights; recital 21, however, states that the notion of arrested or detained should be understood to refer to any situation where, in the course of the criminal proceedings, suspects or accused persons are deprived of liberty within the meaning of Art. 5(1)(c) ECHR, as interpreted in the case law of the ECtHR.

It may be underlined that whilst Member States are only required to provide a letter of rights to suspects or accused persons who are arrested or detained, they are allowed to provide such a letter of rights in other situations during criminal proceedings, since the directive only sets minimum rules.[38]

The Council and the European Parliament debated at length as to what information the letter of rights should contain. There was general agreement that the letter of rights should at least contain information on the rights mentioned under Art. 3; but which other information, if any, should be provided? The European Parliament presented a "wish list" of seven additional items that the letter of rights should contain; after careful consideration, the Council could accept all of them, albeit often in a modified form.

In the final text, a distinction has been made between additional information on "rights," which were given a place in Art. 4(2) and in respect of which the letter of rights should contain "information," and additional information on "possibilities," which were given a place in Art. 4(3) and in respect of which the letter of rights should contain "basic information."

The additional *rights*, in respect of which the letter of rights should contain information, are the following: a) the right of access to the materials of the case (which is organised in Art. 7 of the directive), b) the right to have consular authorities and one person informed (which is the subject matter of measure D of the roadmap), c) the right of access to urgent medical assistance (although one could question whether this really is a procedural right), and d) the maximum number of hours or days suspects or accused persons may be deprived of liberty before being brought before a judicial authority (this information, which relates to Art. 5(3) ECHR, was also contained in the Council's general approach).

The additional *possibilities*, in respect of which the letter of rights should contain basic information, are the following: any possibility under national law of a) challenging the lawfulness of the arrest; b) obtaining a review of the detention; or c) making a request for provisional release (e.g., bail, which the European Parliament referred to). As the text says, Member States only have to provide this information if the relevant possibilities exist in their national law. The reference to "*basic information*" intends to avoid making Member States describe all the details of the relevant procedures. Indeed, it should be sufficient that the suspects or accused persons are aware that the possibilities exist; if desired, they may then seek to obtain more detailed information, e.g., through a lawyer.

With the directive providing minimum rules, Member States may decide to include in the letter of rights information other than that referred to in Arts. 3 and 4, such as information on other rights as they apply in their national law.[39] Member States may, e.g., decide to include in the letter of rights information on any right to communicate with third persons while deprived of liberty, or practical information regarding the operation of detention facilities or the place where the person is kept arrested, e.g., the police station.

In accordance with Art. 4(4) and recital 22, the letter of rights should be drafted in simple and accessible language, such that the content of the letter is easily comprehensible. In order to assist national authorities in drawing up their letter of rights at the national level, an *indicative* model of the letter of rights has been provided in Annex I to the directive. In line with a clear request by Member States, it has been made clear in the heading of this Annex that Member States are not bound to use this model.

Art. 4(5) provides that suspects or accused persons should receive the letter in a language that they understand. Where a letter of rights is not available in the appropriate language, suspects or accused persons should be informed of their rights orally in a language that they understand; a written letter of rights, in a language that they understand, should then be given to them without delay. This will normally mean that Member States are required to make the letter of rights available in multiple languages, not only in the 23 official languages of the European Union but also in many other languages. For example, in application of the directive, the Belgian authorities have already prepared a letter of rights in more than 50 different languages, including such exotic languages as Gujarati, Tatar, and Urdu.[40]

Finally, and returning to Art. 4(1), arrested or detained persons who have received a letter of rights as described above may keep it in their possession during the time they are deprived of liberty. This may seem a harmless provision, but it was the subject of a lively debate in the Council. It was put forth that persons might "abuse" the possession of a letter of rights by fixing it in front of the video camera in the prison cell, thereby impeding the authorities from surveying the situation in the cell; it was also observed that persons might decide to eat the letter of rights with a view to committing suicide. In the end, it

was decided to address these particular concerns by inserting recital 24, according to which the directive "is without prejudice to provisions of national law concerning safety of persons remaining in detention facilities." This should allow national authorities to (temporarily) withdraw the letter of rights from a suspect or accused person if this measure is imperative for reasons of safety.

