

# euocrim

2017 / **2**

**THE EUROPEAN CRIMINAL LAW ASSOCIATIONS' FORUM**



**Focus: Reform of European Criminal Law – PFI and Data Protection**

**Dossier particulier: Réforme du droit pénal européen – PIF et protection des données**

**Schwerpunktthema: Reform des Europäischen Strafrechts – Finanzschutz und Datenschutz**

Guest Editorial

*Alexandra Jour-Schroeder*

The Directive on the Fight against Fraud to the Union's Financial Interests  
by Means of Criminal Law (PIF Directive) – Laying Down the Foundation for a Better Protection  
of the Union's Financial Interests?

*Adam Juszcak and Elisa Sason*

Reform des europäischen Datenschutzrechts – Ein Überblick unter besonderer Berücksichtigung  
des Datenaustausches zwischen Polizei-, Strafjustiz- und Geheimdienstbehörden

*Petra Beckerhoff*

The Associations for European Criminal Law and the Protection of Financial Interests of the EU is a network of academics and practitioners. The aim of this cooperation 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.

## Contents

### News\*

#### European Union

##### Foundations

- 54 Fundamental Rights
- 56 Area of Freedom, Security and Justice
- 57 Schengen

##### Institutions

- 59 Council
- 59 OLAF
- 61 Europol
- 62 Eurojust
- 62 Frontex
- 63 Agency for Fundamental Rights (FRA)

##### Specific Areas of Crime / Substantive Criminal Law

- 63 Protection of Financial Interests
- 65 Money Laundering
- 67 Tax Evasion
- 68 Counterfeiting & Piracy
- 69 Terrorism
- 69 Cybercrime

##### Procedural Criminal Law

- 70 Procedural Safeguards
- 71 Data Protection
- 72 Ne bis in idem
- 73 Victim Protection
- 73 Freezing of Assets

##### Cooperation

- 74 European Arrest Warrant
- 75 European Investigation Order

#### Council of Europe

##### Foundations

- 75 Reform of the European Court of Human Rights
- 76 Human Rights Issues

##### Specific Areas of Crime

- 76 Corruption
- 79 Money Laundering

### Articles

#### Reform of European Criminal Law – PFI and Data Protection

- 80 The Directive on the Fight against Fraud to the Union's Financial Interests by means of Criminal Law (PIF Directive) – Laying Down the Foundation for a Better Protection of the Union's Financial Interests?  
*Adam Juszcak and Elisa Sason*
- 88 Reform des europäischen Datenschutzrechts – Ein Überblick unter besonderer Berücksichtigung des Datenaustausches zwischen Polizei-, Strafjustiz- und Geheimdienstbehörden  
*Petra Beckerhoff*

\* 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](http://www.mpicc.de/eucrim/search.php) and then entering the ID-number of the link in the search form.

# Guest Editorial

Dear Readers,

The year 2017 has brought and will hopefully lead to further major steps in the development of a true European Criminal Justice Area, particularly but not only with regard to the protection of the EU's financial interests by criminal law.

The adoption of the Directive on the fight against fraud to the Union's financial interests by means of criminal law, the so-called "PIF Directive," is a key achievement in putting an end to the largely outdated 22-year-old "PIF Convention." With its comprehensive catalogue of criminal offences, including fraud, corruption, money laundering, and misappropriation affecting the EU budget as well as its ambitious rules for limitation periods, the PIF Directive guarantees a high level of protection. The inclusion of serious cross-border VAT fraud – the most controversial part of the negotiations – is an especially important milestone, given that the financial damage caused by VAT fraud goes into the billions of Euros annually. The Directive's dissuasive effect could have been strengthened even more with the minimum sanctions proposed by the Commission, which were not taken over by the co-legislators.

Following the political agreement of 20 Member States the final adoption of the regulation establishing a European Public Prosecutor's Office (EPPO), after the consent of the European Parliament, is within reach. Thanks to such a truly independent European prosecution office, equipped with investigatory and prosecutorial powers, the EU will not only step up the protection of the EU's budget but also enter into a new level of integration in the area of EU criminal law.

In reaction to the increasing security threat from terrorist offences, the 2017 Directive on combating terrorism will contribute to preventing terrorist attacks by criminalizing acts such as undertaking training or travelling for terrorist purposes. It is important that the Directive simultaneously strengthens the rights of victims of terrorism. As part of the EU strategy against financial crimes and, in particular, terrorist financing, the European Commission has adopted two significant proposals that will hopefully be finalised soon: one addresses the quick and efficient mutual recognition of freezing and confiscation orders; a second one aims at countering money laundering by criminal law, complementing the EU's comprehensive and recently revised preventive anti-money laundering rules.

With these new rules, the Union will be moving closer to its objective of disrupting and effectively cutting off the financial sources of criminals.

At the same time, significant progress has been made in the EU towards strengthening rights in criminal proceedings in full accordance with the EU's Charter on Fundamental Rights. With the final adoption of the Directive on legal aid by the end of 2016, the EU now possesses a strong protective legal framework to ensure the rights of suspects undergoing a trial procedure. The EU rules range from granting the right to interpretation and translation to suspects to information about their rights in criminal procedure, access to the case file, and access to a lawyer. They strengthen the presumption of innocence and the right to be present at one's trial and improve procedural safeguards for children. It is now imperative to ensure their consequent and correct application across the EU.

A high protection of rights also includes the protection of personal data in the field of criminal law. A specific Directive was adopted last year, as part of the Data Protection Reform, in order to protect individuals' personal data when being processed by police and criminal justice authorities. It will also allow police and criminal justice authorities in the EU to more efficiently exchange the information necessary for investigations. A stand-alone data protection regime is foreseen for the EPPO, but this may develop in the future.

Providing a high degree of security, offering protection from crime, and at the same time guaranteeing freedoms and rights remain the yardstick for the EU legislator, especially in times of high security threats. Work in the area of EU criminal justice is not yet finished.

Alexandra Jour-Schroeder\*

Director Criminal Justice, Directorate General for Justice, Consumers and Gender Equality, European Commission

\* The views expressed are those of the author and not necessarily those of the European Commission.



Alexandra Jour-Schroeder



### European Union\*

Reported by *Thomas Wahl (TW)* and *Cornelia Riehle (CR)*

#### Foundations

#### Fundamental Rights

##### Commission Reports on Application of CFR in 2016

On 18 May 2017, the European Commission published its 2016 Report on the application of the EU Charter of Fundamental Rights.

The report outlines the initiatives taken in 2016 by the EU to strengthen fundamental rights. It also includes information on how these rights were applied across a range of EU policies and in the Member States in 2016. The report is accompanied by a staff working paper, which contains more in-depth information and statistical data.

Regarding legislative developments that are important for criminal law, the report highlights the various directives on strengthening procedural safeguards in criminal proceedings adopted in 2016, i.e., the Directives on the presumption of innocence and the right to be present at the trial, on legal aid and on the rights of children in criminal proceedings, which reinforced the

right to a fair trial (Arts. 47 and 48 of the Charter).

The protection of personal data is considered a further key area of focus in 2016, due to the adoption of the General Data Protection Regulation (GDPR – Regulation (EU) 2016/679) and the Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities. The latter aims to establish an efficient information exchange between national enforcement authorities and to ensure that the data of victims, witnesses, and suspects of crimes are duly protected in the context of a criminal investigation or a law enforcement action (for this new data protection framework, see also the article by *Beckerhoff* in this issue). The Commission also mentions the conclusion of the EU-US Umbrella Agreement, which regulates the transfer of personal data between the EU and the United States in the context of police or judicial cooperation in criminal matters.

A further focus of EU action in 2016 referred to combating racism and xenophobia, which affects many fundamental rights of the Charter. The code of conduct on countering illegal hate speech online deserves mention here. It was

concluded between the Commission and Facebook, Twitter, YouTube, and Microsoft in 2016.

The Commission ultimately mentions that it continuously works on improving the compatibility of its actions with fundamental rights. An example in this regard is the new Directive on combatting terrorism, where several fundamental rights were already taken into account in the drafting and negotiating phase.

The 2016 fundamental rights report of the Commission concludes that recent developments pose serious threats to fundamental rights. The Commission particularly supports the important system of checks and balances, in particular the key role of supreme courts and constitutional courts in upholding the EU's common values. It also highlights the key role of civil society organisations in preserving democracy, the rule of law, and fundamental rights.

For the 2015 report, see [eucrim 2/2016](#), p. 66. (TW)

➤ [eucrim ID=1702001](#)

#### FRA's Fundamental Rights Report 2017

Shortly after the above-mentioned Commission report was published, the European Union Agency for Fundamental Rights (FRA) released its 2017 Fundamental Rights Report on 30 May 2017. The report coincides with the 10th anniversary of FRA, which is why the focus section of this year's report reviews the highlights of the past decade as well as the shortfalls in human rights protection

\* If not stated otherwise, the news reported in the following sections cover the period 16 March 2017 – 30 June 2017.

within the EU. Against this background, the report concludes that there is a gap between the fundamental rights framework, in principle, and fundamental rights outcomes in practice. Although key milestones were achieved, such as the binding effect of the EU Charter of Fundamental Rights (CFR) and the establishment of the FRA, the implementation of fundamental rights on the ground remains a concern. According to the report, “this is exacerbated by a political environment in which parts of the electorate and their representatives increasingly appear to question not only certain rights but the very concept of a rights-based polity.”

The remaining chapters reflect on the main fundamental rights developments in 2016 under the three titles “equality, freedoms and justice.” The nine specific thematic areas include the following:

- The EU Charter of Fundamental Rights and its use by Member States;
- Racism, xenophobia, and related intolerance;
- Asylum, borders, and migration;
- Information society, privacy, and data protection;
- Access to justice, including the rights of crime victims.

As reports of the past years indicate (see *eu crim* 2-2016, p. 66 for the 2016 report), each chapter ends with opinions of the FRA, which outline evidence-based advice for consideration by the relevant main actors within the EU.

Regarding privacy and data protection, for example, the FRA report recommends the following:

- Reforms on surveillance should be transparent and include international and European standards and safeguards;
- Measures to overcome the challenges of encryption should be proportionate to the legitimate aim of fighting crime;
- National law on data retention should include strict proportionality checks as well as appropriate procedural safeguards;
- The law on Passenger Name Record data should ensure that retention is duly

justified, that effective remedies are in place, and that the oversight is independent.

As far as access to justice is concerned, the FRA opinions include *inter alia*:

- All relevant actors at the national level need to step up efforts to uphold and reinforce the rule of law;
- The EU actors are called on to develop objective, comparative criteria (like indicators) and contextual assessments that prevent the erosion of the rule of law;
- EU Member States should continue their efforts to ensure that procedural rights in criminal proceedings are duly reflected in national legal orders and effectively implemented across the EU;
- EU Member States should strengthen victim support services;
- All EU Member States should consider ratifying the Council of Europe Convention on preventing and combating violence against women and domestic violence (Istanbul Convention) as well as implementing it.

In general, the report further proposes, *inter alia*, that the full potential of the CFR must be further elaborated, including accession of the EU to the ECHR, and that support for fundamental rights defenders should be strengthened. (TW)

► *eu crim* ID=1702002

### MEPs Want Improvements in Detention Conditions in EU Member States

During the past several years, the European Parliament has called attention to the prison conditions in Member States of the European Union. In a resolution of 2 April 2014, the EP called on the European Commission to reconsider establishing common measures to improve detention standards and to ensure the proper administration of prisons. In a resolution of December 2016, the Parliament reiterated its concerns over prison conditions in some Member States, pointing to overcrowding and ill-treatment. It called on the Commission to assess the effect of the prison and criminal

justice system on children as well as to support Member States by facilitating an exchange of best practices. In this context, the EP started an own-initiative report on prisons’ systems and conditions.

The report was prepared by *Joëlle Bergeron*, EFDD, France. On 21 June 2017, the Parliament’s LIBE Committee adopted the own-initiative report. It is concerned about the systematic use of pre-trial detention and calls on national authorities to give priority to alternatives to imprisonment as much as possible. It also demands that special attention be given to vulnerable prisoners and to the specific needs of women, especially during pregnancy. MEPs insist on the need to prevent radicalisation and to offer adequate remuneration, working conditions and training to prison staff. The report is scheduled for a plenary vote at the September 2017 session of the EP. (TW)

► *eu crim* ID=1702003

### CJEU Judgment on Charter Right to an Effective Remedy and Fair Trial in Tax Case

On 16 May 2017, the European Court of Justice (CJEU) took an important decision on the interpretation of Art. 47 of the EU Charter of Fundamental Rights (CFR) – the right to an effective remedy and to a fair trial – in the context of administrative tax proceedings.

In the case at issue (C-682/15), a Luxembourg company, *Berlioz Investment Fund SA*, objected to providing certain pieces of information to the Luxembourg authorities. The Luxembourg authorities had requested this information on the basis of a request from the French tax authorities, which were carrying out tax investigations against a subsidiary company of *Berlioz* in France. *Berlioz* argued that the information sought was not “foreseeably relevant” to the checks being carried out by the French tax administration and referred to Arts. 1(1) and 5 of Directive 2011/16 on administrative cooperation in the field of taxation (which stipulates this condition).

The referring Luxembourg Administrative Court had doubts as to whether the Luxembourg law is in line with Art. 47 CFR and Directive 2011/16. Under Luxembourg law, the company could apply for cancellation or reduction of a fine, which was imposed due to refusal to provide requested information, but not annulment of the decision requiring the information to be provided (“information order” by the Luxembourg authorities). Therefore it could not reject the underlying request for the exchange of information (here: by the French tax authorities) as the basis of the information order.

The CJEU found that Art. 47 CFR must be interpreted as meaning that a person (here: the legal person *Berlioz*), upon whom a pecuniary penalty had been imposed for failure to comply with an information order in the exchange between national tax administrations pursuant to Directive 2011/16, is entitled to challenge the legality of that decision.

The Court further noted that the “foreseeable relevance” of the information for the purposes of the tax investigations in the requesting Member State is a pre-condition for the lawfulness of the information order and has to be examined by the Luxembourg courts. The condition intends to prevent “fishing expeditions” or requests for information that are unlikely to be relevant to the tax affairs of the taxpayer concerned.

The CJEU adds that the authorities of the requested Member State (here: Luxembourg) are not confined to a brief and formal verification of the regularity of the request for information but must satisfy themselves that the information sought is not devoid of any foreseeable relevance. Attention must be paid in this context to the identity of the taxpayer concerned and to that of any third party asked to provide the information as well as to the requirements of the tax investigation concerned. As a consequence, Directive 2011/16 and Art. 47 CFR must be interpreted as meaning that a national court in the requested state, which re-

views a penalty imposed on a person for non-compliance with an information order, also has jurisdiction to review the legality of that information order. The court’s review is, however, limited to verification that the requested information *manifestly* has no “foreseeable relevance.”

As regards the question of a fair trial, the CJEU ultimately found that Art. 47, second paragraph CFR requires that the court of the requested State conducting judicial review must have access to the request for information made by the requesting State (here: France). The person concerned does not, however, have a right of access to the entirety of said request for information, which is to remain a confidential document in accordance with Art. 16 of Directive 2011/16. Nevertheless, in order for the hearing to be fair, that person must have access to key information in the request, and the national court may provide further information if it considers the key information insufficient to assess the “foreseeable relevance.” (TW)

► [eucrim ID=1702004](#)

## Area of Freedom, Security and Justice

### 2017 EU Justice Scoreboard Looks into Length of Anti-Money Laundering Court Proceedings

On 10 April 2017, the Commission published the 2017 EU Justice Scoreboard. With this tool – meanwhile released for the fifth time – the Commission provides comparative data on the efficiency, quality, and independence of national justice systems in the EU.

The EU Justice Scoreboard regularly focuses on litigious civil and commercial as well as administrative cases with a view to giving guidance to the EU Member States for an investment-, business-, and citizen-friendly environment. Thus, the scoreboard can also be considered a basis for the good functioning of the EU’s single market. Therefore, the

scoreboard also looks into the relevant specific areas where national courts apply EU law.

The 2017 scoreboard for the first time provides data on the length of first instance criminal court proceedings dealing with money laundering offences under the Anti-Money Laundering Directive. Art. 44 of the 4th Anti-Money Laundering Directive (2015/849) requires Member States to maintain statistics on the effectiveness of systems in place to combat money laundering or terrorist financing. The key finding in the scoreboard is that, among those Member States that made data available, there appear to be notable variations in case length, ranging from less than half a year up to almost three years.

Other conclusions of the 2017 EU Justice Scoreboard are as follows:

- In some Member States, access to justice by persons whose income is below the poverty threshold is hampered;
- Use of electronic communication between courts and lawyers is limited in some countries;
- Businesses and citizens cited interference from government and politicians as the main reason for perceived lack of judicial independence; the guarantees provided with regard to the status and position of judges were mentioned as the main reason for a positive perception of judicial independence;
- Most, but not all EU Member States have implemented quality standards to avoid lengthy judicial proceedings, such as fixing time limits or timeframes.

The assessments made in the scoreboard may lead the Commission to propose that the Council adopt country-specific recommendations on improving the effectiveness of Member States’ national justice systems. (TW)

► [eucrim ID=1702005](#)

### Council Conclusions on Security Checks in Cases of Irregular Migration

The Home Affairs Ministers of the EU Member States further intend to improve the detection of potential terrorists who



may exploit irregular migratory movements to enter the EU. Cross-checking of irregular migrants who are apprehended within the EU was found to be divergent among EU Member States.

In order to remedy this deficit, the Ministers, at their meeting on 9 June 2017, adopted Council conclusions giving guidance for a more harmonised practice as regards security checks in the case of irregular migration. When faced with irregular migrants, they recommend that Member States perform checks, where relevant, against a non-exhaustive list of national, European, and international databases. (TW)

► [eucrim ID=1702006](#)

### CJEU: Study in a Sensitive Field May Justify Public Security Threat

On 4 April 2017, the CJEU decided that the national authorities may, for reasons of public security, refuse to grant a visa for study in a sensitive field (here: information technology security) to a national of a country against which the EU has imposed restrictive measures (here: Iran).

The CJEU had been called on to interpret Art. 6 para. 1 lit. d) of Directive 2004/114/EC on the conditions of admission of third-country nationals for the purposes of studies, pupil exchange, unremunerated training or voluntary service. The Directive promotes the mobility of students from third countries to the EU in order to promote the EU as a world centre of excellence for study and professional training. The said provision in the Directive requires, however, that third-country nationals not be regarded as a threat to public security so that they can be admitted to take up studies in a EU country.

The CJEU confirmed that national authorities enjoy a wide margin of discretion when assessing the facts of whether or not a person applying for a visa for study purposes represents a threat – even if potential – to public security. As a result, the CJEU backed a decision by German authorities to deny

a visa to an Iranian student with a degree from a university, which is the subject of restrictive EU measures because of its large-scale involvement with the Iranian government in military related fields. The Court confirmed that plans to carry out research in a sensitive field may be taken into account as justifying the threat to public security because the knowledge acquired could subsequently be used for domestic repressions or human rights violations.

In the case at issue, which had been referred to the CJEU by the Administrative Court of Berlin, Ms Fahimian, an Iranian national, held a Master's degree in the field of information technology awarded by an Iranian university, which is subject of restrictive EU measures because of its support of the Iranian government. The claimant wanted to take up doctoral studies at the Technical University of Darmstadt/Germany involving topics relating to the security of mobile systems, including the intrusion of smartphones. The case at the CJEU is referred to as C-544/15, *Sahar Fahimian v Bundesrepublik Deutschland*. (TW)

► [eucrim ID=1702007](#)

## Schengen

### Council and EP Agree on Principles of Entry-Exit System

On 29 June 2017, the Maltese Council Presidency and representatives of the EP agreed on the main political provisions of the planned Entry-Exit System (EES). The current legislative proposals had been tabled by the Commission in April 2016.

The EES will be a new large-scale IT system at the European level. It records data relating to border crossings from all third-country nationals visiting the Schengen area for a short stay, including visa-required and visa-exempt travellers. The purpose of the EES is threefold:

- Improving the quality of border checks for third-country nationals by re-

## Annual Conference on EU Criminal Justice 2017

Trier, 23–24 October 2017

This annual conference – organized by the Academy of European Law (ERA) – will facilitate the exchange of experiences among legal practitioners on current developments and future initiatives in the field of EU criminal justice. This year's event will focus on 15 years of the European Arrest Warrant (EAW) and on so-called "future crimes" or "crimes 2.0". Highranking representatives of the EU institutions, academics and national experts will discuss and debate the key priorities within the Area of Freedom, Security and Justice for the year ahead.

The conference is addressed to judges, prosecutors, lawyers in private practice, civil servants and policymakers active in the field of EU criminal law. It will be held in English.

*For further information, please contact Mr Laviero Buono, Head of Section - Criminal Law, ERA, e-mail: [lbuono@era.int](mailto:lbuono@era.int). The programme is available via ERA's website: [www.era.int](http://www.era.int)*

placing the current slow and unreliable system of manual stamping of passports. This will allow both a better monitoring of authorised stays as well as more efficient border checks;

- Ensuring systematic and reliable identification of a category of irregular migration, which is currently not covered by the other IT systems in place, i.e., overstayers (persons who legally enter the EU at an official border point but who stay after their entitlement to do so expires). The identification of overstayers is above all ensured by storing biometric data in the EES on all persons not subject to the visa requirement;

- Reinforcing internal security and the fight against terrorism and serious crime: The EES is expected to help identify terrorists, criminals, and victims by allowing the travel histories of third-country nationals, including crime suspects, to be traced.

The draft regulation also provides for interoperability between the Entry-Exit System and the Visa Information System (VIS) as well as the planned ETIAS (see news item below).

The working groups will continue to negotiate technical details of the draft regulations before the texts are again submitted to the EP and Council for adoption of the legislation.

In an opinion of 21 September 2016, the European Data Protection Supervisor already critically examined the negative aspects and impacts of the proposal on the rights to privacy and protection of personal data. (TW)

►eucrim ID=1702008

### Council General Approach on ETIAS

At its meeting on 9 June 2017, the JHA Council agreed on a general approach to the Commission's proposal for a European travel information and authorisation system (ETIAS). For details on the proposal, see eucrim 4/2016, p. 155.

ETIAS will allow for advance checks and, if necessary, deny travel authorisation to visa-exempt third-country nationals travelling to the Schengen area. Its purpose is to improve internal security, prevent illegal immigration, limit public health risks, and reduce delays at the borders by identifying persons who may pose a risk in one of these areas before they arrive at the external borders.

