Europol's data protection framework as an asset in the fight against cybercrime*

Daniel Drewer, Jan Ellermann

Daniel Drewer
Head of the Data Protection Office
Europol, Eisenhowerlaan 73, 2517 KK The Hague, The Netherlands
E-mail: Daniel.Drewer@europol.europa.eu

Dr. jur. Jan Ellermann
Senior Expert in the Data Protection Office
Europol
E-mail: Jan.Ellermann@europol.europa.eu

Abstract

The European Union will launch its own European Cyber**c**rime Centre (EC3) by 2013. A related feasibility study carried out for the European Commission reveals that next to operational considerations strong data protection safeguards constitute one of the main factors for having the centre hosted at the European Police Office (Europol).[1] This article highlights how far Europol's robust data protection regime contributes to effectively fighting cybercrime while duly observing fundamental rights including the right for protection of personal data.

Keywords

European Cybercrime Centre (EC3), Europol, data protection regime, right for protection of personal data

1 Introduction

The value of the cybercriminal economy as a whole is not known. Recent estimates of global corporate losses alone stand at approximately € 750 billion, other figures even amount to 1 trillion per year.[2] The true extent of cybercrime is difficult to assess for a number of reasons. In particular, there are concerns that the quantity of unreported cases is significant. Businesses fear that negative publicity could damage their reputation.[3]
What can be established is that Internet technology has meanwhile emerged as a key facilitator also for the vast majority of offline organised crime. The extensive use of the Internet underpins illicit drug synthesis, extraction and distribution, the recruitment and marketing of victims of trafficking in human beings (THB), the facilitation of illegal immigration, the

* This article is based on a contribution given at the conference "Making Europe Safer: Europol at the Heart of European Security", organised by ERA in cooperation with Europol on 18-19 June 2012 in The Hague. The opinions expressed by the authors in this article are personal ones and do not necessarily represent those of the organisation they work for.
[1] http://www.rand.org/pubs/technical_reports/TR1218.html, in particular, p. 2, 86, 88, 90, 149 and 154, accessed on 26/04/12.
[2] *Europol* [12], p. 14, *Europol* [9], p. 5. For a critical view on the threat posed by cybercrime see *Monroy/Bush*, [20], p. 3 ff. For a critical view on the estimation of cost resulting from cybercrime see *Anderson et al*. [26], p. 23 ff.
[3] *Gercke* [14], p. 35 ff.

supply of counterfeit commodities, trafficking in endangered species, and many other criminal activities.[4]
The European Commission has recognised the emerging threat posed by cybercrime. Its Internal Security Strategy defines an increased level of security for citizens and businesses in cyberspace as one of the core objectives.[5]
The strategy foresees concrete actions to better prevent and fight cybercrime and cyber attacks. This includes capacity building in law enforcement and the judiciary, inter alia by establishing a **E**uropean **C**yber**c**rime **C**entre (EC3) by 2013.
The EC3 is expected to

- strengthen and integrate operational and analytical capacities for cybercrime investigations in the Union, including a reinforcement of the cooperation with Member States, international partners and the private sector;
- evaluate and monitor existing preventive and investigative measures in the area of cybercrime;
- support the development of training and awareness-raising initiatives of law enforcement, judicial authorities and the private sector;
- facilitate the reporting of cybercrimes and simplify subsequent processing of the information by Member States' law enforcement authorities via interlinking national cybercrime alert platforms to a central European cybercrime alert platform;
- improve cooperation with the European Network and Information Security Agency (ENISA) as well as national/governmental Computer Emergency Response Teams (CERTs) on law enforcement relevant aspects of cyber security.

The main axes of functionality are thus to be seen in analysis/intelligence capabilities, investigative support, training and cooperation with law enforcement and non law-enforcement partners.[6]

In March 2012, the Commissioner responsible for Home Affairs, Cecilia Malmström, proposed that the EC3 should be hosted by Europol.[7] A decisive argument was that the organisation is already at the present stage tasked to counter cybercrime by various methods and means in a data protection compliant manner and has considerable experience in handling sensitive information.[8] The Council endorsed the goals of the Communication in June 2012.[9]

2 High standard of data protection

Full compliance with data protection principles is an asset in effectively preventing and combating cybercrime.[10] It forms the basis for the trust of Member States which provide related intelligence to Europol. Also citizens expect the EC3 to tackle the issue of cybercrime