6. Art. 5 – Letter of Rights in European Arrest Warrant Proceedings

When a requested person who is subject to EAW proceedings is arrested in the executing Member State, he should also be provided with a letter of rights. On this point again, the directive provides a completely new right, which, though logical, is neither foreseen in the ECHR, nor in the case law of the ECtHR. Since the nature of EAW proceedings is different from the nature of criminal proceedings, the letter of rights that has to be provided in EAW proceedings in the executing Member State is distinct from the letter of rights that should be provided in criminal proceedings. An indicative model for such letter has been set out in Annex II to the directive. The letter of rights provides *inter alia* information on the possibility of the requested person to consent to being surrendered to the issuing Member State (which, it is claimed, "would speed up the proceedings") and on the right to a hearing if the requested person does not consent to surrender.

7. Art. 6 – Right to Information about the Accusation

The input from experts of the Member States is most visible in the reformulation of Arts. 6 and 7, which were greatly improved during the work in the Council and during negotiations with the European Parliament.

Whereas the Commission proposal in Art. 6 contained a general rule on information about the *charge*, in the final text of this article, the right to information about the *accusation*[41] has been clarified and tailor-made to apply to different situations or phases in the criminal proceedings.

A general right to information, and the corresponding obligation for Member States, is described in Art. 6 (1). The provision sets out a continuing obligation, during the criminal proceedings, for competent authorities to provide suspects or accused persons with information about the criminal act they are suspected or accused of having committed. Such information should be provided *promptly* and in such *detail* as is necessary to safeguard the fairness of the proceedings and the effective exercise of the rights of the defence. Recital 28 makes clear that the information should be provided at the latest before the first official interview by the police or another competent authority (such another authority could, e.g., be an investigating judge). As a result of the reference to "official interview," which has not been defined in the directive, the Member States have some discretion in determining when the relevant obligation starts to apply. However, "before the official interview" is the latest possible moment in time when the information may be provided; in practice, in order to comply with the necessity to safeguard the fairness of the proceedings, it may be necessary that the information be provided at a much earlier stage. As an example, one might think of a house search conducted against the suspect at the very onset of the investigation: if the search warrant is to be contested by him, it must contain at least basic information (insofar as it is available at the early stage of the proceedings) concerning the offence which is being investigated. Thus, in this example, the suspect should get the information about the criminal act he is suspected of having committed at the time of the house search, without any need to wait for a later interview (which, in many cases, may not even take place).

An additional obligation arises when suspects or accused persons are arrested or detained. In this situation, which is described in Art. 6(2), the competent authorities must inform the suspect or accused person of the reason for his arrest or detention. This should include information on the criminal act that he is suspected or accused of having committed. This information may still be incomplete, for instance because the details of the offence are not yet known to the investigators or because certain elements of the provisional accusation on which the arrest is based cannot be disclosed without irreparably harming the investigation (e.g., the identity of an accomplice who is still at large and needs to be apprehended). These aspects are reflected in recital 28, which clarifies that the information on the accusation "should be given in sufficient detail, taking into account the stage of the criminal proceedings when such a description is given" and "without prejudicing the course of ongoing investigations."

A particular obligation arises in the phase which starts, at the latest, upon submission of the merits of the accusation to a court. During this phase, which is described in Art. 6(3), the competent authorities should provide accused persons with detailed information on the accusation, including the nature and legal classification of the criminal offence as well as the nature of participation by the accused person. The nature of the offence could, for example, be a sexual offence, the legal classification could be rape, and the nature of participation of the accused person could be as an accomplice to the main perpetrator. At this stage, the information should be complete and allow the accused person to fully exercise his right of defence throughout the trial stage, which implies full disclosure of the details in order for exculpating evidence to be produced.