The general approach constitutes the Council's position in negotiations with the European Parliament. The two institutions are expected to reach an agreement by the end of 2017, and ETIAS may be operational by 2020. (TW)

►eucrim ID=1702009

### EDPS Critical on SIS Reform

On 2 May 2017, the European Data Protection Supervisor (EDPS) issued a critical opinion on the legislative package for reform of the Schengen Information System (SIS), presented by the Commission on 21 December 2016 (see eucrim 1/2017, p. 7).

The EDPS regrets that he was not able to provide an in-depth analysis of the proposal due to the tight time limits. He points out the present fragmented landscape of EU information systems for law enforcement and border control as well as the ongoing discussions on the interoperability of the systems. In this context, he calls on the EU legislator to reflect more generally on a more consistent, coherent, and comprehensive legal framework for large-scale EU systems in the AFSJ that complies with data protection principles.

Regarding the concrete Commission proposal, the EDPS mainly criticises three issues:

- The introduction of new data categories, including biometric identifiers, raises the question of necessity and proportionality and should therefore be accompanied by an impact assessment on the right to privacy and to data protection as enshrined in the Charter of Fundamental Rights;
- Regarding the higher number of authorities with access to the SIS, questions of responsibility, accountability, and restrictions should be better examined;
- The extension of the data retention period for alerts on persons (from three years in the current legal basis to five years in the proposed legislation) should be better justified.

The EDPS announced that he will further monitor the developments, in particular regarding whether the Commission issues a second set of proposals to improve the interoperability of SIS with other large-scale IT systems in the EU. (TW)

►eucrim ID=1702010

### Commission Looks for Alternatives to Internal Border Controls

The possibility to maintain temporary internal border controls on the part of certain Schengen States is drawing to a close. The measure was introduced to overcome the critical migration situation, particularly in Greece. Upholding internal border checks is regularly

examined by the Commission, which makes corresponding recommendations to the Council as to whether or not to lift these measures (see, e.g., eucrim 1/2017, p. 8 for further reference). On 12 May 2017, the Commission recommended that Austria, Germany, Denmark, Sweden, and Norway be allowed to maintain internal border controls for one last period of six months. The Council has not yet decided on this proposal.

In parallel, the Commission presented a non-binding recommendation to the Schengen States, which calls for an increase in proportionate police checks and better police cooperation in the Schengen area.

The Commission believes that proportionate police checks could prove more efficient than internal border controls, as they can be applied in a more flexible manner and are easier to adapt to emerging risks. Schengen states are, *inter alia*, recommended to do the following:

- Intensify police checks across the entire territory, including border areas;
- Carry out police checks on main transport routes, including border areas;
- Modify police checks in border areas on the basis of continuous risk assessment, while ensuring that they do not have border control as an objective;
- Make use of modern technologies in order to monitor vehicles and traffic flows.

Furthermore, the Commission recommends that Schengen States give precedence to police checks before introducing or prolonging temporary internal border controls if there is a situation of serious threats to public policy or internal security.

Member States should also strengthen cross-border police cooperation, for example through joint police patrols in cross-border trains, joint threat analyses, and enhanced cross-border information exchanges. They should also apply existing bilateral agreements in order to prevent irregular secondary movement. (TW)

►eucrim ID=1702011



## Institutions

### Council

#### Council Work Programme of New Trio Presidencies

“The Union’s ability to act as a security provider” is one of the key terms of the 18-month work programme of the three Council presidencies, Estonia (1 July – 31 December 2017), Bulgaria (1 January – 30 June 2018), and Austria (1 July – 31 December 2018).

Besides progress on managing migration, both in its internal and external dimension, the programme identifies the following priority areas as regards freedom, security, and justice:

- *Implementation of the European Agenda on Security* and the relevant parts of the *European Agenda on Migration*: This area focuses, in particular, on improving the functionalities and interoperability of existing large-scale IT systems (i.e. Eurodac, Schengen Information System, Visa Information System, European Criminal Records Information System) and on introducing new ones (entry-exit system, ETIAS, see also above under “Schengen”). It also focuses on optimising the exchange of information between law enforcement bodies, security services, and EU Agencies by implementing common standards and procedures and by achieving technical compatibility to better re-use existing data. This topic also includes increasing the effectiveness of available instruments to combat terrorism, terrorist financing, money laundering, cyber-crime, and organised crime.
- *Prevention of radicalisation and violent extremism*: The trio continues to work on a comprehensive and integrated approach towards the prevention of violent extremism, also focusing on the role of education and intercultural dialogue.
- In the field of *justice*, e-justice and electronic means enhancing access to justice for citizens and businesses are to be promoted and further developed.

Other topics include the promotion of anti-corruption cooperation between the Member States; the enhancement of the system of mutual recognition (with a priority on increasing the smooth implementation and application of already adopted instruments in the field of judicial cooperation in criminal law matters); and – last but not least – the establishment of the European Prosecutor’s Office.

The programme of the three upcoming presidencies sets long-term goals and prepares a common agenda determining the topics and major issues that will be addressed by the Council over an 18-month period. On the basis of this programme, each of the three countries prepares its own more detailed 6-month work programme. For the programme of the Estonian Presidency, see the following news item. (TW)

➤ [eucrim ID=1702012](#)

#### Work Programme of Estonian Council Presidency

As from 1 July 2017, Estonia has taken over the Presidency of the Council of the European Union. One focus of its work programme for the next six months of its presidency is the protection of the EU’s budget against fraud. In this context, Estonia aims to launch negotiations on a new cross-border VAT system and to finalise the agreement on the establishment of a European Public Prosecutor’s Office.

Security issues remain high on the agenda. They include, first of all, modern IT solutions and databases with a view to maintaining public security within the Schengen area. Concrete plans are, *inter alia*:

- To enhance security in the Schengen area by strengthening cooperation and improving compensatory measures, particularly regarding control and surveillance of the European Union’s external borders;
- To enhance security by means of practical cooperation, e.g., a more frequent and efficient exchange of information on serious crime;

- To seek agreement on the new European Entry-Exit System;
- To reach the final stage of negotiations on the European Travel and Information System;
- To enable a more precise exchange of information on criminals by modernising the Schengen Information System and improving the European Criminal Records Information System;
- To make the information systems interoperable and to facilitate clearly defined and justified access by authorities to the data held in these information systems.

A second major topic of security issues is the reinforcement of cross-border cooperation in order to tackle terrorism and organised crime more effectively. More precisely planned actions, *inter alia*, include:

- Promoting measures that focus both on preventing radicalisation and on building the rapid response capabilities of the Member States, including bringing together more closely the internal and external aspects of the fight against terrorism;
- Strengthening the EU’s capacity to counter money laundering under criminal law and modernising the EU legislative framework on mutual recognition of criminal asset freezing and confiscation orders;
- Improving the availability and processing of e-evidence.

The work programme must be seen in the context of the trio’s 18-month work programme over the next Council presidencies, which are being carried out successively by Estonia, Bulgaria, and Austria (see news item above). (TW)

➤ [eucrim ID=1702013](#)

### OLAF

#### OLAF Annual Report 2016

On 31 May 2017, OLAF published its seventeenth activity report, which covers the period from 1 January to 31 December 2017. The report states that

OLAF concentrated on large, transnational investigations, which often led to multi-million euro financial recommendations. OLAF's performance in 2016 is expressed in the following figures:

- 219 new investigations opened;
- 272 investigations concluded;
- 342 recommendations issued to the EU and Member States' authorities;
- Recovery of €631 million recommended;
- Duration of investigations reduced to 18.9 months in average – a new record for the Office.

For the first time, the OLAF report also presents the most striking trends in fraud with EU funds. The analysis concludes, *inter alia*, the following:

- Public procurement is still an attractive marketplace for fraudsters, who use corruption and off-shore accounts as fraud facilitators;
- Many procurement fraud cases are transnational;
- Research and employment grants constitute a lucrative fraud business, with double-funding and employment subsidy fraud becoming increasingly popular;
- Criminal networks use complex transnational schemes to evade customs duties;
- The nature of cigarette smuggling has significantly changed in the past years, with smugglers turning their attention to trafficking “cheap whites” or non-brand-ed cigarettes.

The annual report also gives several examples, which show that OLAF is a hub for innovation in investigative techniques and tools.

In the legislative field, OLAF supported the Commission in two important policy initiatives in 2016. The first is the inclusion of serious VAT offences within the scope of the new PIF Directive (see also eucrim 4/2016, p. 158). The second is the establishment of the European Public Prosecutor's Office under enhanced cooperation (see also below under “Protection of Financial Interests”).

The report also contains an assess-

## Report

### Renforce Researchers Conclude a Comprehensive Comparative Report on the Investigative Powers of the European Anti-Fraud Service, OLAF

Under the auspices of RENFORCE, an international team of researchers has recently concluded a report on the ‘Investigatory powers and procedural safeguards: Improving OLAF's legislative framework through a comparison with other EU law enforcement authorities.’ The project was co-funded under the Hercule III Programme of the European Commission/OLAF. Headed by Prof. Michiel Luchtman and Prof. John Vervaele, it analyses OLAF's legal framework for the gathering of information and evidence.

The results of the project reveals *inter alia* significant deviations between the legal framework for OLAF and other EU bodies with comparable tasks (European Competition Network/ECN, the European Central Bank/ECB, and the European Securities and Markets Authority/ESMA). These differences highlight shortcomings in the OLAF legal framework, particularly when it comes to its powers of investigation, but also relating to the legal protection of the individuals concerned.

The project uses a comparative approach in which the interaction between the four above-mentioned authorities and their national partners in six legal orders (Germany, the Netherlands, France, Italy, Poland, and the United Kingdom) are analyzed. The report includes findings on each of the four EU authorities individually and in comparison, six national reports, and an overall comparative analysis. The results are relevant for policymakers and legislative bodies at the EU and national levels, for academics and practitioners in the area of enforcement of EU law, and for training purposes.

Renforce researchers Michiel Luchtman, John Vervaele, Mira Scholten, Michele Simonato, Joske Graat, and Danielle Arnold carried out the project together with Prof. Martin Böse and Dr. Anne Schneider (both University of Bonn), Prof. Peter Alldridge (Queen Mary, University of London), Prof. Juliette Tricot (Université Paris Ouest Nanterre La Défense, Paris), Prof. Silvia Allegranza, Prof. Katalin Ligeti and Dr. Gavin Robinson (all University of Luxembourg), and Dr. Celina Nowak (Kozminski University, Warsaw).

The report is related to several other RENFORCE projects, including the VIDJ project led by Prof. Michiel Luchtman and the VENI project coordinated by Dr. Mira Scholten, funded by the Dutch Council of Scientific Research. A second project funded under the Hercule III programme is currently in progress and under the direction of Dr. Michele Simonato, Prof. Michiel Luchtman, and Prof. John Vervaele.

*Prof. Michiel Luchtman, University of Utrecht*

ment of OLAF's work over the past year as well as a vision for OLAF's future. They are presented by OLAF Director *Giovanni Kessler* who is now in the last year of his mandate. (TW).

►eucrim ID=1702014

### Global Anti-Counterfeiting Award for OLAF

OLAF was honoured with the Global Anti-Counterfeiting Awards in the category “International Public Body.” The ceremony took place in Paris on 7 June 2017, on the World Anti-Counterfeiting Day. OLAF received the award for its successful achievements in tackling counterfeiting and piracy. Past investiga-

tions involved the recovery of millions of counterfeit goods, such as pharmaceuticals, spare auto parts (e.g., airbags, brakes, ball bearings), and – significantly – pesticides. Shortly before receiving the award, OLAF announced that its operations helped seize 20 tons of fake detergents by customs authorities.

The Global Anti-Counterfeiting Awards are judged annually and are made as a continuing recognition of special achievements by organisations, companies, and individuals. The awards are sponsored by the Global Anti-Counterfeiting Group and Managing Intellectual Property. (TW)

►eucrim ID=1702015

## Europol

### New Europol Regulation

On 1 May 2017, Regulation (EU) 2016/794 of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA entered into force (see also eucrim 1/2016, p. 6; eucrim 2/2013, pp. 36-37; and eucrim 2/2014, p. 49), which took effect in all EU Member States.

Novelties under the new regulation include the following:

- An enhanced mandate;
- New powers to act as the EU's information hub in the fight against terrorism and serious organised crime;
- Clear rules for existing units or centres, such as the European Counter Terrorism Centre (ECTC) and the European Union Internet Referral Unit (EU IRU);
- Increased data protection safeguards, including supervision by the European Data Protection Supervisor as of 1 May 2017;
- Democratic control and parliamentary scrutiny. (CR)

►eucrim ID=1702016

### Agreement with China

On 19 April 2017, Europol and the People's Republic of China signed a strategic cooperation agreement allowing for the exchange of general strategic intelligence. The agreement also allows for the exchange of strategic and technical information as well as operational information (with the exception of personal data). (CR)

►eucrim ID=1702017

### Agreement with Brazil

On 11 April 2017, Europol and Brazil signed a Strategic Cooperation Agreement allowing for the exchange of general strategic intelligence. The agreement also allows for the exchange of strategic and technical information as

well as operational information (with the exception of personal data). Furthermore, a Brazilian liaison officer will be seconded to Europol. (CR)

►eucrim ID=1702018

### Agreement with Georgia

On 4 April 2017, Europol and Georgia signed an Agreement on Operational and Strategic Cooperation. The agreement allows for the exchange of information, including personal data of suspected criminals, and the joint planning of operational activities. Furthermore, Georgia will designate a national contact point to act as the central point of contact between Europol and the competent authorities in Georgia. (CR)

►eucrim ID=1702019

### Worldwide Operation Dragon

52 countries – including EU Member States, Frontex, Eurojust, and the European Commission as well as third countries from all over the world – joined forces with Europol to operate a series of joint action days targeting serious international and organised crime. Europol provided operational support for law enforcement officers working on the ground from a coordination centre at its headquarters in The Hague. Operation “Dragon” has already led to the detention of 153 individuals suspected of using airline tickets purchased with stolen, compromised, or fake credit card details. Operation “Dragon” follows other joint action days, which took place in 2014, 2015, and 2016. (CR)

►eucrim ID=1702020

### Public Webpage “Stop child abuse, trace an object”

On 31 May 2017, Europol launched a new initiative to combat child abuse. By means of a dedicated webpage, objects featured in the backgrounds of child abuse images, e.g., shampoo bottles, are displayed in order to appeal to the general public to see whether they recognise these objects. Citizens submit information anonymously. Once the origin of an

object is identified, Europol informs the competent law enforcement authority of the involved country so that it may further investigate this lead and hopefully speed up the identification of both the offender and the victim.

The images on the dedicated webpage will change periodically. (CR)

►eucrim ID=1702021

### Operation Pacifier

On 5 May 2017, Europol reported on an important operation that led to the crack-down on a major website of child sexual abuse in the Darknet. “Operation Pacifier” led to the conviction of 30 years of imprisonment of the lead administrators of one of the world's largest child sexual abuse websites, Playpen. The FBI and US Department of Justice – with the support of Europol and many other law enforcement agencies worldwide – launched Operation Pacifier in January 2015 in order to track down Playpen's members.

As a result, so far 368 persons have been arrested or convicted in Europe and 870 worldwide. Furthermore, at least 259 sexually abused children were able to be identified or rescued from their abusers outside of the US. Europol stated that Operation Pacifier was one of the largest and most challenging ever in the fight against online child sexual exploitation because of the size of the data seized and its presence on the Darknet. (CR)

►eucrim ID=1702022

### Darknet Dealer of Drugs and Firearms Arrested

With the support of Europol, at the beginning of May, Slovak authorities were able to arrest a Slovak national trading in firearms, ammunition, and drugs on the Darknet. Five firearms, approx. 600 rounds of ammunition, 58 cannabis plants, and a Bitcoin wallet containing bitcoins worth €203,000 were able to be seized and an online drug marketplace dismantled. (CR)

►eucrim ID=1702023

## European People's Party Merit Award

On 30 March 2017, Europol was awarded the European People's Party (EPP) Merit Award. According to the EPP, the award is granted to individuals or organisations that have made an outstanding contribution to promoting the values and principles which the EPP family stands for. (CR)

► [eucrim ID=1702024](#)

## Eurojust

### Annual Report 2016

Eurojust published its annual report for the year 2016. The six main chapters of the report focus on:

- Eurojust at work;
- Eurojust's casework;
- Eurojust's partners;
- Challenges and best practices;
- Eurojust's administration;
- Cooperation with practitioners' networks.

Compared to the previous year, the number of cases dealt with at Eurojust increased by 4%, from 2214 in 2015 to 2306 in 2016.

The number of coordination meetings held in 2016 decreased to 249, compared to 274 in 2015. Consequently, the participation of Europol, OLAF as well as third states at coordination meetings decreased in comparison to the previous year. Furthermore, the number of coordination centres held in 2016 dropped to 10 (compared to 13 held in 2015).

Eurojust was involved in 148 JITs – a 23% increase over 2015. 90 JITs were financially supported by Eurojust in 2016, compared to 68 in 2015.

Looking at the EAW, Eurojust's assistance was requested on 315 occasions, compared to 292 in 2015.

Areas of crime in which Eurojust's casework increased included terrorism, IIS, THB, fraud, and money laundering.

In 2016, a Memorandum of Understanding with the European Union Intellectual Property Office (EUIPO) and co-

operation agreements with Montenegro and Ukraine were signed. Eurojust's network of judicial contact points in third states was extended to a total of 41 third states.

Furthermore, in 2016, Eurojust organised several strategic and tactical meetings, on terrorism, cybercrime, and illegal immigrant smuggling. The agency also produced several handbooks, reports, and analyses as well as an update of the decision-making guideline "Which jurisdiction should prosecute?"

Eurojust's budget for 2016 increased to €43.539 million in comparison to €33,818 million in 2015. Budget implementation was 99.89 per cent. (CR)

► [eucrim ID=1702025](#)

## Frontex

### Annual Report of the Consultative Forum on Fundamental Rights Published

On 12 May 2017, the Frontex Consultative Forum on Fundamental Rights published its annual report for the year 2016 in which it mainly focused on the development and implementation of the agency's new mandate. In this context, the Consultative Forum reflected, for instance, on the following:

- The establishment of a Frontex individual complaints mechanism and a European pool of forced return monitors;
- The agency's extended mandate in third countries;
- Recommendations concerning, for instance, Frontex operational activities at the Hungarian-Serbian border.

The forum also contributed to the revision of Frontex' fundamental rights strategy. Furthermore, members of the Consultative Forum visited Frontex operations in Greece. (CR)

► [eucrim ID=1702026](#)

### Cooperation with EFCA and EMSA

In June 2017, the 18-month pilot project "Creation of a European coast-

guard function" came to an end. Within the framework of the project, Frontex, the European Maritime Safety Agency (EMSA), and the European Fisheries Control Agency (EFCA) explored ways to further develop their cooperation with regard to:

- The sharing of information generated by fusing and analysing vessel movement and earth observation data;
- Providing surveillance and communication services based on state-of-the-art technology;
- Capacity building;
- Capacity sharing, including multipurpose operations and the sharing of assets and capabilities across sectors and borders.

In March 2017, the three agencies had also signed a Tripartite Working Arrangement intensifying their cooperation on coastguard functions. (CR)

► [eucrim ID=1702027](#)

### Testing Coastguard Functions

In May 2017, representatives from 20 European countries with sea borders – together with Frontex, EFCA, and EMSA – met for a three-day exercise to find the best ways of working together by testing different coast guard functions; e.g.:

- Detecting migrants;
- Search and rescue;
- Medical evacuation;
- Response to pollution;
- Response to illegal fishing;
- Boarding of a ferry transporting a dangerous person;
- Seizure of drugs;
- Arresting traffickers. (CR)

► [eucrim ID=1702028](#)

### First Ship with Multinational Crew

On 20 April 2017, the first ship with a multinational crew taking part in a Frontex operation embarked to patrol the Greek external maritime borders. The operation aims to contribute to border control activities and to increase search and rescue capacity in the area. The 31-member crew includes officers from



border and coast guard authorities of seven EU member states with expertise in various coast guard functions.

The introduction of a multinational crew in sea operations is part of the agency's strategy to increase its role in implementing European coast guard functions and in providing assistance to member states at their external borders. (CR)

➤ [eucrim ID=1702029](#)

### Regional Support for Protection-Sensitive Migration Management in the Western Balkans and Turkey

In April 2017, representatives met to evaluate the Regional Support to Protection-Sensitive Migration Management in the Western Balkans and Turkey (IP-AII) project. The representatives were from six Western Balkan countries, the European Commission, Frontex, the European Asylum Support Office (EASO), the International Organisation for Migration (IOM), and UNHCR. IPAAI was launched in January 2016, with the aim of introducing and sharing EU standards and best practices on migration management. To date, Frontex and EASO have trained 123 border guards and asylum officers from Western Balkan countries (with the support of IOM and UNHCR) as well as organised ten workshops on identification and referral mechanisms. (CR)

➤ [eucrim ID=1702030](#)

### AFIC Joint Report 2016

On 6 April 2017, Frontex published the Africa-Frontex Intelligence Community (AFIC) Joint Report 2016. The report analyses the irregular migratory movements affecting AFIC countries and EU Member States as well as cross-border criminality. It also provides an overview of the main regional security threats affecting the countries in the community. Furthermore, it presents a picture of the smuggling networks in Africa.

According to the report, there is a stable trend regarding the interception of irregular migrants in the Central Medi-

terranean: approx. 117,000 irregular migrants were intercepted between 1 January and 31 August 2016, compared to around 116,000 migrants intercepted during the same period in 2015. Looking at the Western Mediterranean, detections of illegal border-crossings at the sea route increased by almost 55% in 2016, while detections of illegal border-crossings at the land borders decreased by 43%. (CR)

➤ [eucrim ID=1702031](#)

### Agency for Fundamental Rights (FRA)

#### FRA and EDPS Tie Up Cooperation

On 30 March 2017, the European Data Protection Supervisor and the FRA concluded a Memorandum of Understanding (MoU) fostering increased cooperation by the two EU bodies involved in the protection of the EU fundamental rights law. The MoU's purpose is for the EDPS and FRA to cooperate more in relevant areas. It aims to establish, define, encourage, and improve their cooperation in accordance with and subject to their respective statutory duties under EU law.