[4] *Europol* [10], p. 6.
[5] *European Commission* [6], p. 9.
[6] *European Commission* [6], p. 9 f.
[7] COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT: Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre, COM(2012) 140 final, 28/03/2012, p. 1 ff.; http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/317&format=HTML&aged=0&language=DE&guiLanguage=en, accessed on 26/04/12.
[8] See, in particular, p. 2, 86, 88, 90, 149 and 154 of the related feasibility study, http://www.rand.org/pubs/technical_reports/TR1218.html, accessed on 26/04/12.
[9] Council conclusions on the establishment of a European Cybercrime Centre 3172nd Justice and Home Affairs Council meeting Luxembourg, 7 and 8 June 2012.
[10] Also see Opinion of the European Data Protection Supervisor on the Communication from the European Commission to the Council and the European Parliament on the establishment of the European Cybercrime Centre [8], p. 2.

in a way which fully respects fundamental rights including the right of protection of personal data.

Europol has a comprehensive, robust and tested regime in place which is widely recognised as safeguarding and ensuring the highest standards of data protection in the law enforcement world. It aims at ensuring the protection of privacy of the persons whose data are processed in Europol's systems. At the same time it serves the needs of operational units in preventing and combating organised crime, terrorism and other forms of serious crime affecting two or more Member States.

Europol's data protection legal framework is based on the principles contained in Convention 108 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data as well as on the Council of Europe Committee of Ministers Recommendation No R (87) 15 regulating the use of personal data in the police sector.[11]

Europol's data protection regime reflects the core principles of Directive 95/46/EC which forms the most important data protection instrument in the European Union. However, it is tailor-made to Europol's specific mandate and tasks.[12]

The Europol Council Decision (ECD)[13] contains very detailed provisions on data protection, which are further developed by a set of implementing rules such as Council Acts related to the Rules applicable to Analysis Work Files[14], Rules governing Europol's relations with partners[15], Rules on Confidentiality[16] and conditions related to the processing of data for the purpose of determining relevance to Europol's tasks.[17] Additionally, Europol observes the principles of Regulation 45/2001[18] when it comes to the processing of staff data.[19]

As of its launch in 2013, the boundaries of EC3 operations will be determined by the ECD and its implementing rules.[20] Potential operational business needs beyond the current mandate would have to be reflected in the process of the ongoing evaluation of the ECD.[21] A future Europol Regulation is to be adopted by the European Parliament and the Council as required by Article 88 of the Treaty on the Functioning of the European Union.

3 Independent data protection supervision

The application of data protection rules by Europol is supervised on various levels and throughout the entire information cycle.

---

[11] See Art. 27 ECD.

[12] The same is valid for the data protection regime of Eurojust, the EU's judicial cooperation unit, see *Alonso Blas*, Ensuring effective data protection in the field of police and judicial activities, ERA Forum (2010) 11 p 233 ff.

[13] Council Decision of 6 April 2009 establishing the European Police Office (EUROPOL) (2009/371/JHA), OJ L 121/37, 15/05/2009 hereafter referred to as 'ECD'.

[14] Council Decision of 30 November 2009 adopting the implementing rules for Europol analysis work files (2009/936/JHA), OJ L 325/14, 11/12/2009, hereafter referred to as 'AWF Rules'.

[15] Council Decision of 30 November 2009 adopting the implementing rules governing Europol's relations with partners, including the exchange of personal data and classified information (2009/934/JHA) OJ L 325/6, 11/12/2009.

[16] Council Decision of 30 November 2009 adopting the rules on the confidentiality of Europol information, (2009/968/JHA), OJ L 332/17, 17/12/2009.

[17] Decision of the Management Board of Europol of 4 June 2009 on the conditions related to the processing of data on the basis of Article 10(4) of the Europol Decision, OJ L 348/1, 29/12/2009.

[18] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of data.

[19] Art. 39(6) ECD, also see *Europol* (ed.), Data Protection at Europol, p. 10 f.

[20] Also see Opinion of the European Data Protection Supervisor on the Communication from the European Commission to the Council and the European Parliament on the establishment of the European Cybercrime Centre, p. 3 f., 29/06/2012.

[21] Id., p. 2, 6.