During the work in the Council, it was rightly pointed out that information that has been provided under this article could change during the course of the criminal proceedings. It has therefore been set out in Art. 6(4) that suspects or accused persons should be informed *promptly* of any changes in the information provided where this is necessary in order to safeguard the fairness of the proceedings. This provision draws on a steady line of jurisprudence of the ECtHR,[42] which interprets the rights set out in Art. 6(3) letters a) and b) ECHR as requiring the official notification of any relevant change in the accusation, including its legal qualification, in order to grant the accused person the right to present the pertinent legal arguments and, if necessary, evidence, to defend himself against a specific fact. This jurisprudence, naturally, does not require a halt in the procedure every time a development in the evidence effects a minute adjustment to the accusation: the modification must be of such magnitude to imply that, *in abstracto* and *ex ante*, the accused person may be expected to modify his defence accordingly. As with all cases in which the fairness of the proceedings *ex* Art. 6 ECHR is at stake, it will ultimately be for the competent authorities leading the proceedings to evaluate the necessity of informing the person about any modification in the accusation.

It should also be pointed out that the temporal scope of application of Art. 6(4) of the directive is not limited to the trial phase but rather applies throughout the proceedings. This is the result of a compromise between the Council and the European Parliament, the latter having demanded a much wider application of this rule. The provision as it now stands does indeed apply also to the pre-trial stage (within the framework of Art. 2 of the directive); however, the link between the notification of the change in the accusation and the fairness of the proceedings implies that this new information should only be provided when the suspect or accused person must be put in a condition to actively exercise his right of defence. This occurs only in certain moments of the pre-trial stage (e.g., when a person is arrested and must be put in a condition to contest the factual elements at the basis of the detention order): therefore, it should be excluded that any change in the "working hypothesis" of the investigators, before the indictment, always be communicated to the suspect or accused person. This being said, the extension to the pre-trial stage of the right to obtain information about the modification of the accusation goes well beyond the protection provided under the ECHR, as interpreted in the case law of the ECtHR.

8. Art. 7 – Right of Access to the Materials of the Case

In Art. 7 regarding the right of access to the materials of the case, a balance had to be found between, on the one hand, the need to ensure that criminal prosecutions can be conducted efficiently through national systems for carrying out investigations without the suspect or accused person or any other third person being made aware of them and, on the other hand, the wish to ensure equality of arms for the defence, by providing the right to have access to the materials of the case.

Member States' experts considerably modified Art. 7 during the work on the Council's general approach. It subsequently survived the trilogues with the European Parliament almost unchanged. As finally agreed, Art. 7 gives concrete meaning to the case law of the ECtHR in respect of Art. 5(4) and 6(1) ECHR, as mentioned above.[43]

The first change made by the experts concerned the title of the article. The Commission had proposed to refer to the right of access to the *case file*. Some Member States argued, however, that there is no such thing as a case file in their system; therefore, after long discussion, a more neutral term was used, namely the right of access to the *materials of the case*. A reference to the case file was maintained in recital 31. In Art. 7 itself, the experts made a distinction between access regarding two different types of materials.

Art. 7(1) provides a right of access to "documents" which are essential to allowing arrested *and* detained persons, or their lawyers, to challenge effectively the lawfulness of the arrest or detention. The use of the word "documents," which was discussed at length, is explained in recital 30: it not only comprises documents *strictu senso* but also, where appropriate, photographs and audio and video recordings. It will be for the competent authority, usually a judge, to assess which documents should be considered essential documents for the purposes of this provision. The documents should be made available at the latest before a competent judicial authority is called to decide upon the lawfulness of the arrest or detention in accordance with Art. 5(4) ECHR, and in due time to allow the effective exercise of the right to challenge the lawfulness of the arrest or detention (see recital 30).