The main content of the MoU is that the EDPS and the FRA establish a single contact point responsible for coordinating their cooperation and for consulting on another on a regular basis. Furthermore, both institutions are to meet regularly in order to exchange views on the main upcoming challenges for fundamental rights and to exchange information, including the preparation of common strategic documents, such as working programmes or action plans.

By means of the MoU, the EDPS and the FRA will support each other in cooperating more closely as regards their research and consultative roles at the EU level. In this context, the EDPS and the FRA agree, for instance, to collaborate on collecting, recording, and analysing information and data relevant to their areas of cooperation. (TW)

➤ [eucrim ID=1702032](#)

### FRA Joins Human Rights Network AHRI

The FRA joined the Association of Human Rights Institutions (AHRI) on the occasion of AHRI's annual conference in Leuven on 27 April 2017.

AHRI is a network of 62 member institutions from 33 different countries that carries out research and educational activities in the field of human rights. The objective of the network is to bring together human rights researchers from across several disciplines, to facilitate the exchange of ideas and collaboration, and to promote research, education, and discussion in the field of human rights. AHRI is supportive of PhD researchers and facilitates the productive exchange between the different member institutions.

AHRI also organises annual conferences. This year's conference in Leuven focused on "The Promotion and Enforcement of Human Rights by International and Regional Organizations: Achievements, Challenges and Opportunities." (TW)

➤ [eucrim ID=1702033](#)

## Specific Areas of Crime / Substantive Criminal Law

### Protection of Financial Interests

#### PIF Directive Adopted

On 5 July 2017, the European Parliament formally adopted (at second reading) the proposed Directive of the European Parliament and of the Council on the fight against fraud to the EU's financial interests by means of criminal law. After having reached a compromise (see [eucrim 1/2017](#), p. 13), the EP accepted the Council's first reading position without amendments. The legislative procedure is now complete. The Directive was published in the Official Journal L 198 of 28 July 2017, p. 29.

Member States must adopt and pub-



lish, by 6 July 2019, the laws, regulations and administrative provisions necessary to comply with the Directive. The Commission is called on to submit an implementation report by 6 July 2021. For further information on the new PIF Directive, see the contribution of *Adam Juszcak* and *Elisa Sason* in this issue. (TW)

►eucrim ID=1702034

### JHA Ministers Agree on Details of EPPO Regulation

On 8 June 2017, the Justice and Home Affairs Ministers of 20 EU Member States which meanwhile are part of the enhanced cooperation to create the European Public Prosecution's Office (EPPO) agreed on a general approach to the legislative text. After the initial notification by 16 EU Member States, which expressed their willingness to set up the EPPO under the procedure of enhanced cooperation (see also eucrim 1/2017, p. 12), four more Member States joined or expressed their intention to join the enhanced cooperation (i.e., Estonia, Latvia, Italy, and Austria).

Regarding the functioning and competence of the EPPO, the draft legislation maintains the approach followed in January 2017. The EPPO will work as a collegial structure composed of two levels:

- The central level will consist of a European chief prosecutor, who will have overall responsibility for the office and who is the head of the College of European Prosecutors, Permanent Chambers, and European Prosecutors.
- The decentralised level will be made up of European delegated prosecutors located in the Member States; they will be in charge of the day-to-day operation of criminal investigations and prosecutions in line with the regulation and legislation of that Member State.

The main task of the central level is to monitor, direct, and supervise all investigations and prosecutions undertaken by the delegated prosecutors, thereby ensuring a consistent investigation and

prosecution policy across Europe. The material competence of the EPPO will be basically linked to the criminal offences as provided for in the new PIF Directive.

Open issues that were discussed after the transfer of the legislative proceedings into the enhanced cooperation scheme were, above all, cooperation with those EU Member States not taking part in the enhanced cooperation and financing of the EPPO.

After having agreed on the general approach, the draft text of the EPPO regulation was revised by lawyer-linguists, and a consolidated version languages was made available in the EU official: Council doc. 9941/17 of 30 June 2017.

The European Parliament now needs to give its consent. Since the establishment of the EPPO follows the “consent procedure,” the EP has the power to accept or reject the legislative proposal by an absolute majority vote, but it cannot amend it. The EP is expected to take its decision before the summer break so that the legislation can be finalised in October 2017.

The EPPO central office will be based in Luxembourg. The date on which the EPPO will assume its investigative and prosecutorial tasks will be set by the Commission on the basis of a proposal from the European Chief Prosecutor. The EPPO is not expected to be operational before 2020. (TW)

►eucrim ID=1702035

### European Court of Auditors Audits Fraud Prevention and Fraud Responses

Since the figures for fraud against the EU budget are alarming and – based on Eurobarometer surveys – the perception of fraud and corruption affecting the EU budget by EU citizens is increasing, the European Court of Auditors announced on 13 June 2017 that it is preparing an audit of how the European Commission manages the risk of fraud in EU spending. The audit will focus on both fraud prevention and fraud response. It above all intends to analyse the weaknesses in

how fraud is detected and reported at the level of the Commission and at the level of the Member States. The audit will also involve NGOs, academics, and prosecutors as well as Europol and Eurojust. The report is expected to be available in 2018. (TW)

►eucrim ID=1702036

### AG Gives Opinion on Effective Prosecution of PIF Offences and Defence Rights

On 4 April 2017, Advocate General (AG) *Yves Bot* delivered his opinion in Case C-612/15 (criminal proceedings against *Nikolay Kolev*, *Stefan Kostadinov*). The CJEU had been asked by a Bulgarian criminal court to rule on the conformity of specific issues of Bulgarian criminal procedure in conjunction with EU law. The questions arose in the context of PIF-related offenses, since the defendants in the main proceedings, *Mr. Kolev* and *Mr. Kostadinov*, had been accused of having accepted bribes for non-performance of customs inspections in their capacity as customs officers at the border between Bulgaria and Turkey.

The Bulgarian criminal court referred more than 20 questions to the CJEU, which concerned the consequences of the termination of proceedings regarding violation of the right to a speedy trial, the time at which the accused person must be informed of the accusation, the time at which that person or his lawyer must have access to the case file documents, and the conditions of removal of defence lawyers.

The AG reformulated the questions, categorised them into three sets, and answered as follows:

- Art. 325 TFEU and the PIF Convention of 26 July 1995, laying down the obligations of EU Member States to counter fraud and other illegal activities affecting the EU's financial interests, preclude national law provisions (e.g., Arts. 368 and 369 of the Bulgarian Code of Criminal Procedure), which – in a very stringent and formalistic way – require national courts to terminate

criminal proceedings if the prosecution service failed to comply with certain pre-determined time limits to conclude pre-trial investigations, even if the delay was caused by deliberate obstruction attributable to the defendant. Although the Bulgarian legislation was created such to comply with ECtHR case law (which repeatedly blamed Bulgaria for having infringed the “reasonable time” principle of Art. 6 ECHR), the AG emphasised that the Member State’s EU obligations to effectively protect the EU’s financial interests lead to disapplying national law provisions that prevent the Member States from fulfilling their EU obligations.

■ The second set of questions concerned the precise time in the proceedings at which the obligations incumbent from Art. 6 para. 3 and Art. 7 para. 3 of Directive 2012/13/EU, i.e., the right to

information about the accusation and access to the case materials, must be fulfilled. The AG found that EU law (Art. 6 para 3 Directive 2012/13) does not preclude national practice that provides for notification of the accused person of information on the accusation after the indictment has been submitted to the court, under the condition that the accused person has reasonable time to discuss the evidence against him during the hearing. Likewise, Art. 7 para. 3 Directive 2012/13 does not preclude national practice providing for access to the case materials to be granted, at the request of the parties, during the pre-trial investigation and before the final indictment is drawn up. In this case, the national court must ensure that the accused person or his lawyer can have effective access to these materials in order to enable them to prepare an effective defence.

■ As to the right to freely choose one’s lawyer, the AG concluded that Art. 3 para. 1 of Directive 2013/48/EU on the right of access to a lawyer does not preclude national legislation, such as the legislation at issue, which provides that the national court is required to exclude from its proceedings the lawyer of a defendant who is representing or has represented another defendant if the defence of one of the defendants conflicts with that of the other and which provides that the court must appoint new defence lawyers to represent those defendants.

On the latter point, it is interesting that the AG affirmed the applicability of Directive 2013/48/EU, although the implementation period was not yet over at the time of reference to a preliminary ruling. As far as can be seen, this is the first time that Directive 2013/48 on the right of access to a lawyer has played a key role in a preliminary reference proceeding before the CJEU. (TW)

►eucrim ID=1702037

## Annual Forum on Combating Corruption in the EU 2017

*European and Member States’ anti-fraud strategies (prevention, detection and investigation techniques) to protect the EU’s financial interests*

Trier, 21–22 September 2017

The 2017 “Annual Forum on Combating Corruption” – organised by the Academy of European Law (ERA) and co-financed by the European Commission (OLAF) under the Hercule III Programme – will deal with European and Member States’ anti-fraud strategies (prevention, detection and investigation techniques) to protect the EU’s financial interests better. It is linked to the overall objective of the OLAF Anti-Fraud Strategy, i.e. to improve the prevention, detection and conditions for investigations of fraud whilst achieving an adequate level of reparation and deterrence. This annual forum will discuss and exchange ideas on the fight against fraud in the EU from a practical perspective. Panel discussions will debate the operative challenges in investigating and prosecuting fraud and in recovering money unduly paid from the EU budget.

Key topics are:

- Overview of the European legal framework for fighting fraud and protecting the EU’s financial interests;
- Role and powers of OLAF, Eurojust, the European Parliament and the United Nations;
- Improving fraud prevention, detection and investigation techniques in Member States
- Recovering proportions of funds lost due to fraud;
- Deterring future fraud through appropriate penalties;
- Work carried out by the private sector and by the European Court of Auditors (ECA) and European Investment Bank (EIB)

The conference is addressed to judges, prosecutors, government officials, in-house counsel, lawyers in private practice and other stakeholders. It will be held in English.

For further information, please contact Mr. Laviero Buono, Head of Section – Criminal Law, ERA, e-mail: lbuono@era.int. The programme is available via ERA’s website: [www.era.int](http://www.era.int)

## Money Laundering

### Commission’s Risk Assessment Report on Money Laundering

On 26 June 2017, the day on which Member States had to bring into force the laws, regulations, and administrative provisions necessary to comply with the Fourth Anti-Money Laundering Directive (2015/849), the Commission published its first “Supranational Risk Assessment Report” (SNRA Report).

The report is an assessment of the risks of money laundering and terrorist financing affecting the internal market and relating to cross-border activities. Art. 6 of said Directive requires this and is also a deliverable of the European Security Agenda (COM(2015) 185 final) and the Action Plan on Terrorist Financing (COM(2016) 50 final).

The SNRA aims at identifying the vulnerabilities of financial products and services to risks of money laundering and terrorist financing, both in terms of

## The 4th and Upcoming 5th EU Anti-Money Laundering Directives

Trier, 16–17 November 2017

This seminar – organized by the Academy of European Law (ERA) – deals with the practical impact of the new EU anti-money laundering framework. It will explain the current European anti-money laundering landscape and focus on the challenges and changes arising from the transposition of the fourth Anti-Money Laundering (AML) Directive as well as the novelties brought by the upcoming fifth Directive.

Key topics are:

- The latest AML/FAFT trends
- Practical changes for the financial sector in the 4th and upcoming 5th AML Directives
- Innovations regarding due diligence on customers
- Challenges related to beneficial ownership information
- Novelties regarding politically exposed persons (PEP)
- Risk assessment and its technological dimension
- The EU Supranational Risk Assessment Report
- The Commission's new roadmap regarding a new methodology to assess high risk third countries under the 4th AML Directive
- Building effective transaction monitoring
- Data protection in the context of AML
- Tackling terrorism financing especially with regard to virtual currencies and prepaid cards
- Combating predicate offences: the European Commission's anti-tax-avoidance package
- Countering money laundering by a criminal law Directive

The conference is mainly addressed to anti-money laundering officers, compliance officers, lawyers in private practice, in-house counsel, notaries, government officials, professionals in the gambling sector, and other stakeholders working in the financial services sector. It will be held in English.

For further information, please contact: Cornelia Riehle, Course Director – Criminal Law, ERA, e-mail: [criehle@era.int](mailto:criehle@era.int). The programme is available via ERA's website at: [www.era.int](http://www.era.int)

legal framework and effective application.

This report is structured as follows:

- Presentation of the main risks for the internal market in a wide range of sectors;
- Presentation of the horizontal vulnerabilities that can affect such sectors;
- Mitigating measures that should be pursued at the EU and national levels to address these risks;
- Recommendations for the different actors involved in the fight against ML and TF, including the European Supervisory Authorities, the non-financial supervisors and the EU Member States.

The SNRA concludes that the EU internal market is still vulnerable to money laundering and terrorist financing risks. According to the report, terrorists use a wide range of methods to raise

and move funds; criminals employ more complex schemes and take advantage of new opportunities to launder money that have become available through new services and products.

The SNRA report is complemented by an annex providing a factual overview of the risk analysis and describing the methodology used. It also contains a staff working paper with a very detailed analysis of the specific products and services that are delivered in the various financial sectors as well as a staff working document on improving cooperation between EU Financial Intelligence Units (FIUs).

The Commission will further monitor the implementation of the recommendations made to the EU Member States. It will continue to review the development of money laundering and terrorist

financing risks. A new risk assessment will be presented by June 2019 at the latest. (TW)

► [eucrim ID=1702038](#)

## Council Adopts Negotiating Position on New Directive to Counter Money Laundering

At its meeting on 8/9 June 2017, the JHA Council agreed on its position for negotiations with the EP as regards the proposed rules to counter money laundering by criminal law. For the underlying Commission proposal of 21 December 2016 (COM(2016) 826 final), see [eucrim 4/2016](#), p. 159.

The main objectives of the proposed directive are to establish minimum rules concerning the definition of criminal offences and put in place sanctions relating to money laundering as well as to remove obstacles to cross-border judicial and police cooperation.

Discussion at the Council mainly concerned the following issues:

- Scope of the definition of a “criminal activity” as a predicate offence of money laundering; in this context, the Council agreed that cybercrime should be also added to the definition of criminal activity;
- Introduction of a criminalisation obligation for self-laundering;
- Link to the PIF directive, which provides specific rules addressing the money laundering of property derived from PIF offences; here, the Council favours Member States transposing these rules through a single comprehensive framework on money laundering at the national level.

Negotiations between the Council and the EP will continue as soon as the latter sets up its position. (TW)

► [eucrim ID=1702039](#)

## CCBE Critical on New Anti-Money Laundering Proposal

In a statement released on 6 April 2017, the Council of Bars and Law Societies of Europe (CCBE) criticised the Commission's proposal for countering

money laundering by criminal law (see also news item above with further references).

The CCBE believes that the proposal will not reach its objective, i.e., of minimising the differences in national criminal law legislation on countering money laundering. According to the statement, one reason for this is that the proposal in essence refers to the existing international legal framework (Council of Europe Warsaw Convention and FATF Recommendations).

In addition, the CCBE remarks that, in many aspects, the current proposal of the Commission goes beyond FATF Recommendations, in particular as regards the predicate offences, which may not be justified in terms of necessity and proportionality. The CCBE recommends at least reducing the list of predicate offences to activities which a) are serious crimes and b) may generate criminal property.

The CCBE is also very critical as regards the criminalisation of self-money laundering because it infringes the *ne bis in idem* principle and affects the right not to incriminate oneself.

Ultimately, the CCBE statement concludes that the impact of the provisions of the proposed Directive on fundamental rights and proportionality requirements have not been sufficiently assessed yet and urges the Commission, the Council, and the European Parliament to seriously review the need for and the consequences of any such type of anti-money laundering legislation.

It is furthermore worth noting that, in April and May 2017, the General Courts of Spain, the Czech Senate, and the Czech Chamber of Deputies also submitted statements that include some critical remarks on the Commission proposal. (TW)

►eucrim ID=1702040

### MEPs Reject Blacklist of Countries at Risk of Money Laundering

By vote of 17 May 2017, the majority of MEPs rejected an act of the Commis-

sion blacklisting non-EU countries at high risk of money laundering (see also eucrim 2/2016, p. 73 for the blacklist).

The EP wants a more expansive and wide-ranging blacklist. MEPs noted that the Commission's list of 24 March 2017 is largely a duplicate of the one from FATF. They argued that the Commission should develop an autonomous evaluation process instead of relying on FATF sources to judge whether countries are at high risk of money laundering. Furthermore, MEPs admonished that the Commission has not sufficiently recognised the offences of the fourth Anti-Money Laundering Directive, in particular tax crimes, when identifying listing criteria.

Lastly, the EP called upon the Commission to draw up a new delegated act in order to take into account the EP's recommendation to adopt a roadmap for an autonomous evaluation process.

The list is aimed at people and legal entities from blacklisted countries who will face tougher than usual checks when doing business in the EU. (TW)

►eucrim ID=1702041

### CJEU: Obligation to Declare Cash in International Transit Areas of EU Airports

According to Regulation (EC) 1889/2005, any natural person entering or leaving the EU and carrying cash of a value of €10,000 or more must declare that sum to the customs authorities. According to a judgment of 4 May 2017, upon reference for a preliminary ruling by the French *Cour de Cassation*, the CJEU clarified that this obligation also applies to a person travelling from a non-EU State to another non-EU State and transiting through an airport located within the territory of the EU.

The Court points out that the notion of "entering the EU" refers to the movement of a natural person from a territory which is not part of the EU to a territory which is part of that territory. Next, the Court states that the airports of the EU Member States are part of the territory of the EU and that neither the Regula-

tion nor other EU law foresees exceptions.

The Court adds that the finding that any person is obliged to declare also in the international transit areas of airports located in the EU is in addition consistent with the Regulations' objective, i.e. to avoid the introduction of illicit money into the financial system and the investment of that money after laundering. The Court argues that the obligation to declare any sum greater than €10,000 should be given a broad meaning; otherwise the effectiveness of the control system for cash entering or leaving the EU would be jeopardized.

In the case at issue, a passenger travelled from Benin to Lebanon, with a stop-over in a French airport at which customs authorities detected that he was in possession of \$1,607,650 (approx. €1.5 million) in cash. The case reference is C-17/16, *Oussama El Dakkak and Intercontinental SARL v Administration des douanes et droits indirects*. (TW)

►eucrim ID=1702042

### Tax Evasion

#### Commission Wants Tax Advisors to Disclose Tax Plans

Among the phalanx of measures to fight tax evasion and avoidance in the EU (for the strategy, see eucrim 2/2016, p. 74), the Commission added another item with a proposal to enhance transparency rules for intermediaries (law firms, accounting firms, trust companies, banks, etc.) involved in the designing and marketing of aggressive tax arrangements. The legislative proposal of 21 June 2017, which would amend Directive 2011/16/EU "as regards mandatory automatic exchange of information in the field of taxation in relation to reportable cross-border arrangements" aims at countering the central role of intermediaries in creating and selling tax avoidance schemes (as revealed by the media leaks on the Panama Papers). Tax authorities would receive information about such schemes



at an early stage in order to perform risk assessments. Ultimately, the goal of the new EU legislation is to establish a mechanism that deters intermediaries from designing and marketing arrangements that help reduce the tax burden of individuals or companies.

The main features of the proposal are as follows:

- Intermediaries who design or promote tax planning arrangements (e.g., tax and financial advisors, banks, consultants, lawyers, accountants) are obligated to report an arrangement if it bears any features or “hallmarks” defined in the proposed Directive;
- The obligation is limited to cross-border situations, i.e., situations in either more than one Member State or a Member State and a third country;
- The report must be made to the intermediaries’ tax authorities within five days of making such an arrangement for their client;
- Member States must put in place effective, proportionate, and dissuasive penalties for intermediaries who do not respect the reporting requirements;
- Disclosed information must be exchanged automatically among national tax authorities through a centralised database, thus enabling all Member States to scrutinise arrangements and become aware of new risks of tax avoidance.

At the run-up to the Commission proposal, European lawyers’ associations already called for due consideration of the legal privileges of professions. The Directive takes into account this demand by providing that the burden of disclosure is shifted to the taxpayer (i.e., individual or company) if the intermediary is bound by professional privilege or secrecy rules. In addition, the EU-based taxpayer is obliged to supply the information if the intermediary providing for the cross-border scheme is not located in the EU or does not exist because the scheme was developed by in-house tax consultants or lawyers.

Next steps: Since the proposal is based on Art. 115 TFEU it is subject to

the special legislative procedure, i.e., the Directive must be unanimously adopted in the Council after consulting the European Parliament and the Economic and Social Committee. (TW)

►eucrim ID=1702043

### Studies Shed Light on Roles of Advisors/Intermediaries in Panama Paper Scandal

The EP Policy Department A published two studies on the roles of tax advisors and intermediaries in offshore tax avoidance schemes (as revealed by the media leaked Panama Papers). The studies were requested by the EP’s inquiry committee “into money laundering, tax avoidance and tax evasion” (PANA, see also eucrim 2/2017, p. 74). Both studies were completed in April 2017.

The first study assesses the role of advisors (tax experts, legal experts, administrators, investment advisors) and intermediaries (law firms, accounting firms, trust companies, banks, etc.) involved in the identified decision-making cycle of offshore tax avoidance schemes (advice, creation, maintenance, enforcement). The study also formulates policy recommendations for actions to discourage advisors and intermediaries from facilitating money laundering and tax avoidance/evasion through offshore structures. The recommendations include, for instance:

- Strengthening independence and responsibility as well as obligatory reporting of tax avoidance schemes vis-à-vis advisors and intermediaries who are covered by EU law;
- Increasing pressure on offshore jurisdictions by, *inter alia*, gradually extending AML/CFT standards to tax evasion/avoidance and hiding/shielding;
- Better implementing and ensuring compliance with and enforcement of AML/CFT standards;
- More efficiently exchanging financial information on ultimate beneficiary owners of offshore entities.

The second study maps the rules on independence and responsibility appli-

cable at national, EU, and international levels, which govern the service provided by intermediaries (companies working in auditing, tax advice, accountancy, and account certification) or by legal advisors (attorneys, solicitors, legal consultants, in-house lawyers, etc.). As far as the national level is concerned, the study covers professional obligations, rules, and enforcement provisions in seven jurisdictions, i.e., United Kingdom, Germany, Luxembourg, Cyprus, Switzerland, the British Virgin Islands, and the United States of America.