Contributions from national level to Europol are scrutinised by national competent data protection authorities on the basis of applicable national law.
Once the information is processed at Europol, the Data Protection Officer (DPO) has the task to ensure, in an independent manner, lawfulness and compliance with the ECD and its implementing rules.[22] The DPO is a member of staff and an integral part of the organisation. Being an internal function is essential for the role of the DPO as it facilitates the building of trust amongst Europol staff, ensures compliance from the inside and enables the provision of advice or intervention at an early stage when potential risks for data subjects tend to be lower. Established procedures ensure the use of Privacy Enhancing Technologies (PETs) following a privacy by design approach for any new technical infrastructures.[23]
External supervision is carried out by the Joint Supervisory Body (JSB).[24] This independent entity comprises representatives from national data protection authorities of all 27 Member States. Due to its composition this authority provides invaluable expertise regarding data protection in the police sector. The JSB holds frequent and regular inspections, covering all processing operations of Europol and delivers extensive and detailed reports of such inspections, including findings and recommendations.[25]
Next to these data protection specific supervisory mechanisms, Europol is accountable to Member States via the Council through an existing, politically and legally agreed framework. Budgetary supervision is carried out by the budgetary authority consisting of both the Council and the European Parliament, in the same way as for other EU agencies. The European Court of Auditors also plays an important role in this regard. In particular, the European Parliament, namely the Committee for Civil Liberties, Justice and Home Affairs (LIBE), uses its influence also with a view to safeguarding data protection. The role of the European Parliament will further enhance once the new Europol Regulation has entered into force.[26] The European Court of Justice will gain full jurisdiction over Europol as of December 2014 at the latest.[27]
Against this background Europol is sometimes referred to as "the most controlled police agency in Europe".[28]

4 Secure information exchange capabilities

An important feature in the fight against cybercrime is Europol's Secure Information Exchange Network Application (SIENA) which is geared towards fulfilling data protection and data security requirements of competent authorities of Member States and beyond.
This state-of-the-art IT infrastructure, hosted in Europol's highly secure New Headquarters, connects Europol with its national units in all 27 EU Member States. The network operating 24/7 is currently further extended to various designated competent authorities in Member States as well as to selected third party cooperation partners.[29] Council-approved international agreements with major non-EU partners such as Interpol, the USA and Australia form the basis for the exchange of personal data according to European data protection and security

[22] Art. 28 ECD
[23] *Europol* [11], p. 27 ff.; for the importance of Privacy Enhancing Technologies (PETs) fostering privacy by design also see Opinion of the European Data Protection Supervisor on the Communication from the European Commission to the Council and the European Parliament on the establishment of the European Cybercrime Centre, p. 7, 29/06/2012.
[24] Art. 34 ECD
[25] *Europol* [11], p. 32 f.; www.europoljsb.consilium.europa.eu, accessed on 08/02/2012.
[26] For details on how the entry into force of the Lisbon Treaty has further enhanced formal monitoring of Europol see *Fletcher* [13], p. 38 ff.
[27] Article 10(1) and (3) Protocol on Transitional Provisions Lisbon Treaty.
[28] *Fijnaut*, quoted as per *Groenleer* [15], p. 282.
[29] Also see *Europol* [11], p. 19 ff.

standards.[30] The organisation is therefore in a good position to reach out beyond the European Union given the fact that cybercrime does not stop at national borders.[31]
Europol hence has the possibility to use its existing network to manage and disseminate information if so authorised by the owner of the information. Member States and third parties retain full control over their data by allocating handling codes which are mandatory in SIENA.

5 Outreach to the private sector

Building trust and confidence between private sector and law enforcement authorities is of utmost importance in the fight against cybercrime. According to the European Commission EC3 should build trusted networks and information exchange platforms with industries and other actors such as research communities and civil society organisations.[32]
It is in the mutual interest of law enforcement authorities and the private sector to arrive at a better measurement of the cybercrime landscape in real time as well as to strive for more effective dismantling of cybercrime networks via an enhanced detection of new *modi operandi* and the swift arrest of cybercriminals.[33] One focus of EC3 will be to protect social network profiles from e-crime infiltration which will help the fight against online identity theft.[34]
Europol has an established model for data protection compliant outreach to the private sector defined in Article 25 ECD.
The routing of personal data in such cases takes place via the national units or contact points as specified in the applicable cooperation agreements. This bears the advantage of application of the respective underlying national law including any data protection safeguards such as the requirement of obtaining a judicial warrant for retrieval of certain sensitive personal information.[35]
Even for companies in countries outside the European Union with which Europol has no operational cooperation agreement concluded, receipt of personal data may still take place on the basis of a memorandum of understanding provided the private party is mentioned on a list adopted by Europol's Management Board (MB).[36]
It is realised that there is still a gap between the above outlined Commission vision of establishing information exchange platforms with industries and the current legal landscape requiring the routing of information via national authorities at least when it comes to personal data.[37] However, direct strategic cooperation is already possible at the present stage and should not be underestimated.