Art. 7(2) provides a right of access to "material evidence" to which arrested and detained persons, or their lawyers, should have access in order to challenge the merits of the accusation. The right of access concerns all material evidence in the possession of the competent authorities, whether for or against suspects or accused persons, and to which these persons or their lawyers should have access in order to safeguard the fairness of the proceedings and to prepare the defence. The concept of "material evidence" is wider than that of the documents referred to under Art. 7(1), since recital 31 states that it should *include* materials *such as* documents and, where appropriate, photographs, and audio and video recordings; it therefore covers all items in the hands of the authorities that may be used as

evidence, including hard or real evidence (e.g., objects which have been seized, the *corpus delicti*, etc.). In accordance with Art. 7 (3), access to material evidence should be granted in due time and at the latest upon submission of the merits of the accusation to the judgment of a court. Once again, the directive defines only the latest possible moment at which access must be granted; the concrete circumstances of the case may require that access be given long before that moment (e.g., when a piece of evidence is subject to irreversible modifications requiring that examination by the defence be granted in advance). It will be for the competent authority, normally a judge, to establish in each specific case at which concrete moment in time access to material evidence should be granted.

Art. 7 (4) provides an exception to the right of access to material evidence: access to certain materials may be refused if such access may lead to a serious threat to the life or the fundamental rights of another person, or if such refusal is strictly necessary to safeguard an important public interest, e.g., in cases where access could prejudice an ongoing investigation or seriously harm the national security of the Member States in which the criminal proceedings are being carried out. Recital 32 stresses that any refusal of access must be weighed against the rights of the defence of the suspect or accused person and that restrictions should be interpreted strictly and in accordance with the right to a fair trial under the ECHR.

Finally, Art. 7 (5) provides that access shall be provided free of charge.[44] This is incidentally the only provision in the directive regarding costs. The application of the other provisions of the directive should, in principle, not entail any extra costs for Member States – if one discounts the costs for producing the letter of rights foreseen in Art. 4 (which will, in most cases, only have to be borne once, when drafting the letter and having it translated in the most commonly used languages). This being said, the rights to information may of course indirectly invoke extra costs for the Member States. Indeed, when suspects or accused persons are more aware of their rights (e.g., the right to obtain a written translation of a document), they are inclined to make use of these rights more frequently, which often do entail costs for Member States.

9. Other Articles

Art. 8 (1) states that, when information is provided in accordance with Arts. 3–6, this should be noted using the recording procedure specified in the law of the Member State concerned. According to Art. 8 (2) and recital 36, in case a competent authority fails or refuses to provide information or to give access to certain materials of the case in accordance with this directive, the suspect or accused person or his lawyer should be able to challenge this failure or refusal.

The directive contains in Arts. 9 and 10 provisions on training and non-regression that are identical to those in measure A.

In accordance with Art. 11, the Member States have to transpose the directive into their legal orders by 2 June 2014. It is expected that this will not lead to too many difficulties, since the Member States have unanimously agreed to the directive and since the directive in general does not require Member States to make substantial changes to their legal orders.

Art. 12 requires the Commission to submit by 2 June 2015 a report assessing the extent to which Member States have taken the necessary measures in order to comply with the directive. In this report, the Commission can also propose changes to the indicative model for a letter of rights as set out in Annex I to the directive, see recital 22.

III. Concluding Remarks

The directive on the right to information in criminal proceedings constitutes an important step towards establishing a full catalogue of procedural rights for suspects or accused persons in criminal proceedings. The directive ensures that suspects or accused persons are made aware of their procedural rights and provides important rules on the right to information about the accusation and on the rights of access to materials of the case.

The Commission had submitted a prudent and, in some points, very general proposal, but, in the course of the work in the Council and during the negotiations with the European Parliament, the text has been made more ambitious and precise: it has substantially improved and gained in added value.

In a number of areas, the directive now gives a concrete meaning to general indications contained in the ECHR and, notably, in the case law of the ECtHR: such is the case, for example, as regards the right to information about rights and the right of access to the materials of the case. In other areas, the directive goes well beyond the minimum standards of the ECHR and Strasbourg case law by providing completely new rights, such as the provisions concerning a written letter of rights upon arrest (also in the execution of a European Arrest Warrant) and, in the extension to the pre-trial stage, the right to obtain information about the modification of the accusation.

In all these cases, the directive is a good example of how EU law can foster the protection of fundamental rights in compliance with the mission of the European Union to create for its citizens an area of freedom, security and justice, as set out in Art. 3 (2) of the Treaty on European Union.