After having critically analyzed the rules in place and their efficacy, the study formulates several policy recommendations on how to encourage tax advisors, lawyers, and other intermediaries to contribute positively to tax evasion/avoidance and anti-money laundering. (TW)

►eucrim ID=1702044

### Coordination Meeting on “Mossack Fonseca Papers” at Eurojust

In order to exchange information on the various ongoing investigations of alleged criminal activities connected to the law firm Mossack Fonseca, a second coordination meeting was held at Eurojust on 3 and 4 April 2017. The meeting brought together the national members of Germany and Italy at Eurojust, the General Prosecutor of Panama, and representatives of the competent investigating authorities of Belgium, Bulgaria, the Czech Republic, Germany, Greece, Spain, France, Italy, Latvia, the Netherlands, Poland, Portugal, Sweden, the UK, and Norway. (CR)

►eucrim ID=1702045

### Counterfeiting & Piracy

#### 2017 Report on Counterfeiting and Piracy in the EU

On 22 June 2017, Europol and the European Union Intellectual Property Office (EUIPO) released their situation report on counterfeiting and piracy in the EU.



It builds upon the previous 2015 report, tracks the evolution of counterfeiting and piracy in the EU, updated the key conclusions and offers new insights into some emerging trends.

The report looks at the extent of the following problems of counterfeit goods and piracy in the EU:

- Key product sectors;
- Key countries of provenance;
- Smuggling routes and transportation methods;
- Criminal networks and infrastructures;
- Challenges in fighting product counterfeiting and piracy;
- Threats of piracy and other online infringements.

The report *inter alia* concludes that IPR crime remains one of the most lucrative criminal enterprises, and it is frequently closely linked to other serious crime. As a result, only total cooperation between all stakeholders can efficiently tackle this criminal phenomenon. (CR)

►eucrim ID=1702046

### Fake Food and Beverages Seized

9800 tonnes, over 26.4 million litres, and 13 million units/items of potentially harmful food and beverages worth an estimated €230 million were seized in Operation OPSON VI conducted between 1 December 2016 and 31 March 2017. 61 countries involving police, customs, national food regulatory bodies, and partners from the private sector took part in the successful operation led by Europol and Interpol. (CR)

►eucrim ID=1702047

## Terrorism

### Directive on Combating Terrorism Published

On 31 March 2017, Directive (EU) 2017/541 “on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA” was published in the Official Journal of the EU.

The Directive establishes minimum rules concerning the definition of criminal offences and sanctions in the area of terrorist offences, offences related to a terrorist group, and offences related to terrorist activities. The Directive includes obligations for Member States to criminalise the following acts:

- Travelling within, outside, or to the EU for terrorist purposes;
- Organising and facilitating such travel;
- Training and being trained for terrorist purposes;
- Providing or collecting funds with the intention or the knowledge that they are to be used to commit terrorist offences and offences related to terrorist groups or terrorist activities.

Moreover, the Directive provides for measures of protection for, support for, and assistance to victims of terrorism. These measures include a catalogue of services to meet the specific needs of victims of terrorism, such as the right to receive immediate access to professional support services providing medical and psycho-social treatments or to receive legal or practical advice. Furthermore, assistance with compensation claims is regulated. The emergency response mechanisms immediately after an attack have also been strengthened.

Member States have until 8 September 2018 to implement the obligations of the Directive into their national legal orders. (TW)

►eucrim ID=1702048

### Terrorism Situation and Trend Report (TE-SAT) 2017

On 15 June 2017, Europol published the tenth Terrorism Situation and Trend Report (TE-SAT). The report gives an overview of the nature of terrorism that the EU faced in 2016. The report includes a general part that provides, *inter alia*, statistical data on terrorist attacks and suspects arrested in 2016. It also explains certain horizontal issues, such as the financing of terrorism, travel for terrorist purposes, use of explosive devices

and of toxic chemicals, etc. Thematic chapters of the report deal with jihadist terrorism, ethno-nationalist and separatist terrorism, left-wing and anarchist terrorism, right-wing terrorism and single issue terrorism. The TE-SAT 2017 formulates fourteen trends that the EU is facing at present.

The TE-SAT is generated annually by experts from Europol on the information provided and verified by EU Member States, Europol’s partners and Eurojust. It provides basic facts and figures on terrorism in the EU from the past year, while also identifying developing trends in this area of crime as well as charting the established and evolving drivers of terrorism. (TW)

►eucrim ID=1702049

### Conference on Online Terrorist Propaganda

On 10 and 11 April 2017, Europol’s European Counter Terrorism Centre (ECTC) hosted for the first time a high-level conference on online terrorist propaganda. Over 150 participants attended the event to discuss a wide variety of topics pertaining to the online terrorist threat. The participants included:

- Members of the ECTC Advisory Group on Terrorist Propaganda;
- Representatives of the EU Commission and EU Council;
- Representatives of academia and law enforcement practitioners from Europe and the US.

The Conference supported Europol and EU law enforcement in better focusing their counter-terrorism efforts. It also helped to enhance the tools and techniques in place towards more effective prevention and investigation. (CR)

►eucrim ID=1702050

## Cybercrime

### Common Diplomatic Response Against External Cyber Attacks

The EU has reacted to the growing problem of state or non-state actors pursuing

their objectives with malicious cyber-attacks against EU states. On 19 June 2017, the Foreign Affairs Council adopted conclusions “on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (Cyber Diplomacy Toolbox).” The conclusions are designed to be a joint EU diplomatic response to cyber operations.

The conclusions state that the EU’s diplomatic response to malicious cyber activities will make full use of measures within the Common Foreign and Security Policy, including, if necessary, restrictive measures against states. It also sets guiding principles for further development of the framework, including, for instance, that a joint EU diplomatic response take into account the broader context of the EU external relations with the State concerned, which would be proportionate to the scope, scale, duration, intensity, complexity, sophistication, and impact of the cyber activity. (TW)

►eucrim ID=1702051

### Europol Reacts to New Wave of Ransomware

Following the attack on critical infrastructure and business systems of 27 June 2017, Europol set up an urgent coordination cell to monitor the spread of ransomware. Instructions on what to do when infected can be found on Europol’s website. Tips and the latest available decryption keys can also be found on the website of the initiative “No More Ransom” (see eucrim 3/2016, p. 128). (CR)

►eucrim ID=1702052

### Cyber-Investigation Analysis Standard

In their meeting from 11-12 May 2017 at Europol, leading digital forensic experts in the EU called for the adoption of the Cyber-Investigation Analysis Standard Expression (CASE) as a standard digital forensic format. As a result of the meeting, several market leaders agreed to adopt this open-source data format for forensics and to look into implementing the standard. (CR)

►eucrim ID=1702053

## Procedural Criminal Law

### Procedural Safeguards

#### CJEU Clarifies its Jurisprudence on Right to Information about Charge

In its judgment of 22 March 2017, the CJEU had to deal with the repercussions of its judgment in case C-216/14 of 15 October 2015 (*Covaci*). The *Covaci* case concerned the German penal order procedure (*Strafbefehlsverfahren*) – an important type of German criminal procedure that allows the unilateral and rapid disposal of a case without trial and formal judgment for trivial and medium offences. Possible penalties especially include a fine.

At the first stage of the procedure, the defendant need not be heard by the criminal court before the order is issued, but he/she can lodge a formal objection (*Einspruch*) against a penal order within two weeks following service of the penal order. If the objections are admissible, the court sets down a main hearing on the case.

The question is, however, to which extent the two-week period for objections is affected by EU law if the defendant does not reside in Germany but in another EU Member State. In *Covaci* (for this case, see also *Ruggeri*, eucrim 1/2016, p. 42 et seq.), the CJEU ruled that Arts. 2, 3(1)(c) and 6(1) and (3) of Directive 2012/13/EU on the right to information in criminal proceedings

(1) do not preclude German legislation which, in criminal proceedings, makes it mandatory for an accused person not residing in Germany to appoint a person authorised to accept service of a penal order concerning him;

(2) but do require that the defendant has the benefit of the entirety of the prescribed period to lodge an objection against the penal order.

In the aftermath of this judgment, the local and regional court in Munich had to deal with three cases in which addressees of penal orders did not have a

fixed place of domicile or residence in Germany or in their country of origin. Thus, the question was how the German courts have to handle particularly the second requirement set by the CJEU in *Covaci* (benefit of the whole period for the legal remedy).

The Munich courts wanted to “save” the *res judicata* effects of the penal order (and hence its enforcement) and proposed that

- the accused person, who has neither fixed residence in Germany nor in another EU country, must further nominate a person authorised to accept service of a penal order made against him;

- service on the authorised person is principally sufficient for the purpose of calculating the period within which an objection can be lodged;

- however, the German provisions on restoring to the *status quo ante* (*Wiedereinsetzung in den vorigen Stand*) are interpreted in the light of Directive 2012/13, as a consequence of which the accused person can rely on the un-reduced period to lodge an objection within two weeks of the moment he actually becomes aware of the order.

The CJEU backed this procedure by arguing that Art. 6 of Directive 2012/13 does not require the period to begin to run from the moment the accused person actually becomes aware of the penalty order concerning him. The CJEU reiterated, however, that the procedure must be fair and that the effective exercise of the rights of the defence must be guaranteed. The latter condition is fulfilled if an accused person is placed in the same situation as if the penal order decision had been served to him personally (once he has actually been informed of a criminal decision concerning him).

The cases referred to the CJEU have the case numbers C-124/16 (*Ianos Tranca*), C-213/16 (*Tanja Reiter*), and C-188/16 (*Ionel Opria*). The first two cases were brought by the Local Court (*Amtsgericht*) of Munich; the third case was brought to the CJEU by the Regional Court (*Landgericht*) Munich I.

All cases were joined by the CJEU. The CJEU proceeded to judgment without an opinion of the Advocate General. (TW)

► [eucrim ID=1702054](#)

### Advocate General: Penal Orders Must be Notified with Translation

After the cases “*Covaci*” and “*Tranca/Reiter/Opria*” (see news item above), the German penal order procedure is at the centre of another reference for a preliminary ruling (Case C-278/16, *Frank Sleutjes*). The referring Regional Court of Aachen (*Landgericht Aachen*), Germany, faces the problem that the German law – by implementing Directive 2010/64/EU on the right to interpretation and translation – indeed requires, as a general rule, a written translation of penal orders for the exercise of the procedural rights of an accused person who does not have a command of German. However, it only specifies for “judgments” that the period for lodging remedies does not start before the notification of the judgment together with the translation.

In the case at issue, the judicial authorities therefore followed common German practice, i.e., they notified the penal order in German to the defendant, Mr. *Sleutjes*, a Dutch national living in the Netherlands without a sufficient command of German. Only the information on the legal remedies available was additionally and simultaneously delivered in Dutch language translation. It informed Mr. *Sleutjes* that the penal order would be legally binding and enforceable if the defendant did not lodge an objection (*Einspruch*) at the local court (in the present case Local Court (*Amtsgericht*) of *Düren*) within two weeks of notification; in addition, it was pointed out that “the written appeal must be lodged in German.” Although the defendant objected to the penal order by e-mail shortly before the termination of the two-week period for lodging objections, the Local Court of *Düren* refused to accept the objection because the e-mail was in Dutch. A subsequent objection filed by Mr. *Sleutjes*’ German defence lawyer

was considered inadmissible by the local court because it had been submitted after the two-week objection period. As a consequence, the Local Court of *Düren* considered the penal order final and enforceable.

The defence lawyer of the defendant challenged this decision, which is now pending before the referring Regional Court of Aachen. The Regional Court poses the question of whether the German provision, which lets the period for lodging legal remedies start only if a translation of the judgment is submitted to the defendant, also applies to penal orders. In this case, the period for lodging the objection would not yet have been set in motion because the penal order had not been translated.

In its opinion of 11 May 2017, Advocate General (AG) *Nils Wahl* affirms that penal orders within the meaning of Sec. 407 et seq. of the German Criminal Procedure Code are an “essential document” in the sense of Art. 3 of Directive 2010/64, as a result of which they must be translated in the event that the person concerned does not understand German. He argues that this conclusion follows from the wording of Art. 3, the context of Directive 2010/64, and the aim of the Directive. He adds that denying the translation of a penal order that could lead to the lasting imposition of a penalty would, in fact, deny justice to a person who does not understand the language of the court.

As for the legal consequences of the lack of translation, the AG first clarifies that Directive 2010/64 does not indicate any specific measure to be taken by Member States when it comes to a breach of the right to translation. However, he agrees with the Regional Court that, in the present case, notification of the contested penal order without an accompanying Dutch translation of the entire text would have been ineffective. As a result, the period within which to lodge an objection would not yet have been set in motion. (TW)

► [eucrim ID=1702055](#)

## Data Protection

### German Court Rules that German Data Retention Law Contravenes Union Law

In its decision of 22 June 2017, the Higher Regional Court of Münster (*Oberverwaltungsgericht Münster*) agreed with the request of a Munich IT enterprise that, for the time being, it need not retain data according to the new German data retention law. According to the court, the new German telecommunications law, which obliges telecommunications providers to retain the traffic data of their users for a limited period of 10 weeks and location data for four weeks (as from 1 July 2017) in order to be able to provide them to the law enforcement authorities, if necessary, is not in conformity with EU law.

The Higher Administrative Court refers in its reasoning to the judgment of the European Court of Justice of 21 December 2016, in cases C-203/15 and C-698/15, *Tele 2 Sverige et al.* (cf. [eucrim 4/2016](#), p. 164), which provided restrictive conditions for national legislation to maintain data retention rules. In the view of the German court, the German data retention obligation applies to all traffic and location data of nearly all users of telephone and Internet services, whereas the CJEU objects to such blanket retention systems. National legislation can only be lawful if it imposes targeted retention of data to fight serious crime and fulfils strict conditions.

The decision of the Münster court was taken as an interim measure; it will decide on the actual administrative action later. The Federal Network Agency (*Bundesnetzagentur*), which is responsible for technically implementing the surveillance measures in Germany, announced that it will not proceed with further enforcing the retention obligation for telecommunications and Internet service providers for the time being. It is also worth noting that a constitutional complaint against the new German data retention law is pending before the Ger-

man Federal Constitutional Court whose decision is only expected in 2018. (TW)  
 > [eucrim ID=1702056](#)

### Council Conclusions on Interoperability of Databases for Security Purposes

At its meeting on 8/9 June 2017, the JHA Council adopted conclusions on improving the information exchange and ensuring the interoperability of EU information systems. Interoperability is a priority at the highest political level in the EU. It is considered an important means by which to tackle terrorist attacks.

Interoperability is defined as the ability of information systems to exchange data and to enable the sharing of information. Several dimensions of interoperability have been distinguished.

The present Council conclusions contain several guidelines addressed to the Commission, the Member States, and other EU agencies to take steps forward so that interoperability of existing and future EU information systems in the field of migration, asylum, and security can be ensured by 2020.

The JHA Ministers in the Council *inter alia* invite the Commission to implement several interoperability solutions. They include the following:

- Work towards creating a European search portal capable of parallel searching of all relevant EU systems in the areas of borders, security, and asylum;
- Explore the future implementation of a shared biometric matching service for all types of biometric data and analyse their use for the purpose of flagging biometric data from other systems;
- Explore the future establishment of a common identity repository.

All these initiatives also involve Europol because of the inclusion of Europol data into the interoperability solutions and Europol's easier access to support the cross-checking of data.

The Council conclusions mainly take into account the report of the High-Level Expert Group on Information Systems and Interoperability, which was

published in May 2017, including statements by the EU Fundamental Rights Agency (FRA), the European Data Protection Supervisor (EDPS), and the EU Counter-Terrorism Coordinator (CTC) in the annex. The Expert Group was established by the Commission in June 2016. Its mission was to help develop a joint strategy to make data management in the Union more effective and efficient, in full respect of data protection requirements, to better protect its external borders, and to enhance its internal security. (TW)

> [eucrim ID=1702057](#)

### EDPS Issues Paper to Guide the Charter's Necessity Requirement

After public consultation following the release of a background paper (see [eucrim 2/2016](#), p. 79), on 11 April 2017, the European Data Protection Supervisor (EDPS) published the final version of a toolkit designed to help assess the necessity test of new EU measures that may limit the fundamental right to the protection of personal data pursuant to Art. 52(1) and 8 of the Charter of Fundamental Rights. The toolkit is above all addressed to EU policymakers and legislators in order to better carry out their responsibility for preparing or scrutinising measures that involve processing of personal data and that limit the right to the protection of personal data and other rights and freedoms laid down in the Charter. Thus, the toolkit will contribute to raising more awareness of data protection issues in EU legislation.

The toolkit starts with a legal analysis of the necessity test applied to the right to the protection of personal data. It is followed by a practical, step-by-step checklist to assess the necessity of new legal measures. The checklist is the core of the toolkit and can be used autonomously. The points of reference of the toolkit are the case law of the CJEU and the ECtHR, respectively, as well as previous Opinions of the EDPS and of the Art. 29 Working Party. (TW)

> [eucrim ID=1702058](#)

### Ne bis in idem

#### CJEU: Company Reps Can Face Criminal Penalty for Corporation's Failure to Pay VAT

On 5 April 2017, the CJEU delivered its judgment on a preliminary ruling requested by the Tribunale di Santa Maria Capua Vetere, Italy in the Joined Cases C-217/15 and C-350/15 (*Massimo Orsi and Luciano Baldetti*). The Italian court asked whether the *ne bis in idem* principle enshrined in Art. 50 of the EU Charter of Fundamental Rights prohibits criminal proceedings to be brought for non-payment of VAT after imposition of a definitive (administrative) tax penalty with respect to the same act or omission.

The CJEU first reiterated its case law that the Charter is applicable if national criminal law provisions concern offences relating to VAT.

Second, the CJEU however found, that in the case at issue, the *ne bis in idem* rule of Art. 50 of the Charter is not fulfilled because the "same person" was not sanctioned more than once for the same unlawful act. The Court pointed out that the tax penalty at issue in the main proceedings was imposed on two companies, each with a legal personality, whereas the criminal proceedings at issue were directed against *Mr. Orsi* and *Mr. Baldetti*, who are natural persons. The fact that the acts or omissions were committed by *Mr. Orsi* and *Mr. Baldetti* in their capacity as legal representatives of the companies concerned does not call into question the aforementioned conclusion.

The CJEU found that the reached conclusion is ultimately in line with parallel case law of the ECtHR on Art. 4 of Protocol No. 7 to the ECHR, which also legally distinguishes between natural and legal persons who are subject to the penalty at issue. For the latter, see e.g. ECtHR, 20 May 2014, *Pirttimäki v. Finland*, Appl. no. 35232/11.

The CJEU has not decided yet on the question whether Art. 50 of the Charter precludes the possibility of conducting



criminal proceedings concerning an act (non-payment of VAT) for which a definitive administrative penalty has been imposed on the same person. This question is subject of case C-524/15, *Luca Menci*, which is pending at the Grand Chamber of the CJEU. For this constellation, the ECtHR (GC) decided by judgment of 15 November 2016 in *A and B v. Norway* (Applications nos. 24130/11 and 29758/11) that a combination of tax penalties and criminal penalties as punishment for the same tax offences did not infringe the principle *ne bis in idem* affirmed in Art. 4 of Protocol No 7 to the ECHR. (TW)

► eucrim ID=1702059

## Victim Protection

### FRA Opinion on Access to Remedies by Victims of Business-Related Human Rights Violations

In April 2017, the Fundamental Rights Agency (FRA) released an expert opinion exploring possible avenues towards lower barriers for access to remedy by victims in the context of business-related human rights abuses. The opinion had been requested by the Council in June 2016. It complements increasing past and ongoing efforts at the international level (in particular UN and CoE), which address the problem of business companies harming individual's rights and freedoms.

FRA formulates 21 specific opinions that are clustered under the following six headings:

- Lowering barriers to make judicial remedies more accessible;
- Enhancing the effectiveness of judicial remedies – especially in extraterritorial situations;
- Ensuring effective remedies through criminal justice;
- Ensuring effective non-judicial remedies – state based and non-state based;
- Implementing access to remedy – transparency and data collection;
- Implementing access to remedy – ac-

tion plans, coordination, and due diligence.

The following are among the FRA's suggestions:

- Improving access to judicial remedies, e.g., by creating minimum standards on legal aid at the EU level and by better funding legal support, particularly for vulnerable people, as well as by shifting the burden of proof from victims to businesses;
- Supporting victim's redress from companies based abroad, for instance by giving information on how to proceed in cross-border cases;
- Better use of criminal justice systems, in particular increasing the use of existing laws on corporate crime; possible measures in this regard at the EU level could be, for instance, EU-wide data collection on complaints as well as compensation, training, and improving the human and financial resources of law enforcement to tackle corporate crime;
- Creating minimum standards on non-judicial remedies;
- Improving transparency and data collection, e.g., by instigating Member States to set up concrete action plans and by making information on remedies publicly available.

In general, the FRA's opinions allow the conclusion to be drawn that much more could be done at the EU level for victims of rights abuses by business in the areas of judicial and non-judicial remedies. (TW)

► eucrim ID=1702060

## Freezing of Assets

### Commission Proposal on Regulation Regarding Freezing and Confiscation Order Sparks Criticism

European lawyers took a critical standpoint towards the Commission proposal for a Regulation on the mutual recognition of freezing and confiscation orders (see eucrim 4/2016, p. 165).

The Council of Bars and Law Societies of Europe (CCBE) points out in a

comment issued on 19 May 2017 that the current proposal insufficiently safeguards the right of third parties who may be the rightful owner of property subject to confiscation. In addition, the legal text has to introduce provisions on the rights of legal persons or other stakeholders in legal person being the owner of the asset. The CCBE also comments on specific articles of the proposal and remarks on the following two issues:

- The list of offences, on the basis of which a double criminality check does not take place, is too broad and contrary to the principle of legality, as well as the general requirement of criminal regulations, to be strictly necessary and proportionate;
- The issue of remedies has gaps, in particular as regards situations in which the confiscation order in the issuing state is later found unlawful; furthermore, resources to contest a freezing order should be privileged.