---

[30] Art. 23 ECD.
[31] Also see Opinion of the European Data Protection Supervisor on the Communication from the European Commission to the Council and the European Parliament on the establishment of the European Cybercrime Centre [8], p. 9 f.
[32] COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT: Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre, COM (2012) 140 final, 28/03/2012, p. 7.
[33] COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT: Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre, COM(2012) 140 final, 28/03/2012, p. 7.
[34] http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/317&format=HTML&aged=0&language=DE&guiLanguage=en, accessed on 26/04/12
[35] Art. 25(3)(a) and (b) ECD.
[36] Art. 25(3)(c) ECD, *Europol* (ed.), Data Protection at Europol, p. 24 f.
[37] Also see Opinion of the European Data Protection Supervisor on the Communication from the European Commission to the Council and the European Parliament on the establishment of the European Cybercrime Centre [8], p. 7 ff., 29/06/2012.

6 Europol Information System

The previous chapters have described the general data protection legal framework and how information finds its way to and from Europol. The following sections will focus on means and methods of data processing within the organisation.
One of Europol's core databases to fight cybercrime and other forms of serious and organised crime as well as terrorism is the Europol Information System (EIS). It enables Member States to share and retrieve information about persons, events and devices connected with a criminal case (e.g. suspects, weapons, phone numbers, number plates, passports).[38]
The range of data that may be processed in the EIS is limited in a number of ways: only data that is necessary for the performance of Europol's task may be used.[39] Data in the EIS must relate to suspects, convicted criminals or persons on whom there are factual indications or reasonable grounds to believe that they will commit crimes falling within Europol's mandate. An exhaustive list of the type of data that may be stored and processed is contained in Art. 12(2) ECD: name, date and place of birth, nationality, sex, place of residence, profession, identification documents, fingerprints and DNA profiles.
A strict data retention regime applies not only for data processed in the EIS but also beyond. In general, information is only held for as long as is necessary and must be reviewed no later than three years after insertion.[40]
Review in any case takes place if circumstances arise that necessitate deletion of data. For example, data in the EIS must be deleted when persons have been acquitted or proceedings against them have been definitively dropped.[41]

7 Analysis Work Files

Europol's Analysis Work Files (AWFs) form the organisation's most important tool in preventing and combating cybercrime while respecting applicable data protection legislation.[42]

7.1 General data processing framework

AWFs allow for relevant data to be collected and analysed in a comprehensive manner. The crime analysis performed relies on the application of analytical techniques and cutting edge technology. This includes Social Network Analysis[43], geographic profiling, open sources

[38] *Europol* [11], p. 14 f.
[39] Art. 12(1) ECD.
[40] Art. 20 ECD.
[41] Art. 12(5) ECD.
[42] See Art. 14 ff. ECD.
[43] Social Network Analysis (SNA) is a scientific approach that was adopted as an innovative way to conduct crime analysis. Now computer-assisted SNA techniques (i.e., algorithms) can be employed by analysts to measure and visualize any type of network data (data which are relational and related to certain attributes). Operational analysts are able to deal with complex and large volumes of data to quickly identify structural patterns that otherwise would remain unnoticed. SNA should not be confused with social networking and the types of network data available on websites such as Facebook and Google+. SNA may also be performed on such data sets but analysis of these publicly available sources is not a constituent element of this analytical technique. For a critical view on SNA in the context of social networking sites see *Schulzki-Haddouti* [23], p. 32 ff.; *Kant/Busch* [18], p. 40 ff.

analysis, image analysis including EXIF retrieval[44], financial trail, telephone call and email analysis to name but a few.[45]
Accordingly, data processed within AWFs may not only relate to suspects and (potential) criminals, but also to contacts, associates, witnesses, victims and informants. The list of data categories[46] that may be stored and processed is broader than in the EIS. However, additional data protection rules apply and ensure the responsible handling of data.
Access to AWFs and the content of individual files are strictly limited by documentation referred to by the ECD and its implementing rules as 'opening orders'.[47] These opening orders specify the purpose of the file. Information that does not fit the purpose description may not be inserted. Data already contained in an AWF may not be used for any other purpose. Art. 4 AWF Rules further stipulates that personal data may only be processed as far as it is 'not excessive in relation to the purpose of the analysis work file'.[48]
In addition, sensitive personal data may only be processed where strictly necessary for the purpose of the file. Sensitive personal data are data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership as well as health and sex life. Selecting a particular group of persons solely on the basis of such data is prohibited.[49]
The opening orders also specify the conditions under which data may be communicated to recipients and the appropriate procedure for doing so, as well as time limits for retaining data. With regard to data retention the same principles apply as for the EIS.[50]
Participation in analysis activities is limited to an expressly nominated analysis group: in general, only authorised and designated Europol staff and Liaison Officers or experts from the relevant Member States can join a particular file. Third parties can be associated to the activities of the analysis group and receive analysis results concerning them.[51] At the same time, the members of the analysis group can set limits to the use of their data by assigning predefined handling codes. For instance they can determine or exclude potential recipients.[52]