Steven Cras
General Secretariat of the Council of the European Union (DG D 2B – Criminal Law and Fundamental Rights)
steven.cras@consilium.europa.eu

Luca De Matteis
Italian Ministry of Justice (Criminal Law – International Affairs)
luca.dematteis@giustizia.it

* The authors, who have written this article on their personal title, would like to thank Caroline Morgan and Signe Öhman for their inspiration and critical comments on an earlier draft; all errors in the article should, however, be attributed to the authors only.

1 O.J. L 142, 1.6.2012, p. 1.
2 O.J. C 295, 4.12.2009, p. 1.
3 Directive 2010/64/EU, OJ L 280, 26.10.2010, p. 1. On this directive, see Steven Cras/Luca De Matteis, "The Directive of the right to interpretation and translation: genesis and description", in: eucrim 2010 (4), p. 153.
4 Together with the Treaty on European Union, the TFEU was amended (established) by the Lisbon Treaty.
5 It happens very often, of course, that interpretation and translation is needed in purely domestic cases, simply because the suspect or accused person, while being a national of the Member State in which the criminal proceedings are conducted, does not (sufficiently) understand the language of the criminal proceedings.
6 COM(2004) 328 final, Council doc 9318/04.
7 "CATS" stands for "Coordinating Committee in the area of police and judicial cooperation in criminal matters", the follow-up of the Art. 36 Committee *(Comité Article Trente-Six)* that was created by the Amsterdam Treaty (and which in its turn was the successor of the Coordinating Committee referred to in Article K4 of the Maastricht Treaty).
8 Permanent Representatives Committee.
9 Droipen is the abbreviation of droit pénal (criminal law).
10 For practical reasons, though, some Member States – in particular the smaller ones – often tend to send Brussels-based (JHA) counsellors to meetings of the Friends of the Presidency.
11 Council doc 17503/10.
12 S&D is the Group of the Progressive Alliance of Socialists and Democrats in the European Parliament.
13 In measure B, in fact, rapporteur Ms. Sippel seemed to work on the basis of case-by-case *ex ante* mandates by the shadow rapporteurs. This is a different approach than that taken for measure A, where it appeared that rapporteur Baroness Sarah Ludford (ALDE – Group of the Alliance of Liberals and Democrats for Europe) negotiated with the Council more directly, apparently working on the basis of *ex post* approval by the shadow rapporteurs (negotiations "*ad referendum*"). This difference in approach between the rapporteurs in measures A and B might be a question of personality or negotiation style, but it might also have to do with the fact that the "honeymoon feeling" about the European Union finally legislating in the field of procedural rights had dissipated.
14 Council doc 16342/11.
15 See, e.g., *Padalov v. Bulgaria*, 10 August 2006, par. 52-54; *Talat Tunç v. Turkey*, 27 March 2007, par. 61; *Panovits v. Cyprus*, 11 December 2008, par. 73. See also the explanatory memorandum to the Commission proposal.
16 See, e.g., *Jasper v. United Kingdom*, 16 February 2000, par. 51; *Edwards v. United Kingdom*, 27 October 2004, par. 46-48.
17 *Schöps v. Germany*, 13 February 2001, par. 44; *Mooren v. Germany*, 9 July 2009, par. 124.
18 See *Cras* and *De Matteis*, op.cit., p. 157, where reference is made to the following case law: *Engel and others v. the Netherlands*, 8 June 1976, par. 70-81; *Öztürk v. Germany*, 21 February 1984, par. 53; *Campbell and Fell v. the United Kingdom*, 28 June 1984, par. 70; *Garyfallou AEBE v. Greece*, 24 September 1997, par. 33.
19 H. v. Spain, 15 December 1983.
20 OJ L 190, 18.7.2002, p.1.
21 In its general approach, the Council had even agreed putting "*made aware by official notification or otherwise, as established under national law.*" These last words were inserted at the last minute of the negotiations on the Council general approach, but they had the potential – and probably intended – consequence of substantially reducing the scope of the directive. It was therefore fortunate that they were eliminated during the negotiations with the European Parliament.
22 See *Cras / De Matteis*, *op. cit.* (n. 3), p. 157, where reference is made to the case of *De Weer v. Belgium*, 10 March 1977 (Commission Decision, plenary).