Similar criticism is expressed in a statement of the German Bar Association (*Deutscher Anwaltverein – DAV*) released in June 2017. The statement mainly concludes that the Commission proposal lacks clarity and legal certainty in view of different legislations and practices among the EU Member States in the field of freezing assets. For example, the DAV considers the imprecise use of categories of offences or the description of criminal acts in the draft text utterly problematic. It criticises that the Commission seemingly took over the list of offences for the abolition of the verification of double criminality from the framework decision on the European Arrest Warrant in an unfiltered way.

In addition, the DAV regrets that procedural safeguards have not been taken into account and that the issue of remedies has been insufficiently answered. Lastly, the legislation should include compensation measures for unlawful decisions of freezing and confiscation.

Next, several national parliaments also submitted statements and comments on the Commission proposal, including



the Czech and Portuguese parliaments and the General Courts of Spain. The German Bundesrat noted, *inter alia*, the following:

- The instrument of an EU directive should be preferred over the regulation;
- Some provisions would harmonise national criminal procedure law, which goes beyond the possibilities conferred to the EU legislator by Art. 82 TFEU;
- An *ordre public* refusal ground should be included that is in line with the Directive on the European Investigation Order and recent case law on the European Arrest Warrant;
- Fixed time limits as well as information and consultation obligations for national executing authorities are regulated too bureaucratically.

The Commission proposal will be further debated in the Council and the EP in the forthcoming months. The LIBE committee decision is expected. (TW)

► [eucrim ID=1702061](#)

## Cooperation

### European Arrest Warrant

#### CJEU: Member States Must Ensure Undertaking to Enforce Sentence Against Residents

According to Art. 4 no. 6 of Framework Decision 2002/584 on the European Arrest Warrant (FD EAW), the executing judicial authorities can refuse to execute an EAW if it has been issued for the purpose of execution of a custodial sentence, where the requested person is staying in or is a national or a resident of the executing Member State. In case of refusal, the executing Member State must undertake to execute the sentence in accordance with its domestic law.

By judgment of 29 June 2017 in case C-579/15 (*Daniel Adam Poplawski*), the CJEU provided guidance on an old practical problem in the application of Art. 4 no. 6: to which extent are Mem-

## Report

### Update on the EU Framework for the Freezing, Confiscation and Recovery of Assets

#### Tools and Challenges

Academy of European Law (ERA), Trier, 4–5 May 2017

The seminar aimed to analyze the current European framework for the freezing, confiscation, and recovery of assets. It gave prosecutors, government officials and judges the opportunity to discuss national and cross-border challenges and actions in the light of Directive 2014/42/EU and the 2016 Commission proposal for a regulation on the mutual recognition of freezing and confiscation orders.

The contributions started with an overview of the different typologies of confiscation mechanisms in the Member States and the latest developments in the international legal and policy framework. Particular attention was paid to the origin, rationale, and evolution of confiscation as well as to the main systems developed in the EU Member States and in the USA. A comparison of the Member States' different asset recovery regimes showed a decline in the field of defense protection in favor of the efficiency of the proceedings.

The overview of the EU legal framework focused on the implementation of Directive 2014/42/EU, including the obligation of establishing extended confiscation mechanisms and the possibility of a future non-conviction based confiscation model at the European level. Additionally, the CoE 2016-2020 action plan on fighting transnational organized crime was analyzed, providing an overview of its key points, such as the improvement of financial investigations and the strengthening of international cooperation on non-traditional forms of confiscation. The discussants agreed that there is significant resistance on the part of many Member States to introduce non-conviction based confiscation. This is because the punitive character of confiscation is often incompatible with the lower burden of proof required for non-conviction based confiscation and because resorting to a punitive measure is often the only way to allow confiscation of gross proceeds.

The difficulty of striking a fair balance between efficient confiscation measures and due protection within the European human rights framework was addressed by Professor Robert Esser. He also analyzed the broad scope of the protection of property enshrined in Art. 1 of Protocol No.1 ECHR, together with the restriction it allows, and the case law of the ECtHR in the matter.

In-depth contributions about national operative perspectives were also presented. Among them, HH Judge Michael Hopmeier discussed the Recent Developments and the Criminal Finances Act 2017 concerning restraint, confiscation, and asset recovery and illustrated the methods of recovering proceeds of crime in the UK. Senior public prosecutor Paul P.A.M. Notenboom highlighted the increasing importance of extended confiscations over possible future non-conviction based confiscations in Dutch legal practice.

In addition, the participants focused on the question of how to overcome hurdles when dealing with confiscation or victim compensation and restitution in cross-border cases, with an emphasis on the victims' priority rights. Attention was especially drawn to the complex cases in which the frozen assets belong to the victim. Last not least, the topic of cross-border and inter-agency cooperation was explored. Among other things, the discussants agreed on increasing investigations targeted at financial items and on the need to speed up cooperation through traditional formal channels (such as Europol and Interpol) whose shortcomings often have to be compensated by informal networks.

*Salvatore Romano, Faculty of Law, Sapienza University of Rome*

ber States able to introduce conditions into their national implementation law to take over the custodial sentence?

In the case at issue, Poland issued an EAW against *Mr. Poplawski*, a Polish national residing in the Netherlands,

with a view to enforcing a custodial sentence imposed in Poland against him. Dutch authorities refused the surrender because *Mr. Poplawski* is in possession of a residence permit of indefinite duration in the Netherlands. According to

the underlying Dutch law applicable at the time of the decision of the executing Dutch court, the issuing state, i.e. Poland, was required to request the taking over of the execution of the sentence in accordance with the procedure laid down in the 1983 CoE Convention on the Transfer of Sentenced Persons. However, Poland was unable to submit this request because, according to Polish legislation, such requests are precluded if the person concerned is a Polish national. As a consequence, in such situation the refusal to surrender may lead to the impunity of the person concerned because there has been no (formal) request for execution.

The CJEU clarified that Art. 4 no. 6 FD EAW entails the obligation to undertake to enforce the sentence and that the declaration of a mere “willingness” to execute, as foreseen in Dutch law, is insufficient. As a result, Member States must ensure that the execution of the custodial sentence is in fact taken over at the time of refusal of surrender, and such execution cannot be made impossible at a later stage. The CJEU adds in this context that creating the risk of impunity of a requested person cannot be regarded as compatible with the FD.

The CJEU then had to decide on how this finding can be implemented by the Dutch court. The CJEU reiterated its case law on the obligation to interpret national law in conformity with EU law, including FDs. Although this principle has limitations, the CJEU states that national courts are required to do whatever lies within their jurisdiction to ensure that the FD EAW is fully effective and to achieve an outcome consistent with the objective pursued by it. In this context, the CJEU pointing out that it is not inconceivable to place the FD EAW on the same footing as the formal legal basis required by the domestic Dutch law: thus, its interpretation in conformity with EU law is possible. However, it is up to the Dutch court to decide on this question. (TW)

► eucrim ID=1702062

## European Investigation Order

### Five Member States Transposed EIO on Time

26 EU Member States (Ireland and Denmark do not take part) had to implement Directive 2014/41/EU regarding the European Investigation Order in criminal matters by 22 May 2017. According to the information made available to the EJM Secretariat, only five Member States (Belgium, France, Germany, Hungary, Latvia) transposed the EIO Directive on time. These Member States are now ready to apply in practice this new EU legal instrument on gathering evidence located in another EU country.

The EIO Directive is based on the principle of mutual recognition of judicial decisions when it comes to obtaining evidence for use in criminal proceedings. The European Commission pointed out that the EIO will offer the following advantages in comparison with past legal instruments:

- Creation of a single comprehensive instrument with a large scope;
- Strict deadlines for the executing Member State to gather the evidence;

- Limitation of refusal grounds to execute the order, e.g., if the request is against the country’s fundamental principles of law or harms national security interests;

- Reduction of paperwork by introducing a single standard form translated into the official language of the executing State for authorities to request evidence;
- Protection of the fundamental rights of the defence: The issuing authorities must assess the necessity and proportionality of the investigative measure requested. A European Investigation Order has to be issued or validated by a judicial authority. Member States must ensure legal remedies equivalent to those available in a similar domestic case and ensure that the persons concerned are properly informed of these possibilities.

The Commission announced that it will now analyse the state of the implementation and follow up with those Member States which have not yet taken the necessary measures. As reported in eucrim 1/2017, p. 19, the status of information is available via the EJM website. (TW)

► eucrim ID=1702063



## Council of Europe\*

Reported by Dr. András Csúri

### Foundations

#### Reform of the European Court of Human Rights

#### Court Launches New System for Single Judge Decisions

In 2010, in order to tackle the massive backlog of clearly inadmissible cases,

Protocol No. 14 introduced the “single judge decision” in order to be able to declare applications inadmissible in a summary procedure. Accordingly, applicants received a decision letter rejecting complaints in a global manner.

\* If not stated otherwise, the news reported in the following sections cover the period 16 March 2017 – 30 June 2017.

Since then, the backlog has been eliminated and, in light of the Brussels Declaration of March 2015, the ECtHR has adopted a new procedure. The aim is to allow for more detailed and individualized reasoning, while maintaining an efficient process for handling inadmissible cases.

Instead of a decision letter, as from June 2017, applicants will receive a single judge decision in one of the Court's official languages, signed by a single judge and accompanied by a letter in the relevant national language. The decision will include reference to specific grounds of inadmissibility in many but not all cases, as the Court will still issue global rejections, for example when applications contain numerous ill-founded, misconceived, or vexatious complaints.

►eucrim ID=1702064

## Human Rights Issues

### HR Commissioner Publishes Annual Activity Report for 2016

On 26 April 2017, *Nils Muižnieks*, CoE Commissioner for Human Rights, published his annual activity report for 2016. The primary thematic activities of the Commissioner in 2016 included the following:

- Freedom of expression and media freedom;
- Human rights of immigrants, refugees, and asylum seekers;
- Children's rights;
- Human rights of persons with disabilities;
- Human rights of LGBTI persons;
- Human rights of Roma and travellers;
- Women's rights and gender equality;
- Combating racism and intolerance;
- National minorities;
- Systematic implementation of human rights;
- Addressing statelessness;
- Transitional justice and missing persons;
- Counter-terrorism and human rights protection;

■ The treatment of prisoners and rehabilitation of victims of torture.

While presenting the report, the Commissioner described 2016 as a critical turning point for human rights in Europe, which will mark either a dramatic low point to be bounced back from or the beginning of the end of the European human rights system and European integration. He also highlighted the following:

- The unprecedented situation that three countries – Ukraine, France, and Turkey – have derogated from the ECHR;
- The fact that the UK decided to leave the EU;
- The human rights situation in Turkey;
- The policy initiatives endangering the rule of law in Poland;
- The growing number of Member States refusing to co-operate with CoE institutions and mechanisms.

He added that the alternative to shaking up the system might only be chaos.

As regards the migration crisis, the Commissioner called on Member States to do their part to alleviate the strain on frontline countries. He remarked that countries should not go unchallenged when providing insufficient support to new arrivals, thus encouraging their non-integration and departure to another country.

Regarding counter-terrorism measures, the Commissioner urged strengthening the democratic oversight of security services and of the automatic prolongation of states of emergency and derogations from the ECHR.

►eucrim ID=1702065

## Specific Areas of Crime

### Corruption

#### Germany Ratifies CoE's Anti-Corruption Convention

On 10 May 2017, Germany ratified the Criminal Law Convention on Corruption and its Additional Protocol. The in-

struments will enter into force on 1 September 2017 with respect to Germany.

►eucrim ID=1702066

### GRECO Launches Fifth Evaluation Round

On 20 March 2017, GRECO launched its Fifth Evaluation Round that will focus on preventing corruption in central governments and law enforcement agencies.

The new evaluation round will look at measures that states have put in place to prevent and combat corruption in top executive functions. These include the heads of state, heads and members of central government (e.g., ministers), as well as other political appointees who exercise top executive functions, e.g., deputy ministers, state secretaries, heads and members of a minister's private office, and senior political officials. With regard to these functions, GRECO will look into issues such as conflicts of interest, the revolving door phenomenon between different sectors, the declaration of assets, and accountability mechanisms.

The first countries to be evaluated include the UK, Slovenia, Finland, Iceland, and Luxembourg.

►eucrim ID=1702067

### GRECO: Fourth Round Evaluation Report on Switzerland

On 15 March 2017, GRECO published its fourth evaluation report on Switzerland. This latest evaluation round was launched in 2012 in order to assess how states address the prevention of corruption with respect to Members of Parliament (MPs), judges, and prosecutors (for more recent reports, see eucrim 3/2014, p. 83; 4/2014, pp. 104-106; 1/2015, p. 11; 2/2015, pp. 43-45; 3/2015, pp. 87-88; 1/2016, pp. 20-22; 2/2016, pp. 82-83; 3/2016, pp. 134-135; 4/2016, pp. 168-169; 1/2017, pp. 22-23).

The report highlighted that various specificities of Switzerland's relevant institutions lead to considerable public confidence, but that the very organiza-

tion of the system still allows for subtle pressure to be exerted on politicians and the judiciary. On a general scale, GRECO called on Switzerland for the development of ethical rules applicable to MPs at the federal level and to judges and prosecutors.

As regards MPs, GRECO recommends adopting a code of ethics in order to increase awareness, publicly announcing conflicts of interest as part of parliamentary procedure, and developing the system for declaring relevant interests. Additionally, MPs' compliance with their obligations should be monitored.

As regards the judiciary, while recognizing the election of judges of the federal courts by the Federal Assembly, GRECO calls for improvements to better ensure the quality and objectivity of the recruitment of these judges. Additionally, ties of elected judges to the political sphere should be cut, especially by doing away with the practice of judges paying part of their salary to "their" political party. The report further calls for an improved code of ethics for judges and for a transparent disciplinary system.

According to the report, the Office of the Attorney General of the Confederation also needs to develop rules of professional ethics for its members and to provide greater transparency in disciplinary matters.

► eucrim ID=1702068

### **GRECO: Fourth Round Evaluation Report on Lithuania**

On 24 April 2017 GRECO published its Fourth Round Evaluation Report on Lithuania. While welcoming the reforms to prevent corruption among MPs, the report highlighted that the country has satisfactorily implemented only three of the 11 previously made recommendations, and it called on the authorities to step up efforts regarding especially the judiciary and the prosecution service. On a general note, cooperation between the Chief Official Ethics Commission

and the oversight institutions responsible for preventing corruption among MPs, judges, and prosecutors should be significantly improved.

As regards MPs, the adoption of the legal amendments to enhance the transparency of the legislative process and improve the regulation of parliamentarians' engagement with lobbyists is still pending. Additionally, further measures are necessary to improve supervision and enforcement of the rules regarding declarations of private interests and conflicts of interest.

As regards judges, the report emphasizes the lack of steps taken so far to strengthen the independence and the role of the Selection Commission of Candidates to Judicial Offices and to consolidate the procedure for appealing against the Commission's decisions. Nevertheless, GRECO welcomed various positive developments, such as the approval of standards on the quality of judicial decisions, improved communication with the public, and increased awareness of ethical issues and conflicts of interest.

Finally, as regards prosecutors, the report welcomes the improved rules (and their practical implementation) on communication between the prosecution service and the public as well as the publication of a practical guide to the Code of Ethics of Prosecutors. Nevertheless, there is still more to be done in order to strengthen the role of the selection commissions in the recruitment of prosecutors.

► eucrim ID=1702069

### **GRECO: 17th Annual Activity Report**

On 7 June 2017, GRECO presented its 17th annual activity report.

In 2016, GRECO adopted over 40 evaluation and compliance reports, largely under the third and fourth rounds of evaluation, covering incriminations, political party funding, and the prevention of corruption in respect of MPs, judges and prosecutors.

While the implementation rate of GRECO's recommendations for the first

two rounds has been very high, countries increasingly need more time to comply with GRECO's recommendations in the 3rd and, especially, in the 4th rounds. This is also due to the increasing complexity of the issues discussed under these evaluations and the fact that not only government initiatives are called for in many of the respective areas.

According to the report, countries tend to overly rely on the repressive aspects of fighting corruption, too often underestimating the strength and effectiveness of preventive mechanisms. Preventive measures may help, however, to ensure impartiality and thus boost trust in political and other institutions, and they can also help deal with problematic situations before they become a criminal offence (e.g., bribery, trading in influence).

The trends under the 4th round evaluation ("Corruption prevention in respect of members of Parliament") revealed some positive developments – also in anticipation of GRECO's 4th Round Evaluation visits –, like the introduction of codes of conduct or codes of ethics for MPs in many countries. Although a code in itself does not guarantee ethical behavior, it does help to foster a climate of integrity, requiring institutional set-up for its implementation. Nevertheless, the monitoring and enforcement regime for integrity and the prevention of conflicts of interest in the legislature needs to be strengthened significantly.

Some legislation has not provided for a written definition of conflicts of interest or rules for disclosing potential conflicts, and only very few Member States have developed any regulations in respect of lobbying. Lobbying is a growing phenomenon in several Member States, and GRECO has therefore recommended that they establish guidelines for MPs in this respect. The overall aim of the regulatory framework is to provide transparency, to a large extent through registration and reporting obligations. In addition, asset declaration systems for MPs (and to some extent their close



relatives) suffer from crucial shortcomings regarding their transparency and actual scrutiny. In light of this, ensuring public access to MPs' financial declarations, e.g., through their timely publication has been recommended repeatedly by GRECO. Moreover, several Member States have weak supervisory mechanisms and, accordingly, have received recommendations aimed at establishing/making more effective or independent, the monitoring of MPs' adherence to the above standards.

The recommendations as regards corruption prevention in respect of judges and prosecutors are closely linked to matters such as the independence of the judiciary, from the particular angle of preventing corruption and strengthening integrity within the respective professions.

The issue of "revolving door" between justice and politics (e.g. the direct participation of magistrates in political life) increases the risk of politicization among the judiciary in some Member States. GRECO emphasizes that the particularities of judicial functions require a reasonable balance between judges' visible involvement in society and the independent and impartial discharge of their functions. Therefore, in the interest of the right to a fair trial and legitimate public expectations, judges should show restraint in the exercise of public political activity. As a positive example, the report highlights the Prosecution Service Integrity Bureau (BI-OM), established in 2012 in the Netherlands in order to foster integrity and prevent misconduct within the prosecution service.

Additionally, in a few cases, GRECO has seen the need for fundamental reforms relating to the independence of the judiciary. These include such issues as

- The conversion of judicial councils into self-governing bodies proper;
- Independence from the executive powers;
- The need to increase the awareness of judges and prosecutors of ethical is-

ssues through the development of further guidance and training;

- Establishment of objective criteria for appointments;
- Career advancement of judges and prosecutors.

The report also emphasizes that, following Liechtenstein's ratification of the Criminal Law Convention on Corruption in December 2016, all but two Member States (Germany and the USA) have ratified the Convention [note of the author: since the publication of the annual report, Germany has also ratified the Convention, see news item above]. The situation in respect of the ratifications of, and compliance with, the Additional Protocol to the Convention remains slightly more problematic, as

seven Member States have not yet ratified this instrument, and even more of them are not fully complying with its requirements.

As regards the topics covered by the 3rd round evaluation (transparency of party funding), at the end of 2016, only four Member States remain in the special "non-compliance procedure." They are Bosnia and Herzegovina, Denmark, Switzerland, and Turkey.

The report suggests considering the revision of GRECO's procedures for the next, 5th Evaluation Round, in particular regarding the compliance procedure. During the last two cycles, the difficulties encountered and the time needed to comply with the recommendations put too heavy a burden on Member States to

Council of Europe Treaty	State	Date of ratification (r), signature (s) or accession (a)
Additional Protocol to the Convention on the Transfer of Sentenced Persons (CETS No. 167)	Spain	19 July 2017 (r)
Criminal Law Convention on Corruption (ETS No. 173)	Germany	20 May 2017 (r)
Protocol No. 12 to the Convention for the Protection of Human Rights and Fundamental Freedoms (CETS No. 177)	Portugal	16 January 2017 (r)
Convention on Cybercrime (CETS No. 185)	Senegal Greece Monaco San Marino Chile Tonga	16 December 2016 (a) 25 January (r) 17 March 2017 (r) 17 March 2017 (s) 20 April 2017 (a) 9 May 2017 (a)
Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (CETS No. 189)	Senegal Greece Monaco San Marino	16 December 2016 (a) 25 January (r) 17 March 2017 (r) 19 May 2017 (s)
Protocol amending the European Convention on Suppression of Terrorism (CETS No. 190)	Italy	21 February (r)
Additional Protocol to the Criminal Law Convention on Corruption (CETS No. 191)	Germany	10 May 2017 (r)
Council of Europe Convention on the Prevention of Terrorism (CETS No. 196)	Italy	21 February 2017 (r)

Council of Europe Treaty	State	Date of ratification (r), signature (s) or accession (a)
Council of Europe Convention on Action against Trafficking in Human Beings (CETS No. 197)	Czech Republic	29 March 2017 (r)
Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism (CETS No. 198)	Italy Germany	21 February 2017 (r) 20 June 2017 (r)
Third Additional Protocol to the European Convention on Extradition (CETS No. 209)	Lithuania	2 January 2017 (r)
Convention on preventing and combating violence against women and domestic violence (CETS No. 210)	Moldova Georgia European Union Norway	6 February 2017 (s) 19 May 2017 (r) 13 June 2017 (s) 5 July 2017 (r)
Convention on the counterfeiting of medical products and similar crimes involving threats to public health (CETS No. 211)	Burkina Faso	27 July 2017 (r)
Fourth Additional Protocol to the European Convention on Extradition (CETS No. 212)	Russia	29 May 2017 (r)
Protocol No. 15 amending the Convention for the Protection of Human Rights and Fundamental Freedoms (CETS No. 213)	Portugal Greece Latvia Iceland Slovenia	16 January 2017 (r) 2 March 2017 (s) 9 May 2017 (s) 3 July 2017 (r) 4 July 2017 (r)
Protocol No. 16 to the Convention for the Protection of Human Rights and Fundamental Freedoms (CETS No. 214)	Armenia Greece Moldova	31 January 2017 (r) 2 March 2017 (s) 3 March 2017 (s)
Council of Europe Convention against Trafficking in Human Organs (CETS No. 216)	Latvia Moldova	30 March 2017 (s) 21 June 2017 (r)
Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism (CETS No. 217)	FYROM Italy Moldova Bosnia and Herzegovina Cyprus Andorra Latvia Russia	18 January 2017 (s) 21 February 2017 (r) 23 February 2017 (r) 29 March 2017 (r) 24 April 2017 (s) 19 May 2017 (s) 11 July 2017 (r) 27 July 2017 (s)
Protocol No. 16 to the Convention for the Protection of Human Rights and Fundamental Freedoms (CETS No. 214)	Netherlands Turkey Estonia	7 November 2013 (s) 20 December 2013 (s) 17 February 2014 (s)

Compiled by Antonia Meyer

➤ eucrim ID=1702072

report frequently, as well as for GRECO to adopt compliance reports at an acceptable pace. The time for compliance as currently envisaged is also out of tune with the time needed for reforms to be implemented in Member States.