7.2 New AWF concept

A former AWF concept was based on 23 AWFs which meant 23 different, largely disconnected databases. This large number of data silos entailed clear disadvantages from an operational perspective.[53] Emphasis had traditionally been on vertical thinking which was effective but incomplete. It encouraged a selective type of crime analysis which needed to be complemented by a more generative lateral thinking approach.[54]

---

[44] Exchangeable image file format (EXIF) is a standard that specifies the formats for images, sound and tags used by digital cameras etc. EXIF data of a camera will reveal, for example, manufacturer, resolution, data and time, pixels and sometimes geo location.
[45] See *International Association of Law Enforcement Intelligence Analysts*, Inc. (ed.), Law Enforcement Analytic Standards, Richmond 2004.
[46] Art. 6 AWF Rules.
[47] Art. 16 ECD, Art. 5 ff. AWF Rules.
[48] *Europol* [11], p. 16 f.
[49] Art. 14(1) ECD.
[50] Art. 20(1) ECD.
[51] *Europol* (ed.), Data Protection at Europol, p. 17.
[52] Art. 14(6) ECD.
[53] For a collation of 'organisational pathologies' including the establishment of information silos see *Sheptycki* [24], p. 307 ff. and 'Review of influence of strategic intelligence on organised crime policy and practice', London: Home Office Research and Statistics Directorate, quoted as per *Ratcliffe* [21], p. 253; also see *Ratcliffe* [22], p. 1.
[54] *de Bono* [2], p. 7 ff.

The new AWF concept is geared to an innovative role of crime analysis taking enhanced account of the fact that cybercrime as well as other forms of serious and organised crime are changing, displaying increasing diversification.[55]
The new AWF concept foresees the existence of only two AWFs instead of 23. One focus is on 'serious and organised crime' (AWF SOC) including various aspects of cybercrime. The other is 'counterterrorism' (AWF CT), which may certainly also entail cybercrime related aspects.
The new concept entails that analysts will in principle have access to all information processed in the AWF they are allocated to. The same applies to specialists who have read-only access. From a data protection related viewpoint the utilization of access is, however, not unconditional but must always bear a clear link to the purpose of the AWF in question. Europol has appropriate auditing capabilities at its disposal in order to ensure full traceability of user actions within its databases.

7.2.1 Managing AWFs via Focal Points and Target Groups

One of the core assumptions under the new AWF concept is that there can be multiple analysis groups within one AWF.
In practical terms the different analysis groups within an AWF are each responsible for a specific Focal Point[56] and/or Target Group[57]. Even though Europol's legal framework does not explicitly foresee 'Focal Points' or 'Target Groups', the use of terminology that is common in the world of law enforcement facilitates the understanding by operational colleagues at Europol and in the field. 'Focal Points' and 'Target Groups' in that sense form a legitimate implementation of the term 'analysis project' as mentioned in the ECD.
The opening orders of both AWFs consequently determine the nature of the data and the individuals on whom data may be stored on the level of Focal Points and Target Groups in dedicated annexes. A number of Focal Points will for instance require the processing of personal data related to victims or witnesses while others will not.
In particular, the necessity of processing operations upon sensitive personal data is specified drawing the link to Focal Points and/or Target Groups in order to ensure that such analysis is only conducted where strictly necessary and where already existing information is supplemented.[58]
Notably, the definition of Focal Points and Target Groups is in legal terms a specification of the purpose of the file in the sense of Article 16(1)(b) ECD. According to Article 16(2) ECD the Management Board and the JSB are immediately informed by the Director of any subsequent change in the particulars referred to in paragraph 1 and receive the dossier. In consequence, any opening or closure of a Focal Point or Target Group as well as any modification in scope has to be reported to Europol's supervisory entities.