23 See Art. 10 in measure B; Art. 8 in measure A.
24 See also recital 40 of the directive.
25 France, see Council doc 18702/11 (not classified).
26 The declaration is set out in Council doc 18702/11: "The provisions of the Directive on the right to information in criminal proceedings do not necessarily constitute a precedent in the framework of discussions concerning other proposals for measures contained in the Roadmap for strengthening procedural rights of suspected or accused persons in criminal proceedings. However, overall consistency with the remaining measures provided for by the Roadmap shall be ensured."
27 Another reason may be that the new French government, which came into power after the elections in Spring 2012, takes a more pro-rights approach.
28 "die Rechte des Einzelnen im Strafverfahren"
29 „de rechten van personen in de strafvordering"
30 "les droits des personnes dans la procédure pénale"; although all language versions of the Treaty are equally authentic, the fact that the text was originally drafted in the French language, under the Presidency of Valéry Giscard d'Estaing, might carry some weight in this matter.
31 It may be interesting to note in this context that, in the fairly recent DEB case (C-279/09, DEB Deutsche Energiehandels- und Beratungsgesellschaft, mbH, judgment of 22 December 2010, in particular point 59), the European Court of Justice concluded that the principle of effective judicial protection, as enshrined in Art. 47 of the Charter, must be interpreted to mean that it is not impossible for *legal persons* to rely on this principle.
32 See Cras / De Matteis, *op. cit.* (n. 3), p. 157.
33 The concept of "Miranda rights" was enshrined in U.S. law following the 1966 *Miranda v. Arizona* Supreme Court decision, which found that the Fifth and Sixth Amendment rights of Ernesto Arturo Miranda had been violated during his arrest and trial for domestic violence. According to the ruling, "... The person in custody must, prior to interrogation, be clearly informed that he or she has the right to remain silent, and that anything the person says will be used against that person in court; the person must be clearly informed that he or she has the right to consult with an attorney and to have that attorney present during questioning, and that, if he or she is indigent, an attorney will be provided at no cost to represent her or him."
34 COM(2006) 174 final. Section 2.5 is on the right to silence.
35 See the case-law cited in footnote 17.
36 The deadline for the implementation of measure A (Directive 2010/64/EU on the right to interpretation and translation in criminal proceedings) was 27 October 2013.
37 According to the Commission's Impact Assessment accompanying the proposal, 11 Member States were already operating a letter-of-rights system before the proposal was submitted.
38 This has also been indicated in the heading of Annex I to the directive: "The Member State's Letter of Rights must be given upon arrest or detention. This however does not prevent Member States from providing suspects or accused persons with written information in other situations during criminal proceedings."
39 See also recital 22 and the heading of Annex I to the directive.
40 http://justice.belgium.be/fr/themes_et_dossiers/services_du_spf/telecharger_des_documents/declaration_de_droits/1/
41 See above under Art. 1 for an explanation of why this change in terminology, from charge to accusation, was implemented.
42 See, e.g., *Pélissier and Sassi v. France*, 25 March 1999, par. 51; *I.H. v. Austria*, 20 April 2006, par. 30; *Drassich v. Italy*, 11 December 2007, par. 31.
43 See the ECtHR case-law mentioned in footnotes 18 and 19.
44 In accordance with recital 34, however, the persons concerned or their lawyers, may be sent a bill for the costs of photocopies or stamps.
lawyers, may be sent a bill for the costs of photocopies or stamps!

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. mult. Ulrich Sieber
Guenterstalstrasse 73, 79100 Freiburg i.Br./Germany

Tel: +49 (0)761 7081-0
Fax: +49 (0)761 7081-294
E-mail: u.sieber@mpicc.de h

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)761-7081-256 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.