Finally, in 2016, the EU also showed growing interest in GRECO's work, whereby the EU stressed that, among its priorities for cooperation with the CoE, its participation in GRECO could contribute to more coordinated anti-corruption policies in Europe. The analysis of the implications of the EU's full participation in GRECO is still ongoing, with participation remaining a long-term objective.

➤ eucrim ID=1702070

## Money Laundering

### MONEYVAL: Annual Report for 2016

On 30 May 2017, MONEYVAL published its annual report for 2016. After the numerous horrific terrorist attacks in 2016, Chair *Daniel Thelesklaf* highlighted the need to cut off the financial lifeline of terrorists. In 2016, MONEYVAL actively monitored 20 jurisdictions through the adoption of mutual evaluation reports (including onsite visits) or follow-up reports. Throughout the year, MONEYVAL continued its 5th round of mutual evaluations, focusing on whether the AML/FTF legal frameworks of the Member States are actually and effectively put to use. The results of this new round have been rather mixed so far, with significant challenges for countries to ensure the transparency of legal persons and entities. Chair *Thelesklaf* underlined that these deficiencies have been confirmed all the more through the revelations of the so-called "Panama Papers," which also showcased that the Member States are not sufficiently investigating and prosecuting all forms of ML in accordance with the risks detected and that there are practically no prosecutions and convictions for terrorist financing.

➤ eucrim ID=1702071

## The Directive on the Fight against Fraud to the Union's Financial Interests by Means of Criminal Law (PFI Directive)

### Laying Down the Foundation for a Better Protection of the Union's Financial Interests?

Adam Juszczyk and Elisa Sason\*

#### I. Introduction

After five years of intense and constructive negotiations,<sup>1</sup> the Council<sup>2</sup> and the European Parliament have adopted the Directive on the fight against fraud to the Union's financial interests by means of criminal law (the "PIF Directive").<sup>3</sup> The Directive, which is binding for all Member States, save for Denmark and the United Kingdom,<sup>4</sup> is part of the Commission's overall strategy to strengthen the protection of the Union's financial interests. It will increase the protection provided by the current legislative framework by further harmonising the definitions, sanctions, and prescription periods of criminal offences affecting the Union's financial interests. The Convention on the protection of the European Communities' financial interests of 1995<sup>5</sup> (the "PIF Convention") and its three protocols<sup>6</sup> will be replaced by the Directive for the Member States bound by it.<sup>7</sup>

Given the diverging rules in the laws of the Member States, as well as the unsatisfying level of both effectiveness and deterrence across the Member States when it comes to protecting the financial interests of the Union,<sup>8</sup> the adoption of the Directive seeks to significantly step up the equivalent and effective protection of the Union's financial interests required by Art. 325 TFEU. The Directive will also facilitate the recovery of misused EU monies, which causes considerable damage to the EU budget. According to the EU's Anti-Fraud Office (OLAF), the damage to the Union budget lies in the range of more than half a billion Euros per year,<sup>9</sup> while other

sources see the financial damage going into the billions of Euros; the financial damage to the Union and the national budgets resulting from serious cross-border value added tax (VAT) fraud alone is estimated to be around 50 billion per year,<sup>10</sup> in addition to the economic damage as a result of the distortion of the markets.

This article will briefly give an account of the negotiations of the Commission proposal for the PIF Directive (below 2.), outline in detail the key elements of the finally adopted legal instrument (below 3.) as well as its significance for the European Public Prosecutor's Office (below 4.). The article concludes (below 5.) that the comprehensive approach followed by the EU in fighting crime against the Union budget – with the new Directive, the envisaged European Public Prosecutor's Office, and, last but not least, the EU's Anti-Fraud Office (OLAF) being the constitutive elements – will lead to tangible results and a significantly better protection of the financial interests of the European Union.

#### II. Negotiations of the Commission Proposal for the Directive

The Commission proposal for the Directive was adopted on 11 July 2012,<sup>11</sup> based on Art. 325(4) TFEU. Compared to the PIF Convention and its protocols, the Commission proposal includes a comprehensive set of fraud and fraud-related of-

fences, more deterrent sanctions for “serious” offences, and also common rules on limitation periods.<sup>12</sup>

On 6 June 2013 already, the Council adopted its position on the Directive,<sup>13</sup> thereby departing from the Commission proposal on a number of points. The European Parliament issued its report on 16 April 2014,<sup>14</sup> suggesting a number of changes to the text as proposed by the Commission. In particular, the envisaged inclusion of VAT fraud within the scope of the Directive posed a great challenge in the negotiations, even giving rise to concerns that this initiative could fail as a whole.<sup>15</sup> Although not explicitly mentioned in the main body, recitals 4 and 5 of the Commission proposal made it clear that VAT fraud falls within the definition of the Union’s financial interests and hence the scope of the Directive. Opposition by the Council<sup>16</sup> against any inclusion of VAT fraud within the scope of the Directive, on the one hand, and strong support by Commission and Parliament<sup>17</sup> for an inclusion of VAT fraud, on the other, eventually led to a standstill in the negotiations in June 2015. This deadlock was only broken by the Court of Justice’s decision in the *Taricco* case,<sup>18</sup> when the negotiations were taken up again with new verve. And it was only after numerous meetings at the technical level as well as discussions at both the Justice and Home Affairs and the Economic and Financial Affairs Councils that a compromise solution and political agreement on the text of the Directive could eventually be found between Parliament and Council in January/February 2017.

The following section will examine in detail the compromise solutions found.<sup>19</sup> Before moving on to this section, however, one issue, though unrelated to the substance of the Directive, yet subject to lengthy legal debates, deserves special mention: the question of the legal basis of the Directive. While the Commission has based its proposal on Art. 325(4) TFEU, Council and Parliament have opted for an adoption on the basis of Art. 83(2) TFEU within the EU’s competence in the area of freedom, security and justice.

In the explanatory memorandum accompanying the Directive, the Commission provided the reasons why it based its proposal on Art. 325(4) TFEU.<sup>20</sup> The Commission argued that Art. 325 TFEU confers upon the Union strong powers to adopt measures that act as a deterrent and afford effective and equivalent protection. In order to achieve this aim, Art. 325 equips the EU itself with the power to enact measures not only in the fields of prevention but also in the fight against fraud and any other illegal activities affecting the Union’s financial interests, including by means of criminal law. Art. 325(4) TFEU provides for the legislative procedure to adopt these measures, whereby the term “fraud” within the meaning of this article has to be understood in a broad sense, i.e., including not only fraud but also certain fraud-related

criminal offences. This will ensure the necessary effective and equivalent protection of the Union’s financial interests, as required by Art. 325 TFEU.

The Commission moreover stressed that the fight against illegal activities affecting the Union’s financial interests is a very specific policy area, particularly highlighted by the very first article in the title on financial provisions in the TFEU, Art. 310(6), which underscores the obligation to fight illegal activities affecting the Union’s financial interests (“shall” provision). The Commission also pointed to a historical interpretation by arguing that contrary to the precursor of Art. 325 TFEU, namely Art. 280 (particularly para. 4) EC Treaty, the EU law today contains a criminal law dimension, including the power to enact criminal law provisions on the basis of Art. 325(4) TFEU.

This view has been challenged by Council and Parliament. In October 2012, the Legal Service of the Council issued an Opinion on this matter, in which it argued in favour of Art. 83(2) TFEU as the legal basis for the Directive.<sup>21</sup> It stated that the proposed Directive pursues the objective expressed in Art. 83(2) TFEU, which is to ensure the effective implementation of a Union policy (i.e., the protection of the EU’s financial interests).<sup>22</sup> It disagreed with the Commission’s stance that Art. 325 TFEU allows for measures under criminal law. The Legal Service of the Council further stressed that, compared to the previous Art. 280 EC Treaty, the absence of an explicit exclusion of criminal law measures in Art. 325 TFEU is insufficient to argue in favour of a legal basis for them. This is because the new legal basis in Art. 83(2) TFEU was meant to tackle all cases in which the EU legislature needs to harmonise the definition of criminal offences and sanctions in order to make other (non-criminal) harmonised EU measures more effective.<sup>23</sup>

Following this line of argument, Council changed the legal basis for the Directive to Art. 83(2) TFEU<sup>24</sup> and Parliament<sup>25</sup> shared this position. As a result thereof, the Directive falls within the scope of the opt-in/opt-out rules according to Protocols 21 and 22 on Ireland and the United Kingdom and Denmark, respectively: it will not apply to Denmark and the United Kingdom, while Ireland indicated that it will participate in this measure.

The opinion of the Council Legal Service as regards the legal basis for the Directive is not convincing. Art. 325 TFEU is a special provision, embedded in the Title regulating the composition and management of the EU budget, which aims at the widest possible and most effective protection of the financial interests of the Union. Unlike the precursor provision, Art. 280 EC Treaty, measures under Art. 325 TFEU may also



include those falling in the area of criminal law. The obligations enshrined in this provision are binding (“shall”) on all Member States and the Union, and they are not subject to any exemptions, such as measures under the Title on Freedom, Security and Justice. Also, the protection under Art. 325 TFEU is not striving to set minimum standards only but for a comprehensive and effective protection of the Union budget.

The measure undertaken in the case at hand – the adoption of the Directive – pursues its own policy purpose within the realm of the financial provisions of the TFEU; unlike Art. 83(2), it is not confined to indirectly making other EU harmonised measures more effective should this be proven to be essential. This *proof of essentiality* has been proffered by the Treaty for cases of combating fraud and other illegal activities affecting the financial interests of the Union. As laid out above, the grammatical, historical, systematic, and teleological interpretations all point to Art. 325(4) TFEU as the appropriate legal basis for the Directive. This interpretation does not deprive Art. 83(2) TFEU, which does not even mention crimes affecting the financial interests of the Union amongst the so called “Eurocrimes” listed in its first paragraph, of its effective scope of application in other areas of crime, while, by contrast, the interpretation of the Council and Parliament in favour of Art. 83(2) as the legal basis for the Directive, would deprive Art. 325(4) TFEU of an essential part of its content.

### III. Main Elements of the Directive

The duty to protect the Union’s financial interests, as enshrined in Art. 325 TFEU, calls for a comprehensive approach that includes preventive measures as well as civil law, administrative law, and, as an *ultima ratio*, criminal law measures.<sup>26</sup> The new Directive pursues this goal by laying down the foundation for a better protection of the Union’s financial interests by means of criminal law. This will be achieved by setting common standards as regards definitions of criminal offences affecting the financial interests of the Union (here under a) as well as in relation to sanctions (b) and limitation periods (c) for these offences. At the end, this section will briefly touch upon the remaining provisions of the Directive (d).

#### 1. Definitions of criminal offences

Central provisions on the definition of criminal offences affecting the Union’s financial interests are Arts. 3 and 4 in Title II of the Directive. The Directive builds upon the *acquis* of the PIF Convention and its accompanying protocols.<sup>27</sup> It modernises, extends, and, in some instances, narrows down the scope of the definitions.

Art. 2(1)(a) of the Directive defines the financial interests of the Union as being all revenues, expenditures, and assets covered by, acquired through, or due to the Union budget, as well as the budgets of the institutions, bodies, offices, and agencies established under the Treaties or budgets directly or indirectly managed or monitored by them, hence bringing about greater clarity on this point compared to the PIF Convention.

#### a) Fraud

As regards the offence of fraud affecting the Union’s financial interests (Art. 3), the Directive initially closely followed the PIF Convention; however, it underwent some substantial changes in the course of negotiations. This applies particularly to the now clear language on VAT fraud in Art. 3(2)(d).

Like the PIF Convention, the Directive differentiates between fraud in respect of expenditures and revenue. As far as expenditure is concerned, the definition has been concretised further compared to the PIF Convention, because the Council favoured making a distinction between non-procurement related expenditure, on the one hand (Art. 3 paragraph 2 lit. a), and procurement related expenditure, on the other (Art. 3 paragraph 2 lit. b). While the Directive follows the definition of the PIF Convention for fraud concerning non-procurement related expenditure, such as grants or other financial instruments, fraud concerning procurement-related expenditure, however, requires that it was committed in order to make an unlawful gain for the perpetrator or another person by causing a loss to the Union’s financial interests. Procurement-related expenditure means any expenditure in connection with the public contracts determined by Art. 101 paragraph 1 of Regulation No. 966/2012,<sup>28</sup> such as building contracts, supply contracts, works contracts, or service contracts between economic operators and the EU contracting authority.<sup>29</sup> In the case of procurement-related expenditure fraud, it is hence not sufficient that the fraudster aimed at obtaining an advantage; in addition, the damage must actually have been caused.

As far as revenue is concerned, the by far most controversial point was, as mentioned above, the question of whether and, if so, to what extent VAT fraud falls within the scope of the Directive. While Commission and Parliament strongly favoured that VAT fraud be included, the Council disagreed with this, stating that VAT is solely a national matter and that the damage resulting from VAT fraud only occurs in the EU Member State affected by it.

The PIF Convention itself did not exclude VAT from its scope, nor did it explicitly include it. In the Explanatory Report to the PIF Convention,<sup>30</sup> the Council took the view that, for the purpose of the PIF Convention, “revenue” means only customs

duties and certain agricultural levies and contributions, i.e., the first two categories of the European Union's own resources only. VAT was explicitly excluded by the Council, as VAT was not an own resource collected directly for the account of the Communities.

Against this view, the Commission, supported by the Parliament, stressed from the beginning that the general reference in the PIF Convention to the EU's financial interests means nothing other than that VAT falls within the ambit of that Convention and, accordingly, that VAT has to fall within the scope of the proposed Directive. Both Commission and Parliament pointed out that this would not only be desirable from a criminal policy perspective but, in particular, also in view of the significant damage that complex and serious VAT fraud cases cause each year, both to the national and EU budgets as well as to the Single Market in the EU.

It was at a time when the negotiations were stalled that the Court of Justice shed some light on this matter, which, in turn, led to a new dynamic on the question of VAT and the negotiations on the Directive as a whole. In the *Taricco* decision, the Court of Justice confirmed the Commission's view that VAT fraud falls under the scope of the definition of fraud in the PIF Convention.<sup>31</sup> The Court had already held earlier that VAT is an own resource of the Union and that there is a direct link between the collection of VAT by the Member States and the availability of the corresponding VAT resources to the European Union budget.<sup>32</sup>

In *Taricco*, the Court further stated that "criminal penalties may ... be essential to combat certain serious cases of VAT evasion in an effective and dissuasive manner"<sup>33</sup> and that the Member States must ensure that cases of serious VAT fraud and VAT evasion "are punishable by criminal penalties which are, in particular, effective and dissuasive."<sup>34</sup> In this light, there seemed no doubt that VAT fraud also falls within the scope of the Directive, since the Directive uses the same definition of fraud as the PIF Convention.

Despite these clarifying words by the Court, the Council maintained its view that VAT was excluded from the PIF Convention, as outlined in the Explanatory Report. However, Advocate General *Juliane Kokott* in the *Taricco* case already pointed out in her opinion<sup>35</sup> that only the Court is entitled to give an interpretation of the PIF Convention, which is legally binding within the European Union, not the Council's Explanatory Report, to which neither the Convention nor the third protocol make any reference.<sup>36</sup>

Following various meetings at the technical and political levels – including with Ministries of Finance – the majority of

Member States at the Economic and Financial Affairs Council on 11 October 2016 and at the Justice and Home Affairs Council on 14 October 2016 expressed their readiness to agree on a political compromise solution to the inclusion of VAT fraud within the scope of the Directive.<sup>37</sup> This solution however entails that not all VAT fraud cases but only serious offences against the common VAT system fall within the scope of the Directive (Art. 3(2)(d) jointly read with Art. 2(2)). That is, offences connected with the territory of at least two or more Member States, which result from a fraudulent scheme and involve a total damage of at least €10 million. The total damage of €10 million refers thereby to the estimated damage resulting from the entire fraud scheme, both to the financial interests of the Member States concerned and to the Union, excluding, however, interests and penalties due.

In order to dispel concerns on the part of various Member States, Art. 2(3) further stresses that the structure and functioning of the national tax administrations are not affected by the Directive.

The definition of VAT fraud in Art. 3(2)(d), read in conjunction with Art. 2(2), targets the most serious forms of VAT fraud, such as VAT carousel fraud, Missing-Trader Intra-Community (MTIC) fraud or fraud committed within a criminal organisation. It is understood in a broad way, so as to capture all of the possible forms of VAT fraud; however, some raised the concern that the definition of VAT fraud is not precise enough. The transposition and implementation process will therefore need to be carefully scrutinised. Art. 18 accordingly obliges the Commission to provide assessment reports on the extent to which Member States have complied with the Directive and the impact of national law transposing the Directive on the prevention of fraud to the Union's financial interests.

Even if only serious cross-border VAT fraud cases of at least €10 million fall within the scope of the Directive – by contrast, the PIF Convention, as construed by the Court of Justice, covers all VAT fraud cases – the need to establish a comprehensive set of rules on the protection of the Union's financial interests in the Directive, i.e. including VAT fraud, is evident. Even if this leads to a limited scope for VAT fraud offences in the PIF Directive, it has not been considered as viable to keep the PIF Convention in place for the purpose of VAT fraud only, as this would create a complex and in practice unworkable legal patchwork of two parallel legal instruments (Directive and PIF Convention). Moreover, Art. 18(4) explicitly foresees that the financial threshold of €10 million foreseen in Art. 2(2) of the Directive will be subject to scrutiny and review. It is in this light that the approach taken in the Directive has to be seen.

## b) Other criminal offences

Art. 4 governs other criminal offences than fraud affecting the Union's financial interests. This provision follows the *acquis* of the PIF Convention and its protocols but makes some important improvements and introduces a completely new offence of misappropriation.

The initial Commission proposal included a new offence in Art. 4(1) that concerned the abuse of public procurement procedures. This provision did not find support in the Council, as it was considered too far-reaching by criminalising conduct that is merely a breach of contractual obligations. Art. 4(1) of the finally adopted Directive now provides an updated reference to money laundering offences, thereby referring to Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (the "4th AML Directive").<sup>38</sup> It is of note in this context that, on 21 December 2016, the Commission adopted a proposal for a Directive on countering money laundering by criminal law.<sup>39</sup> This future Directive, which is still in the legislative process, will not, however, change anything with regard to money laundering related to the financial interests of the Union, as the PIF Directive will remain untouched as *lex specialis*.

Furthermore, the PIF Directive brings the offence of active and passive corruption (Art. 4(2)) in line with best practices and the United Nations Convention against Corruption by removing – compared to the PIF Convention – the element of "breach of duties" from the definition.

A new element of the Directive is the criminal offence of misappropriation (Art. 4(3)). This offence was not foreseen in the PIF Convention and its inclusion received broad support. This new offence will cover the conduct of a public official who is entrusted with the management of funds or assets and who spends these funds or assets contrary to the purposes for which they were initially intended and thereby damages the Union's financial interests. A prerequisite for the criminalisation of the offence is that such misappropriation has been committed intentionally.

For the purpose of the offences of corruption (Art. 4(2)) and misappropriation (Art. 4(3)), the Directive defines the meaning of a "public official" in Art. 4(4) in a wide manner, thereby extending the definition of public official to any other person who exercises a public service function. This notion hence also applies to private persons involved in the management of EU funds.

Linked to the list of offences are the general provisions on inciting, aiding and abetting, and attempt in Art. 5. Member

States are required to criminalise forms of preparation of and participation in the criminal offences listed in the Directive.

## 2. Sanctions for offences

In order to ensure an equivalent protection of the Union's financial interests throughout the EU, the inclusion of proportionate and dissuasive sanctions, which may involve a custodial sentence, is also essential. This aspect is of utmost importance in order to create a higher level of deterrence for committing PIF offences, as required by the Treaties and the jurisprudence of the Court of Justice.

The Directive follows the logic of the PIF Convention. While the PIF Convention foresaw that criminal conduct affecting the Union budget shall be punishable by effective, proportionate, and dissuasive criminal penalties and that other, non-criminal sanctions could be provided for minor cases below a threshold of 4000 ECU<sup>40</sup>, Art. 7(1) of the Directive similarly stipulates the obligation to punish the offences listed in Arts. 3, 4, and 5 by effective, proportionate, and dissuasive criminal sanctions. Art. 7(4), however, raises the criminalisation threshold to €10,000.

Like the PIF Convention, the Directive foresees in Art. 7(3) that the criminal offences referred to in Artt. 3 and 4, which cause considerable damage or advantage, are punishable by a maximum penalty of at least four years of imprisonment. Unfortunately the co-legislators did not take up the Commission's proposal to introduce minimum sanctions. Instead, the Directive now provides only for a maximum penalty of at least four years of imprisonment ("minimum maximum sanctions").

While the PIF Convention set the threshold at 50,000 ECU for serious fraud, the Directive presumes the damage or advantage to be considerable if the damage or advantage involves more than €100,000. Beyond the mere financial damage or advantage, however, the Art. 7(3) expands this scope to other serious circumstances defined under national law. For offences against the common VAT system, the Directive sets the threshold as of which the damage or advantage is to be considerable at €10 million, in line with Art. 2(2).

The Directive further states that when a criminal offence is committed within a criminal organisation in the sense of Framework Decision 2008/841/JHA, this also shall be considered an aggravating circumstance (Art. 8).

As regards the liability of and sanctions for legal persons (Arts. 6 and 9), the provisions of the Directive largely correspond to the obligations under Artt. 3 and 4 of the Second

Protocol of the PIF Convention. When legal persons are held liable for any of the listed criminal offences, they shall be subject to effective, proportionate, and dissuasive criminal or non-criminal sanctions. In line with the Second Protocol, the Directive includes a non-binding and non-exhaustive list of possible sanctions. Following the request of the Parliament, the sanction of “temporary or permanent exclusion from public tender procedures” was included in the list.