7.2.2 Enforcing purpose limitation within the AWF

Purpose limitation still plays a decisive role within the AWF and it remains enforceable despite the fact that each analyst will have the ability to see further than before.
The purpose limitation principle states that data collected may only be processed for specific, explicit and legitimate purposes and not processed further in a way incompatible with those

[55] For a comprehensive overview on the diversity of criminal offences qualifying as cybercrime refer to *Gercke*, [14], p. 41-120.
[56] A Focal Point is an area within an AWF which focuses on a certain phenomenon from a commodity based, thematic or regional angle. It allows Europol to provide analysis, prioritise resources, ensure purpose limitation and maintain focus on expertise.
[57] A Target Group is an operational project with a dedicated Europol team to support an international criminal investigation or criminal intelligence operation against a specific target.
[58] See Article 14(1) subpar. 2 ECD.

purposes.[59] The legal definition of 'data processing' is broad and includes the element of 'consultation' of data.[60]
A distinction is drawn between different forms of processing operations depending on their potential impact on data subjects.
'Consultation' of data beyond the allocated Focal Point/Target Group is necessary in order to improve the detection of increasingly poly-criminal and multi-commodity oriented serious and organised crime.
The criterion of serving a 'specific, explicit and legitimate purpose' is fulfilled in cases of 'motivated consultations'. A triggering event for such a 'motivated consultation' of data beyond the allocated Focal Point/Target Group could be a cross-match with data already processed in another Focal Point/Target Group. Another trigger could be an investigative lead, i.e. factual indications or reasonable grounds for believing that a certain manual query could result in additional criminal intelligence fostering the purpose of the same Focal Point/Target Group. This purpose is also proportionate as entailed risks for data subjects are low as long as pure consultation is concerned.
Further 'usage' of data requires a more specific purpose description as defined per Focal Point and Target Group.
As a consequence, whenever analysis activity goes beyond pure consultation of data, a clear link to the specific purpose of a Focal Point or Target Group must be drawn and processing operations limited to the respectively defined data categories, in particular when it comes to drafting analysis reports.

7.2.3 Opportunities to further enhance data protection

The new AWF concept takes due account of the importance of intelligence analysis that can draw on all relevant sources of information while maintaining a high data protection and security standard. It even offers a number of opportunities to further enhance data protection, namely in the areas of data quality, data retention and data subject access requests.
The former existence of 23 different AWFs entailed different ways of handling personal data. The new AWF concept facilitates the enforcement of common standards and procedures, but also helps to reduce the duplication of data. Data which was previously relevant and inserted in several work files is now only stored in maximum two AWFs. This makes it easier to check accuracy and update where necessary. Also the data retention regime can be applied in a more efficient manner. The new AWF in that sense indirectly fosters the aim of data minimisation which also makes sense from an operational perspective. Administrative demands are decreasing, in particular as far as right of information requests in accordance with Article 30 ECD are concerned: fewer queries are necessary in order to determine whether personal data relating to the requesting individual are processed by Europol.
Europol does not consider compliance with data protection principles only as a burden. Data protection and effective law enforcement in fact go hand in hand. Data in the files are thoroughly checked since only high quality information generates high quality analysis. Law enforcement authorities have to be able to rely on the information provided by Europol to be correct and valid. Regular compliance monitoring performed by the DPO and inspections

[59] See Art. 6(1)(b) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/40, 23/11/95; also see *Brouwer* [4], p. 276.
[60] Processing of personal data includes the collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction of personal data, see Art. 2(b) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/40, 23/11/95.

carried out by the JSB are indispensable for the proper functioning of AWFs from a human rights but also from an operational perspective.[61]

7.3 The specific cybercrime context

A number of analysis projects at Europol are involved in preventing and combating cybercrime. CYBORG deals with Internet and ICT related crime as referred to in Articles 2-8 Cybercrime Convention,[62] TERMINAL conducts crime analysis on payment card fraud, and TWINS deals with sexual exploitation of children via the Internet.

While these three projects obviously process data on particular forms of crime in which computers or networks are a tool, target or place of criminal activity,[63] others also involve such offences even though the actual purpose of the file does not immediately suggest links to cybercrime. For instance, COPY prevents and combats the manufacturing and/or trading of counterfeited products and product piracy while SUSTRANS conducts crime analysis on suspicious financial transactions. Another example is CHECK THE WEB which has its focus on Islamist extremist terrorism propaganda on the Internet.