### 3. Limitation periods

An important new element of the Directive concerns the inclusion of limitation periods. This provision did not exist in the PIF Convention and governs the time periods within which criminal offences affecting the financial interests of the Union should be followed up and enforced. In Art. 12(1), the Directive foresees a general obligation for Member States to provide for a limitation period that enables the investigation, prosecution, trial, and judicial decision of criminal offences for a *sufficient period of time* after the commission of the offences listed in Arts. 3, 4, and 5.

A specific limitation period of five years has been introduced for serious offences punishable by a maximum sanction of at least four years of imprisonment (Art. 12(2)). Provided that the limitation period may be interrupted or suspended upon specified acts, Member States are allowed to establish an even shorter period than five years, however not shorter than three years (Art. 12(3)). As regards the enforcement part, the Directive stipulates that, within at least five years of the date of the final conviction, Member States are required to take the necessary measures to enable the enforcement of a penalty of more than one year of imprisonment or, alternatively, a penalty of imprisonment in case of a criminal offence punishable by a maximum sanction of at least four years of imprisonment (Art. 12(4)).

### 4. Other issues

Other issues covered by the Directive concern the freezing and confiscation of instrumentalities and proceeds (Art. 10), the establishment of jurisdiction (Art. 11), and rules on recovery (Art. 13). Furthermore, the Directive includes provisions clarifying the interaction between administrative and criminal sanctioning regimes (Art. 14) as well as the cooperation between the Member States and the Commission (OLAF) and other Union institutions, bodies, offices, or agencies, including Eurojust and the yet to be established European Public Prosecutor’s Office (Art. 15). Finally, the Directive governs the replacement of the Convention and its protocols (Art. 16) as

well as the transposition obligations for Member States and, the reporting duties for the Member States and the Commission (Arts. 17 and 18).

The Directive also includes a set of review clauses in Art. 18(4). The Commission has to assess, as mentioned above, the appropriateness of the threshold of €10 million applying to cross-border VAT fraud and furthermore the effectiveness of the provision relating to limitation periods. It must also assess whether the Directive effectively addresses cases of procurement fraud, given that this new specific provision has been removed from the initial Commission proposal.

## IV. Significance of the Directive for the European Public Prosecutor’s Office

The Directive will not solely serve as an instrument to harmonise the criminal law of the Member States in the area of fraud against the EU budget; it will also be of essential importance to the future European Public Prosecutor’s Office (hereinafter: EPPO), as it provides for the material scope of the criminal offences falling within the EPPO’s competence. The Directive and EPPO are fully interlinked and have to be considered together as key elements of the comprehensive approach towards a stronger protection of the Union budget. Whereas the Directive lays down the foundation of harmonising criminal offences, sanctions, and limitation periods, the EPPO will play a key role in investigating, prosecuting and enforcing these offences in practice.

A general approach on the Regulation establishing the European Public Prosecutor’s Office under enhanced cooperation was reached by 20 Member States at the Justice and Home Affairs Council of 8 June 2017.<sup>41</sup> While the Regulation has undergone several changes throughout the course of the negotiations, the EPPO’s main features remain. The EPPO will be an independent and highly specialised European prosecutorial body fully equipped with investigatory and prosecutorial powers. As a single office, it will operate across all participating Member States in real-time, thus allowing for round-the-clock information exchanges, coordinated police investigations, fast freezing or seizure of assets, and arrests on the basis of a common European investigation and prosecution strategy.

Once established, the EPPO will help overcome the current fragmented efforts to fight offences affecting the Union’s financial interests. There will be no need for lengthy and complicated *ad hoc* cooperation between different national authorities on a case-by-case basis. The establishment of the Office is expected to lead to a greater number of prosecutions, convictions, and a higher level of recovery of fraudulently lost Union funds.<sup>42</sup>



The EPPO will work closely with the EU's anti-fraud watchdog, OLAF. The EPPO Regulation clarifies that the EPPO and OLAF will maintain a close relationship with due respect for their distinct mandates. It ensures that there will be no overlaps or duplication of work between the EPPO and OLAF and that the Union budget is, hence, protected in the widest possible manner. An evaluation of OLAF Regulation 883/2013 is currently ongoing and may lead to legislative changes so as to reflect the future relationship between OLAF and the EPPO.

The competence of the EPPO is defined by reference to the PIF Directive, as implemented by national law.<sup>43</sup> An interesting legal discussion in this regard concerns the choice of the legal instrument, i.e. Directive or a Regulation, in order to define the EPPO's competence.<sup>44</sup> Since a Directive allows Member States some leeway in its transposition, variations in national rules could occur. For the EPPO, this would mean that the way in which Member States transpose the Directive, to a certain extent affects the competence of the Office as well as, potentially, the rights of defendants subject to EPPO investigations to the extent the differences in transposing the Directive would impact upon their rights. Certainly, a Regulation containing criminal offences falling within the EPPO's competence would bring about greater clarity and legal certainty. Adopting a Regulation with the material law for the EPPO on the basis of Art. 86(1) TFEU or Art. 325(4) has, for various, not least also political, reasons, not been considered viable. A "PIF Regulation", compared to a "PIF Directive", would be the more "intrusive" legal instrument on the national legal systems. Furthermore, a Directive, as transposed into national law, is also in line with the fact that the EPPO will, for a large part, rely on national law to conduct its investigations and will eventually bring its prosecutions before national courts. Operating on the basis of a Directive therefore appears more practical in ensuring successful investigations and prosecutions in the Member States.

Moreover, the EPPO Regulation and the Directive have built in certain safeguards to ensure legal certainty. Member States have to supply the EPPO with a list of the national substantive criminal law provisions, as transposed on the basis of the Directive, and any other relevant national law.<sup>45</sup> Similarly, Member States are obliged to communicate the transposed measures to the Commission, on the basis of which the Commission will assess and report the extent to which the Member States have taken the necessary measures to comply with the Directive.<sup>46</sup> This will enable the EPPO to operate on the basis of a clear set of criminal offences, while at the same time respecting the national judicial systems and traditions.

## V. Conclusions

Although the Directive is not as far-reaching as initially proposed by the Commission, it constitutes a significant improvement by setting a more modern and more comprehensive set of rules to better fight fraud and other offences affecting the EU budget. In particular, in conjunction with the operations of the EPPO, both, the Directive and the EPPO Regulation, will jointly be a cornerstone in fighting PIF crimes more effectively by means of criminal law, while OLAF may continue with its administrative investigations as a complementary measure<sup>47</sup>. The Directive has to be seen in this context – as part of the EU's comprehensive approach towards protecting its financial interests.

While the Directive has only been adopted recently, it will surely not mark the end of the EU's legislative action to protect its financial interests. Not least with the reporting and assessment provision foreseen in Art. 18, the Directive will maintain a dynamic character in order to further enhance the fight against crimes affecting the financial interests of the Union in the future.

\* The authors are desk officers for the negotiations on the European Public Prosecutor's Office (EPPO) and the PIF Directive, Directorate General for Justice, Consumers and Gender Equality, European Commission. The views set out in this article are those of the authors and do not necessarily reflect the official opinion of the European Commission.

1 Regular updates on the state of play of the negotiations have been provided in eucrim.

2 Six Member States voted against the Council's position at first reading of 25 April 2017, namely Cyprus, Germany, Hungary, Ireland, Malta and Poland, but they were not able to reach a blocking minority in accordance with the applicable voting rules in the legislative procedure.

3 Directive of 5 July 2017 (PE-CONS 32/17). Published in the Official Journal on 28 July 2017 (*O.J. L* 198, 28.07.2017, 29).

4 Based on Protocol nos. 21 and 22 of the Lisbon Treaty.

5 *O.J. C* 316, 27.11.1995, 48.

6 Protocol of 27.11.1996 (*O.J. C* 313, 23.1.1996, 1); Protocol of 29.11.1996 (*O.J. C* 151, 20.5.1997, 1); Protocol of 19 June 1997 (*O.J. C* 221, 19.7.1997, 11).

7 I.e. it will remain in force for Denmark and the UK.

8 Protection of the European Union's financial interests – Fight against fraud 2015 Annual Report, COM(2016) 472 final of 14 July 2016 and Protection of the European Union's financial interests – Fight against fraud 2014 Annual Report, COM(2015) 386 final of 31 July 2015.

9 Communication from the Commission and Commission staff working paper on the protection of the financial interests of the European Union by criminal law and by administrative investigations – COM(2011) 293 final of 26 May 2011 and SEC(2011) 621 final of 26 May 2011.

10 Cf. V. Jourova, “The Cost(s) of Non-Europe in the Area of Freedom, Security and Justice – The European Public Prosecutor’s Office as a Guardian of the European Taxpayers’ Money,” (2016) *eu crim*, 94 et seqq. with further references.

11 Proposal for a Directive of the European Parliament and of the Council on the fight against fraud to the Union’s financial interests by means of criminal law, COM(2012) 363 final.

12 For the contents of the proposal and its background, see also L. Kuhl, “The Initiative for a Directive on the Protection of the EU Financial Interests by Substantive Criminal Law”, (2012) *eu crim*, 63–66.

13 General Approach on the PIF Directive of 10 June 2013 (Council document: 10729/13).

14 Cf. European Parliament position at first reading of 16 April 2014, Document P7\_TA(2014)0427.

15 See also T. Wahl, *eu crim* 2016, p. 9.

16 General Approach on the PIF Directive of 10 June 2013 (Council document: 10729/13).

17 Cf. European Parliament position at first reading of 16 April 2014, Document P7\_TA(2014)0427.

18 Judgment of the Court (Grand Chamber) of 8 September 2015, case C-105/14, *Ivo Taricco and others*.

19 See below 3.

20 Point 3.1 of the Explanatory Memorandum of COM(2012) 363 final, *op. cit.* (n. 11).

21 Opinion of the Legal Service of 22 October 2012 (Council document: 15309/12).

22 Point 10 of the Opinion, *op. cit.*

23 Points 11 and 12 of the Opinion, *op. cit.*

24 With the change to Art. 83(2) TFEU as the legal basis the ordinary legislative procedure remained, however, with the procedural specificities foreseen in Art. 83(3) TFEU (the so called “emergency break”).

25 The Parliament agreed to change the legal basis in its position at first reading of 16 April 2014, following an opinion of the Parliament’s Committee on Legal Affairs of 27 November 2012, which considered that Art. 83(2) TFEU was a *lex specialis* with regard to Art. 325(4) TFEU, cf. document PE500.747v02-00, included in the Parliament’s report of 25 March 2014 (A7-0251/2014). On 22 May 2013 the Legal Service of the Parliament issued a legal opinion on the consequences of this choice, without taking a position as to its correctness, cf. document SJ-0320/13.

26 The area of the protection of the Union’s financial interests has been already subject of harmonisation measures, such as Regulation No 2988/95 relating to homogenous checks and to administrative measures and penalties.

27 Cf. notes 5 and 6 above.

28 Regulation No 966/2012 of the European Parliament and of the Council of 25 October 2012 on the financial rules applicable to the general budget of the Union (*O.J. L* 298, 26.10.2012, 1).

29 Cf. Arts. 101, 117 and 190 of Regulation No 966/2012.

30 Explanatory Report on the Convention on the protection of the European Communities’ financial interests, approved by the Council on 26 May 1997 (*O.J. C* 191, 23.06.1997,1); in the report, see in particular the explanations relating to Art. 1(1) of the Convention (*O.J. C* 191,23.06.1997, 4, last paragraph).

31 CJEU, *Taricco*, *op. cit.* (n. 18), para. 41.

32 CJEU, 15 November 2011, case C-539/09, *-European Commission v Federal Republic of Germany*, para. 72; CJEU, 26 February 2013, case C-617/10, *Åklagaren v Hans Åkerberg Fransson*, para. 26).

33 CJEU, *Taricco*, *op. cit.* (n. 18), para. 39.

### Adam Juszcak

Directorate General for Justice, Consumers and Gender Equality, European Commission



### Elisa Sason

Directorate General for Justice, Consumers and Gender Equality, European Commission



34 CJEU, *Taricco*, *op. cit.* (n. 18), para. 43.

35 Cf. Opinion of Advocate General Kokott, 30 April 2015, case C-105/14, *Ivo Taricco and Others*, para. 97.

36 AG Kokott continued by stating that this was made apparent from the very outset by the additional protocol to the PIF Convention, which empowered the Court to interpret that convention. Today, this follows from the second sentence of Art. 19(1) TEU, Art. 19(3) TEU, and Article 267 TFEU.

37 See also T. Wahl, (2016) *eu crim*, 158.

38 *O.J. L* 141, 5.6.2015, 73.

39 Proposal for a Directive of the European Parliament and of the Council on countering money laundering by criminal law, COM(2016) 826 final of 21 December 2016. See also T. Wahl, (2016) *eu crim*, 159.

40 European Currency Unit.

41 A general approach was reached by 20 Member States (Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Estonia, Finland, France, Germany, Greece, Italy, Latvia, Lithuania, Luxembourg, Portugal, Romania, Slovakia, Spain, and Slovenia) on the basis of the draft Regulation implementing enhanced cooperation on the establishment of the EPPO of 2 June 2017 (Council document: 9545/2/17). See also the news section in this issue.

42 European Commission press release IP/17/1550 of 8 June 2017 ([http://europa.eu/rapid/press-release\\_IP-17-1550\\_en.htm](http://europa.eu/rapid/press-release_IP-17-1550_en.htm)) and Council of the EU press release 333/17 of 8 June 2017. (<http://www.consilium.europa.eu/en/press/press-releases/2017/06/08-epo/>).

43 Art. 22 of the draft EPPO Regulation of 30 June 2017 (Council document: 9941/17).

44 These points were also raised by the Committee of the Regions in its opinion of 30 January 2014 (2014/C 126/10) as well as by some Member States.

45 Art. 117 of the draft EPPO Regulation of 30 June 2017 (Council document: 9941/17).

46 Art. 17 of the PIF Directive.

47 Of course OLAF will continue as before in respect of Member States which do not participate in the EPPO.

# Reform des europäischen Datenschutzrechts

## Ein Überblick unter besonderer Berücksichtigung des Datenaustausches zwischen Polizei-, Strafjustiz- und Geheimdienstbehörden

Petra Beckerhoff

Data protection is one of today's most important challenges. Cross-border crime, terrorist risks, and new technologies all contribute to an increase in the collection and movement of personal data. This contribution first gives an overview of the content of the recently reformed European data protection law, i.e. the General Data Protection Regulation (GDPR). It also provides an analysis of Directive 2016/680, which regulates the specific protection of personal data in the prevention, investigation, detection and prosecution of criminal offences as well as the enforcement of criminal penalties. The article further outlines current projects and new developments regarding data transmission between intelligence agencies and prevention/prosecution authorities. It also focuses on the principle of limitation for the purpose of data use as well as the "compatibility" of operation purposes as rules for restricting data processing. The paper concludes by recommending the creation of harmonised and clear rules for data transmission with the intelligence agencies.

### I. Einleitung

Die jüngste europäische Datenschutzreform besteht mit der ab dem 25. Mai 2018 in allen Mitgliedstaaten anzuwendenden EU-Datenschutzgrundverordnung (DS-GVO)<sup>1</sup> und der bis zum 6. Mai 2018 national umzusetzenden Richtlinie (EU) 2016/680<sup>2</sup> aus zwei Bestandteilen. Diese bilden im europäischen Datenschutzrecht die größte Neugestaltung seit der Datenschutzrichtlinie 95/46 (EG)<sup>3</sup> und legen erstmalig auch unionsweit einen Mindeststandard für den Datenschutz bei Polizei und Justiz fest.

Mit der Schaffung eines einheitlichen Schutzniveaus werden zugleich auch die Voraussetzungen für eine informationelle Zusammenarbeit zwischen den Strafverfolgungs- und Gefahrenabwehrbehörden geschaffen. Angesichts der aktuellen Herausforderungen durch die grenzüberschreitende Kriminalität und die terroristische Bedrohung wird ein Austausch relevanter Informationen verstärkt gefordert. Zudem können aufgrund von technischen Entwicklungen in zunehmend großem Umfang Daten verarbeitet, ausgetauscht und verknüpft werden. Allerdings ist ein Austausch von Informationen zwischen den Sicherheitsbehörden – einschließlich den Nachrichtendiensten – wegen der unterschiedlichen Aufgabenbereiche zumeist mit einer Änderung der Zweckbestimmung der Daten verbunden. Überdies handelt es sich oftmals um Daten, die mit eingriffsintensiven und aufgabenspezifischen Befugnissen und Methoden erhoben worden sind. Der Datenaustausch verlangt daher eine Balance zwischen den Interessen einer effektiven Strafverfolgung und Gefahrenabwehr einerseits und dem Schutz der Grund- und Menschenrechte

des Einzelnen bei der Verarbeitung der ihn betreffenden Daten andererseits.

Mit dem vorliegenden Beitrag sollen neben den wesentlichen Inhalten der DS-GVO und der Richtlinie (RL) (EU) 2016/680 auch die aktuellen Bestrebungen im europäischen Datenschutz sowie die neueren Entwicklungen beim Ausbau und bei der Nutzung der Möglichkeiten des Informationsaustausches eingegangen werden. Beleuchtet wird dabei insbesondere der Zweckbindungsgrundsatz, dem bei der Zulässigkeit einer Zweckänderung von Informationen besondere Bedeutung zukommt.

### II. Die Datenschutz-Grundverordnung (DS-GVO)

Die folgende Darstellung der grundlegenden Strukturen und wesentlichen Neuerungen der DS-GVO soll bereits mit Blick auf die gleichzeitig erlassene, in der öffentlichen Diskussion jedoch weniger beachteten RL (EU) 2016/680 zum Datenschutz bei Polizei und Justiz erfolgen (unten III.).

#### 1. Zielsetzung

Unter Bezugnahme auf den der RL 95/46 (EG) zugrundeliegenden Harmonisierungsgedanken betont die neue Verordnung vor allem den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten. Die Schaffung eines unionsweit gleichmäßigen Schutzniveaus soll den freien Verkehr personenbezogener Da-

ten im Binnenmarkt ermöglichen und der technisch und integrativ bedingten deutlichen Zunahme der Erhebung und des Austausches personenbezogener Daten gerecht werden.<sup>4</sup>

## 2. Anwendungsbereich

Die DS-GVO betrifft nach Art. 2 grundsätzlich die gesamte Verarbeitung personenbezogener Daten im Anwendungsbereich des Unionsrechts. Der Begriff der Verarbeitung von Daten schließt alle in Art. 4 Nr. 2 DS-GVO im Einzelnen genannten Datenverarbeitungsvorgänge ein, und damit neben der Ersterhebung auch die für den Datenaustausch mögliche Abfrage und Übermittlung. Nicht in den Anwendungsbereich fallen Datenverarbeitungsvorgänge, die die nationale Sicherheit und die Gemeinsame Außen- und Sicherheitspolitik der Union betreffen.<sup>5</sup> Der Bereich der nationalen Sicherheit umfasst den Verteidigungsbereich und auch die Tätigkeiten der Inlands- und Auslandsgeheimdienste.<sup>6</sup> Mit der Ausnahmeregelung des Art. 2 III DS-GVO ist auch die Datenverarbeitung durch die EU und ihre Institutionen ausgenommen. Hierfür gilt zunächst weiterhin die VO (EG) 45/2001.<sup>7</sup>

Nicht in den Anwendungsbereich der DS-GVO einbezogen sind nach dessen Art. 2 II ferner Datenverarbeitungen zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich der Datenverarbeitung zum Schutz vor und zur Abwehr von Gefahren für die öffentliche Sicherheit, sowie zum freien Verkehr dieser Daten. Hierfür gilt die neue RL (EU) 2016/680. Wie sich aus Erwägungsgrund (im Folgenden: EW) Nr. 19 der DS-GVO ergibt, soll die Abgrenzung nicht nach der institutionell organisatorischen Einordnung der Behörde, sondern nach dem Zweck erfolgen, zu dem die Datenverarbeitung erfolgt. Diese Betrachtung ist auch bei der Abgrenzung der einzelnen Datenverarbeitungsschritte heranzuziehen. In der Begründung zur Verordnung heißt es dazu, dass auch personenbezogene Daten, die von der Behörde nach der DS-GVO verarbeitet werden, dann der RL (EU) 2016/680 unterliegen sollten, wenn die Daten zu den in der RL genannten Zwecken verwendet werden.<sup>8</sup> Korrespondierende Ausführungen enthalten auch Art. 9 I 2, II der RL (EU) 2016/680 sowie die Erläuterungen in EW 34 der RL. Für einen Datenaustausch bedeutet dies, dass für die Ersterhebung der Daten durch die übermittelnde Behörde einerseits und die Verwendung der Daten durch den Empfänger andererseits auch unterschiedliche Rechtsgrundlagen maßgeblich sein können. Je nachdem, ob der jeweilige Datenvorgang zu den Zwecken der DS-GVO oder der RL (EU) 2016/680 erfolgt, beurteilt sich die Rechtmäßigkeit der Datenverarbeitung nach den Bestimmungen der DS-GVO oder den zur Umsetzung der Richtlinie ergangenen nationalen Bestimmungen. Als Beispiel kann der Abruf von Bankdaten

zum Zwecke der Ermittlung, Aufdeckung oder Verfolgung von Straftaten genannt werden.

Die unmittelbar in den Mitgliedstaaten geltende Verordnung lässt den nationalen Gesetzgebern durch Öffnungsklauseln einige Spielräume zur Konkretisierung und Regelung.<sup>9</sup> Diese betreffen beispielsweise die Rechtmäßigkeit von Datenverarbeitungen im öffentlichen Interesse und ihre Zweckbindung, die Verarbeitung besonderer Kategorien von Daten oder den Datenschutzbeauftragten.<sup>10</sup>

## 3. Grundsätze der Datenverarbeitung

Der Katalog der Grundsätze, die jede Datenverarbeitung gemäß Art. 5 DS-GVO erfüllen muss, ist im Vergleich zur RL 95/46 um weitere unstrittige Datenschutzprinzipien, wie Vertraulichkeit und Rechenschaftspflicht, ergänzt worden. Der insbesondere für den Datenaustausch bedeutsame Zweckbindungsgrundsatz ist in Art. 5 I b) DS-GVO definiert. Danach müssen personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesem Zweck nicht zu vereinbarenden Weise weiterverarbeitet werden. Die Voraussetzungen für die Zulässigkeit eines Datenaustausches werden durch den Grundsatz der Vereinbarkeit der Zwecke von Ersterhebung und geänderter Nutzung normiert.

Konkretisierungen, aber auch Ausnahmetatbestände zur Zweckbindung finden sich fernerhin in den Bestimmungen zur Rechtmäßigkeit der Verarbeitung (Art. 6 III und IV DS-GVO), welche im EW 50 näher erläutert werden. Für den Fall der Vereinbarkeit von Erhebungs- und Weiterverarbeitungszweck sei, so EW 50 der Verordnung, keine andere gesonderte Rechtsgrundlage erforderlich als diejenige für die Erhebung der personenbezogenen Daten. Für die Beurteilung der Vereinbarkeit sieht Art. 6 IV DS-GVO eine nicht abschließende Auflistung maßgeblicher Kriterien vor. Zugleich folgt aus Art. 6 IV DS-GVO eine weitere Einschränkung: Hat die betroffene Person ihre Einwilligung erteilt oder beruht die Verarbeitung auf Unionsrecht oder dem Recht der Mitgliedstaaten, was in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz insbesondere wichtiger Ziele des allgemeinen öffentlichen Interesses darstellt, sollen die Daten ungeachtet der Vereinbarkeit der Zwecke weiterverarbeitet werden dürfen. Die Verordnung sieht beim Schutz hochrangiger Interessen eine Zweckänderung somit grundsätzlich als gerechtfertigt an.

Die Verordnung zeigt damit bereits einige Aspekte der grundlegenden Problematik der Zulässigkeit von Zweckänderungen auf. Das Bundesverfassungsgericht hat in einer neueren



Entscheidung zur Verfassungsmäßigkeit des Gesetzes für das Bundeskriminalamt das Kriterium der Vereinbarkeit durch das Prinzip der hypothetischen Datenneuerhebung ersetzt, womit die früheren Maßstäbe an eine Zweckänderung teilweise zurückgenommen werden.<sup>11</sup> Auch wenn an dieser Stelle nicht auf die Einzelheiten der Voraussetzungen einer Zweckänderung eingegangen werden kann, sollen einige Gesichtspunkte kurz aufgezeigt werden. Fraglich ist danach, welcher Maßstab für den Begriff der Vereinbarkeit gelten sollte; in Betracht kommt eine Entsprechung der Zweckbestimmung oder, wie es die DS-GVO nahelegt, eine Interessenabwägung. Eine Rolle können auch die Mittel und Methoden der Erlangung der Daten oder die Erhebungsvoraussetzungen spielen. Eine weitere Frage ist, ob eine Rechtsgrundlage für jeden Datenverarbeitungsschritt zu fordern ist. Ferner kann bereits der Konkretisierungs- bzw. Abstrahierungsgrad der ursprünglichen Zweckbestimmung ein entscheidendes Kriterium für das Vorliegen einer Zweckänderung sein. Auch der Zeitpunkt ist für die Beurteilung der Vereinbarkeit von Bedeutung.<sup>12</sup> Schließlich dürfte nach der deutschen höchstrichterlichen Entscheidung als Maßstab für die Zweckbindung das Verhältnis zwischen dem Kriterium der Vereinbarkeit und der Rechtsfigur der hypothetischen Datenneuerhebung eine gesonderte Betrachtung erfordern.

#### 4. Wesentliche Neuerungen

Die wesentlichen Neuerungen der DS-GVO betreffen die Rechte des Betroffenen, technische und organisatorische Anforderungen an Datenschutz bzw. Datensicherheit, die Übermittlung von Daten an Drittstaaten sowie Aufsichts- und Sanktionsmaßnahmen. Darüber hinaus bringt die Verordnung Veränderungen beim Beschäftigten-Datenschutz und der Auftragsdatenverarbeitung.

Ein Anliegen der DS-GVO ist es, die Verarbeitung der Daten für den Betroffenen fair und transparent zu gestalten. Dazu ist der Umfang der Informationen, die dem Betroffenen nach Art. 13 und 14 DS-GVO im Vergleich zur RL 95/46 (EG) mitgeteilt werden müssen, erweitert worden. Zusammen mit dem Auskunftsrecht bilden die Informationspflichten schon zumeist rein tatsächlich die Voraussetzung dafür, die Rechtmäßigkeit der Datenverarbeitung überprüfen zu lassen und Rechte wie das Recht auf Berichtigung, Löschung Widerspruch und Beschwerde geltend machen zu können. Die DS-GVO enthält in Art. 12 Vorgaben über Aufbereitung der Information für den Betroffenen, die auch spezielle Vorgaben für an Kinder zu richtende Informationen beinhalten. Das auch als „Recht auf Vergessenwerden“ bezeichnete Lösungsrecht wird im Hinblick auf das Internet nach Art. 17 DS-GVO ausgeweitet und ein Recht auf Datenportabilität (Art. 20 DS-GVO) wird eingeführt.

Im Bereich der technischen und organisatorischen Anforderungen sind auf europäischer Ebene die Bestellung eines Datenschutzbeauftragten, eine Datenschutz-Folgenabschätzung, Zertifizierungs- sowie Melde- und Dokumentationspflichten statuiert.<sup>13</sup> Das technische Konzept der *Privacy by Design* und *by Defaults* wird geregelt.<sup>14</sup>

Der Datentransfer in Staaten außerhalb der EU folgt nach Art. 44 ff DS-GVO weiterhin dem Grundsatz der Angemessenheit, über den die Kommission entscheidet; er wird jedoch durch zwei weitere Bestimmungen zur Möglichkeit der Datenübermittlung vorbehaltlich geeigneter Garantien und – als Ausnahmetatbestand konzipiert – derjenigen für den Fall berechtigter Interessen erweitert.

Überdies sind Aufgaben und Befugnisse der Aufsichtsbehörden überarbeitet worden. Für grenzüberschreitende Datenverarbeitungen gilt zukünftig das Prinzip einer einheitlichen Aufsichtsbehörde, das sog. One-Stop-Shop-Prinzip. Weitere Neuerungen betreffen Sanktions- und Haftungsbestimmungen.

### III. Richtlinie (EU) 2016/680 zum Datenschutz bei Polizei und Justiz

Die Richtlinie (EU) 2016/680 entspricht hinsichtlich des Aufbaus und vieler Regelungsinhalte weitgehend der gleichzeitig verkündeten DS-GVO. Sie ersetzt den Rahmenbeschluss 2008/977/JI<sup>15</sup> des Rates und gilt im Unterschied zu diesem nicht nur für die grenzüberschreitende, sondern auch für die innerstaatliche Datenverarbeitung.

#### 1. Zielsetzung

Ziele der RL sind nach Art. 1 II die Grundrechte natürlicher Personen, insbesondere deren Recht auf Schutz personenbezogener Daten, zu schützen und gleichzeitig den ungehinderten Datenverkehr im Polizei- und Justizbereich zu erleichtern. Um jedoch ein hohes Schutzniveau zu gewährleisten, erhalten die Mitgliedstaaten nach Art 1 III der RL (EU) 2016/680 ausdrücklich die Möglichkeit, strengere Garantien für die Datenverarbeitung festzulegen, als sie in der Richtlinie vorgesehen sind, was zulasten einer Vollharmonisierung geht.

#### 2. Anwendungsbereich

Der Anwendungsbereich wird durch den Gegenstand der Datenverarbeitung nach Art. 1 I RL (EU) 2016/ 680 bestimmt, durch den auch die Abgrenzung zur DS-GVO erfolgt. Wie die DS-GVO ist auch die Richtlinie nicht auf den Bereich der nati-

onalen Sicherheit und auf die Institutionen der EU anwendbar, sodass die Datenverarbeitung durch die Nachrichtendienste sowie durch Europol und Eurojust ausgenommen sind. Für den Austausch mit Interpol soll die Richtlinie neben dem Gemeinsamen Standpunkt 2005/ 69/JI und dem Beschluss 2007/533/ JI des Rates anwendbar sein.<sup>16</sup> Im Unterschied zur DS-GVO differenziert die Richtlinie, dem spezifischen Schutzgedanken entsprechend, zwischen verschiedenen Datenkategorien, wie die des Verdächtigen, der Opfer oder Zeugen und den unterschiedlichen Grundlagen der Daten.

### 3. Grundsätze der Datenverarbeitung

Art. 4 I RL (EU) 2016/680 enthält, wie die DS-GVO, grundlegende Prinzipien für die Datenverarbeitung, zu denen auch der Grundsatz der Zweckbindung zählt. Art. 4 I b) RL (EU) 2016/680 knüpft die Datenverarbeitung zu anderen Zwecken, als zu denen sie erhoben worden sind, ebenfalls an die Vereinbarkeit der Zweckbestimmung von Datenerhebung und Datenverarbeitung. Die Bestimmungen der Richtlinie zur Zweckänderung gehen jedoch nicht so weit wie die der DS-GVO, was unter anderem dadurch begründet ist, dass die Richtlinie den Mitgliedstaaten Regelungsspielräume lässt. Art. 4 II RL (EU) 2016/680 sieht lediglich vor, dass für die Verarbeitung der Daten innerhalb der Zwecksetzung der Richtlinie eine Rechtsgrundlage besteht und die Datenverarbeitung für den neuen Zweck erforderlich und verhältnismäßig ist.

Für die Zweckänderung durch Datenübermittlung sieht Art. 9 III RL (EU) 2016/680 vor, dass besondere Bedingungen, die für die Datenverarbeitung gelten, auch vom Datenempfänger eingehalten werden sollen. Dies soll jedoch nach Art. 9 IV RL (EU) 2016/680 nur gelten, sofern die besonderen Bedingungen auch für entsprechende Datenübermittlungen im innerstaatlichen Recht vorgesehen sind und insoweit eine Gleichbehandlung gewährleistet ist.

### 4. Wesentliche Neuerungen

Die wesentlichen Neuerungen der Richtlinie sind im Kern denen der DS-GVO ähnlich. Dies gilt beispielsweise für die Informations- und Löschungspflichten, die Rechtsbehelfe sowie die Regelungen zum Datenschutzbeauftragten, zum technischen Datenschutz und zur Datenschutz-Folgenabschätzung. Entsprechungen zur DS-GVO bestehen auch bei der Datenübermittlung an Drittstaaten und den Kontrollmechanismen. Abweichungen erfolgen teilweise dem spezifischen Anwendungsbereich der RL entsprechend, um Ermittlungen nicht zu gefährden oder einem besonderen Schutzbedürfnis gegenüber den Ermittlungen gerecht zu werden.<sup>17</sup>

## IV. Aktuelle Reformbestrebungen

Mit den jüngsten umfangreichen Reformen ist der Erneuerungsprozess nicht abgeschlossen. Bereits am 10. Januar 2017 hat die Kommission im Rahmen der Digitalen Binnenmarktstrategie ein weiteres Datenschutz-Reformpaket vorgelegt, das zeitgleich mit der DS-GVO ab dem 25. Mai 2018 anwendbar sein soll. Dieses beinhaltet einen Vorschlag für die Verarbeitung personenbezogener Daten durch die Organe und Institutionen der EU, der die derzeit geltende VO (EG) 45/2001 ersetzen soll.<sup>18</sup> Der Entwurf orientiert sich zwar an der DS-GVO, lässt neben speziellen anwendungstypischen Abweichungen aber auch Beschränkungen durch die EU-Institutionen zu.

Das Reformpaket sieht ferner eine Neuordnung der für die elektronische Kommunikation geltenden Datenschutz-Richtlinie 2002/58 (EG) vor.<sup>19</sup> Diese sogenannte E-Datenschutz-Richtlinie regelt die Verarbeitung personenbezogener Daten durch öffentlich zugängliche elektronische Kommunikationsdienste in der EU. Sie erfasst auch die Verarbeitung von Verkehrsdaten. Diese sind wiederum auch Gegenstand der äußerst streitigen sog. Vorratsdatenspeicherung.

Im Rahmen der Bewältigung technischer Herausforderungen plant die Kommission auch eine Initiative zum Aufbau einer europäischen Datenwirtschaft.<sup>20</sup> Durch die Initiative soll der freie grenzüberschreitende Datenverkehr in der EU ermöglicht werden, indem ungerechtfertigte nationale Beschränkungen, die nicht dem Grundrechtsschutz dienen, abgebaut werden und insbesondere die durch neue Datentechniken aufgeworfenen Zugangs-, Eigentums- und Haftungsfragen geklärt werden. Für den ungehinderten Datenfluss als Voraussetzung für die Grundfreiheiten des EU-Binnenmarktes soll ein sicherer Rechtsrahmen geschaffen werden, damit Daten über die gesamte Wertschöpfungskette hinweg für wissenschaftliche, gesellschaftliche und industrielle Prozesse genutzt werden können. Die Regelungen sollen auch nicht personenbezogene maschinengenerierte Daten umfassen und können einen Beitrag zur Industrie 4.0 leisten, bei der industrielle Produktionsprozesse mit moderner Informations- und Kommunikationstechnik vernetzt sind.<sup>21</sup>

Der europäische Datenschutz steht jedoch noch vor weiteren Herausforderungen. Vor dem Hintergrund terroristischer Bedrohungen regt die Europäische Kommission die Einrichtung eines sog. Drehkreuzes für den Informationsaustausch an, um einen effektiven und zeitnahen Informationsaustausch auch zwischen den Strafverfolgungsstellen und den Nachrichtendiensten herzustellen.<sup>22</sup> Ein Austausch zwischen den nationalen Diensten findet in der derzeit außerhalb des EU-Rahmens bestehenden Gruppe für Terrorismusbekämpfung

(CTG) statt.<sup>23</sup> Eine Zusammenarbeit von Strafverfolgungsstellen und Nachrichtendiensten soll im Rahmen der geltenden EU-Verträge mit den zuständigen Mitgliedstaaten im Wege „praktischer Lösungen“ erfolgen und bei Europol angesiedelt werden.<sup>24</sup> Aus Deutschland können Erfahrungen des Terrorismusabwehrzentrums in Berlin eingebracht werden.

Auf der Grundlage der seit dem 1. Mai 2017 geltenden neuen Europol-Verordnung VO (EU) 2016/794<sup>25</sup> sollen Europol und insbesondere das dort eingerichtete Europäische Zentrum zur Terrorismusbekämpfung weiter ausgebaut werden.<sup>26</sup> Die Europol-Verordnung enthält ebenfalls Datenschutzregelungen, insbesondere die Statuierung des Zweckbindungsgrundsatzes sowie bereichsspezifische Rechtssätze zur Zweckbestimmung der Informationsverarbeitung und zur Zusammenarbeit mit Eurojust und OLAF.

Eine neue Stufe der Zusammenarbeit bei der Strafverfolgung wird durch die geplante Errichtung einer Europäischen Staatsanwaltschaft erfolgen.<sup>27</sup> Der Europäische Staatsanwalt soll als unabhängiges Organ der Union für die Untersuchung, Verfolgung und Anklage von Straftaten zum Nachteil der finanziellen Interessen der Union und damit untrennbar verbundenen Tätigkeiten zuständig sein. Geplant sind eine Zentralstelle sowie die Einsetzung der delegierten europäischen Staatsanwälte, die in den Mitgliedstaaten angesiedelt sind. Für die Verarbeitung personenbezogener Daten enthält Kapitel VI des Verordnungsentwurfs umfangreiche bereichsspezifische Bestimmungen, die auch von einer Zweckbindung der Daten ausgehen.

## V. Ausblick

Die nationalen Maßnahmen zur Anpassung des Datenschutzrechts an die DS-GVO und zur Umsetzung der RL (EU) 2016/680 haben in Deutschland mit einem entsprechenden Gesetzentwurf begonnen.<sup>28</sup> Es sollen jedoch noch weitere bereichsspezifische Regelungen folgen. Angesichts der Vielzahl der geltenden Rechtsakte und dem unterschiedlichen Umfang nationaler Regelungskompetenzen für einen Datenaustausch zwischen den für die Strafverfolgung, die Gefahrenabwehr sowie die nationale Sicherheit zuständigen Behörden können die Kriterien für eine Zweckänderung ein wirksames Instrument für den Gleichlauf der Datenverarbeitung bilden. Anknüpfungspunkte sind der Grundsatz der Zweckbindung und der Maßstab der hypothetischen Datenerhebung. Insbesondere im Verhältnis von Strafverfolgung und nationaler Sicherheit können – angesichts dessen, dass die nationalen Sicherheitsbehörden aus dem Anwendungsbereich des europäischen Datenschutzrahmens fallen – diese Ansätze eine Möglichkeit bieten, die Datenerhebungs- und Datenverwendungsbestimmungen anzugleichen. Überdies können einheitliche Anforderungen an eine Zweckänderung zu einer Begrenzung der Datenverknüpfungen der sog. Big-Data-Anwendungen führen. Bei diesen Prozessen sind ebenfalls personenbezogene Daten betroffen, deren Verwendung nicht nur durch das technisch Machbare begrenzt werden können. Insgesamt bleibt zu wünschen, dass weitere Schritte zur Harmonisierung des Datenschutzes erfolgen, die auch einheitliche und klare Regelungen für den notwendigen Datenaustausch zwischen den Nachrichten- und Sicherheitsdiensten festlegen.



**Petra Beckerhoff**  
Rechtsanwältin in Münster (Westfalen)

1 ABl. (EU) L 119, 1 vom 4.5.2016.  
2 ABl. (EU) L 119, 89 vom 4.5.2016.  
3 ABl. (EU) L 281, 31 vom 23.11.1995.  
4 Erwägungsgründe Nr. 5 und 9 der DS-GVO.  
5 Erwägungsgrund Nr. 16 der DS-GVO.  
6 BT-Drucks. 18/11325, S. 2, 74.  
7 ABl. (EU) L 8, 1 vom 12.1.2001.  
8 Erwägungsgrund Nr. 19 der DS-GVO.  
9 Zu den einzelnen Öffnungsklauseln Kühling/Martini et al., *Die Datenschutz-Grundverordnung und das nationale Recht*, 2016.  
10 Vgl. Art. 6 II, III; 9 IIa), IV; 37 IV, 88 DS-GVO.  
11 BVerfG, Urt. vom 20.4.2016, 1 BvR 966/09, 1 BvR 1140/09, Rn. 287, 292 (abrufbar unter: [http://www.bverfg.de/e/rs20160420\\_1bvr096609.html](http://www.bverfg.de/e/rs20160420_1bvr096609.html) [zuletzt abgerufen: 3.7.2017]).

12 Es kommen der Zeitpunkt der Datenerhebung, der der Datenübermittlung oder der Moment der Datenverwendung in Betracht.

13 Vgl. Art. 37, 35, 42, 33, 30 DS-GVO.

14 Vgl. Art. 25 DS-GVO.

15 ABl. (EU) L 350, 60 vom 30.12.2008.

16 Erwägungsgrund Nr. 25 der RL (EU) 2016/680.

17 Vgl. die Regelungen der Art. 13 III, 15 RL (EU) 2016/680 einerseits und Art. 6 RL (EU) 2016/680 andererseits.

18 Europäische Kommission, COM (2017) 8 final; dazu Pressemitteilung vom 10.1.2017, IP/17/5.

19 Europäische Kommission, COM (2017) 10 final; dazu Pressemitteilung vom 10.1.2017 IP/2017/5.

20 Siehe die Mitteilung: Europäische Kommission > Vertretung in Deutschland > News > "Europäische Datenwirtschaft: EU-Kommission stellt Konzept für Daten-Binnenmarkt vor", abrufbar unter: [https://ec.europa.eu/germany/news/europ%C3%A4ische-datenwirtschaft-eu-kommission-stellt-konzept-f%C3%BCr-daten-binnenmarkt-vor\\_de](https://ec.europa.eu/germany/news/europ%C3%A4ische-datenwirtschaft-eu-kommission-stellt-konzept-f%C3%BCr-daten-binnenmarkt-vor_de) (zuletzt abgerufen: 3.7.17).

21 Siehe Europäische Kommission, COM(2017) 9 final.

22 Ratsdok. 12307/16, S. 17, 18.

23 Ratsdok. 12307/16, S. 14.

24 Ratsdok. 12307/16, S. 15, 18.

25 ABl. (EU) L 135, 53 vom 24.05.2016.

26 Ratsdok. 12307/16, S. 16, 17.

27 Zum Stand siehe News-Sektion in dieser Ausgabe.

28 BT-Drucks. 18/11325.

# 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](mailto:u.sieber@mpicc.de)

Internet: <http://www.mpicc.de>

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



MAX-PLANCK-GESELLSCHAFT

**Editor in Chief:** Prof. Dr. Dr. h.c. mult. Ulrich Sieber  
**Managing Editor:** Thomas Wahl, Max Planck Institute for Foreign and International Criminal Law, Freiburg  
**Editors:** Dr. András Csúri, Utrecht University; Cornelia Riehle, ERA, Trier  
**Editorial Board:** Peter Csonka, Head of Unit, DG Justice and Consumers, European Commission Belgium; Francesco De Angelis, Directeur Général Honoraire, Commission Européenne Belgique; Prof. Dr. Katalin Ligeti, Université du Luxembourg; Lorenzo Salazar, Ministero della Giustizia, Italia; Prof. Rosaria Sicurella, Università degli Studi di Catania, Italia  
**Language Consultant:** Indira Tie, Certified Translator, Max Planck Institute for Foreign and International Criminal Law, Freiburg  
**Typeset:** Ines Hofmann, Max Planck Institute for Foreign and International Criminal Law, Freiburg  
**Produced in Cooperation with:** Vereinigung für Europäisches Strafrecht e.V. (represented by Prof. Dr. Dr. h.c. mult. Ulrich Sieber)  
**Layout:** JUSTMEDIA DESIGN, Cologne  
**Printed by:** Stückle Druck und Verlag, Ettenheim/Germany

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



© Max Planck Institute for Foreign and International Criminal Law 2017. All rights reserved: no part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical photocopying, recording, or otherwise without the prior written permission of the publishers. The views expressed in the material contained in eucrim are not necessarily those of the editors, the editorial board, the publisher, the Commission or other contributors. Sole responsibility lies with the author of the contribution. The publisher and the Commission are not responsible for any use that may be made of the information contained therein.

### 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](mailto:eucrim-subscribe@mpicc.de).

For cancellations of the subscription, please write an e-mail to:  
[eucrim-unsubscribe@mpicc.de](mailto:eucrim-unsubscribe@mpicc.de).

### For further information, please contact:

Thomas Wahl  
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: [t.wahl@mpicc.de](mailto:t.wahl@mpicc.de)