The new AWF concept acknowledges the reality of cybercrime as a multi-commodity and poly-criminal enterprise in that analysis projects CYBORG, TERMINAL, TWINS, COPY and SUSTRANS have all become Focal Points in the newly created AWF SOC tackling serious and organized crime.

Europol's analysts and specialists are hence in a better position to draw links for instance between card skimmers and related suspicious transactions to name just one example. Further usage of this information will still be bound to the specific purpose of the respective Focal Points as defined in annexes to the opening order.

The analysis project CHECK THE WEB dealing with Islamist extremist terrorism propaganda on the Internet has become a Focal Point in AWF CT, i.e. in the counterterrorism related file. From a purpose limitation viewpoint it appears appropriate to treat terrorism related cases in a separate database.

Still, links to traditional forms of cybercrime can be identified by means of a so called Index Function. The Director, the Deputy Directors, duly empowered Europol staff, liaison officers and duly empowered members of national units have the right to access this search engine. It is configured in a way that it is clear to the person using it whether an analysis work file contains data which are of interest. However, it is not possible to establish connections or further conclusions regarding the content of the file, i.e. the Index Function provides hit/no-hit access only.[64]

An analyst allocated to Focal Point CHECK THE WEB can hence not directly access information processed in any of the AWF SOC Focal Points. Upon a hit-notification by the Index Function he would first have to seek the consent of the respective analysis group in order to determine what is behind that hit. Further usage of data would then again depend on whether the information is necessary to pursue the specific purpose of Focal Point CHECK THE WEB.

The new AWF concept enables Europol's analysts and specialists to see further in order to overcome commodity or criminal group driven silo thinking and compartmentalisation. As a consequence the detection of trends and patterns across different commodities and criminal groups is significantly facilitated by enabling the combination of contextual information beyond entity level of already structured intelligence. Links between investigations and common *modi operandi* can more easily be identified. Also cross-matches can immediately be checked for their relevance, which should boost the fight against cybercrime while maintaining a high standard of data protection and data security.

---

[61] *Europol* [11], p. 17.
[62] Council of Europe Convention on Cybercrime, ETS 185, Budapest, 27/11/2001.
[63] For an overview of cybercrime definitions refer to *Gercke* [14], p. 25 ff.
[64] See Art. 15 ECD.

8 Conclusion

The Internet has not only revolutionised the way we live, establishing a worldwide cyber society which appears to be borderless.[65] It has also eliminated distance, bringing the general public and organised crime activity into close proximity, eroding the distinction between internal and external threats.[66]

The "information superhighway" predicted thirty years ago is now a reality, with the world increasingly dependent on high-tech communications and banking systems. This has provided new opportunities for criminals, and created new illicit markets. Personal data is the new commodity driving much of today's cybercrime. In the digital age we are increasingly identifiable by numbers (bank accounts, passwords, social security, etc.). These numbers have become the stock in trade for fraudsters across the world.[67]

Data protection and the fight against cybercrime do certainly not constitute a contradiction. On the contrary, due protection of information relating to identified or identifiable natural persons is a prerequisite to prevent identity theft and other forms of cybercrime.

The previous chapters have illustrated the solid data protection regime at Europol. Prominent features in this regard are independent data protection supervision, Europol's secure information exchange capabilities, data protection compliant outreach to the private sector and – most importantly - clearly defined purpose specifications for processing operations upon personal data in Europol's databases.

The aims of preventing and combating cybercrime are balanced against the goal of safeguarding the freedom of individuals. In fact, they go hand in hand: at Europol, it is recognised that the data protection rules in place are essential for the success of operations. High data protection standards lead to high quality of data which itself is a precondition for high quality crime analysis.

An EC3 placed at Europol will take due account of the pan-European dimension of cybercrime, tie in with existing structures of reporting and handling of cybercrimes including outreach to the private sector and fully utilize already existing European law enforcement IT systems thereby saving costs. Moreover, an EC3 built upon Europol's robust data protection framework is an appropriate step to ensure full respect for the protection of personal data as a core fundamental right in today's information society.

References

1. Alonso Blas, D.: Ensuring effective data protection in the field of police and judicial activities. In: ERA Forum 11 p. 233 ff. (2010)
2. Bono, E. de: Lateral thinking, London (1970)
3. Brenner, S. / Clarke, L. M.: Combating cybercrime through distributed security. In: International Journal of Intercultural Information Management 1.3:259-274 (2009)

[65] However, the freedoms of speech, association and assembly – including both political speech and organising conducted via the Internet – are not available to citizens in every country. In some countries activists are in danger any time they access or even attempt to access a prohibited website or service or promote political dissent, see *Moloney Figliola* [19], p. 1 and 8 with suggestions for further reading. For the discussion on access to the Internet as a human right see *Gercke* [14], p. 128.

[66] *Brenner/Clarke* [3], pp. 259-274.

[67] *Wainwright*, Press statement on the occasion of the World Economic Forum Davos summit, www.europol.europa.eu/content/press/fighting-cybercrime-%E2%80%93-major-challenge-global-society-1247, accessed on 26/01/2012.

4. Brouwer, E.: Legality and Data Protection Law: The Forgotten Purpose of Purpose Limitation. In: Besslink, L. / Pennings, F. / Prechal, S. (ed.): The Eclipse of Legality in Europe, p. 273 ff., Alphen aan den Rijn (2011)
5. Council of the European Union (ed.), Council conclusions on the establishment of a European Cybercrime Centre 3172nd Justice and Home Affairs Council meeting Luxembourg, 7 and 8 June (2012)
6. European Commission (ed.): The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, COM(2010) 673 final, Brussels (2010)
7. Id., Communication from the Commission to the Council and the European Parliament: Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre, COM(2012) 140 final, 28/03/2012
8. European Data Protection Supervisor: Opinion of the European Data Protection Supervisor on the Communication from the European Commission to the Council and the European Parliament on the establishment of the European Cybercrime Centre, page 2, 29/06/2012
9. Europol (ed.): Threat Assessment (abridged) Internet Facilitated Organised Crime iOCTA, The Hague (2011)
10. Id.: Organised Threat Assessment 2011 (OCTA), Luxembourg (2011)
11. Id.: Data Protection at Europol, Luxembourg (2011)
12. Europol et al. (ed.): The Joint Report by EUROPOL, EUROJUST and FRONTEX on the State of Internal Security in the EU, Council document 9359/10, 07/05/2010
13. Fletcher, M.: EU Criminal Justice beyond Lisbon. In:: Eckes, C. / Konstadinides, T. (ed.): Crime within the Area of Freedom, Security and Justice, Cambridge (2011)
14. Gercke, M.: Understanding Cybercrime: A Guide for Developing Countries, Geneva (2011)
15. Groenleer, M.: The Autonomy of European Union Agencies, Delft (2009)
16. Hammond, B.: Europol sees growing threat from organized cyber crime, Cybersecurity Policy Report, 01/10/2011, New York (2011)
17. International Association of Law Enforcement Intelligence Analysts, Inc. (ed.): Law Enforcement Analytic Standards, Richmond (2004)
18. Kant, M. / Busch, H.: Der Staat surft mit, in: Bürgerrechte & Polizei/CILIP (1/2011), pages 40 ff., Berlin (2011)
19. Moloney F.: Patricia, Promoting Global Internet Freedom: Policy and Technology, Congressional Research Service Report for Congress, Washington, D.C. (2011)
20. Monroy, M. / Busch, H.: Digitaler Untergrund. In: Bürgerrechte & Polizei/CILIP (1/2011), pages 3 ff., Berlin (2011)
21. Ratcliffe, J.: Intelligence-Led Policing, Devon (2008)
22. Id.: Integrated Intelligence and Crime Analysis: Enhanced Information Management for Law Enforcement Leaders, Washington, D.C. (2007)
23. Schulzki-Haddouti: Christiane, Gläserne soziale Netzwerke, in: in: Bürgerrechte & Polizei/CILIP (1/2011), pages 32 ff., Berlin (2011)
24. Sheptycki, J.: Organisational pathologies in police intelligence systems: some contributions to the lexicon of intelligence-led policing', European Journal of Criminology, 1(3), Thousand Oaks (2004)
25. Id.: Review of influence of strategic intelligence on organised crime policy and practice', London: Home Office Research and Statistics Directorate, London (2004)

Internet sources

26. Anderson et al.: Measuring the costs of Cybercrime, http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf, accessed on 11/07/12

27. http://www.rand.org/pubs/technical_reports/TR1218.html, accessed on 26/04/12

28. http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/317&format=HTML&aged=0&language=DE&guiLanguage=en, accessed on 26/04/12

29. www.europol.europa.eu/content/press/fighting-cybercrime-%E2%80%93-major-challenge-global-society-1247, accessed on 26/01/2012
30. www.europoljsb.consilium.europa.eu, accessed on 08/02/2012