DATA PROTECTION AT EUROPOL
HOW TO OBTAIN EU PUBLICATIONS

Free publications:

Priced publications:

Priced subscriptions (e.g. annual series of the

and reports of cases before the Court of Justice

of the European Union):
DATA PROTECTION AT EUROPOL
CONTENTS

Foreword

1 INTRODUCTION

2 IS EUROPOL WATCHING YOU?

3 THE LEGAL FRAMEWORK:
   TAILOR-MADE LEGISLATION
   3.1 Europol’s mandate
   3.2 The data protection regime
   3.3 Core definitions
   3.3.1 Personal data
   3.2.2 Data processing

4 METHODS AND MEANS
   4.1 The Europol Information System
   4.2 Analysis work files
   4.3 Information security
   4.4 SIENA
   4.5 The liaison bureaux

5 REACHING OUT:
   INFORMATION ACQUISITION BEYOND EUROPOL
   5.1 EU institutions
   5.2 Third parties
   5.3 Private parties
   5.4 Publicly available sources

6 EXERCISING THE RULES OR:
   WHO WATCHES THE WATCHDOG?
   6.1 The Data Protection Officer – an independent insider
   6.2 The Joint Supervisory Body
   6.3 National supervisory bodies

7 DATA PROTECTION AND LAW ENFORCEMENT –
   A SUCCESSFUL UNION
FOREWORD

Europol is proud to have one of the most robust data protection frameworks in the world of law enforcement. This is an asset, and at the same time a responsibility, as the legal framework needs to be put into practice and applied in day-to-day operations.

The aim of this booklet is to introduce Europol’s data protection framework in a way which is understandable, not only to data protection experts, but to anyone who is interested in this fascinating subject.

The Data Protection Officer would like to thank Europol staff for the trust shown towards his office in asking for advice, guidance and best practice in relation to the processing of personal data. Because of this cooperation and mutual exchange of views, the vast majority of Europol colleagues regard data protection as an important element in the quality of Europol’s work.

The Data Protection Officer would also like to thank the Europol Joint Supervisory Body for its availability and advice, the Management Board and the Directorate for their valuable cooperation and, last but not least, the Data Protection Office staff for their commitment and dedication.

Daniel Drewer
Data Protection Officer
Introduction

The idea to establish a setting for efficient cooperation between European law enforcement authorities to tackle transnational crime is almost as old as the notion of European unity itself. Born out of concerns about international terrorism in the 1970s, the idea soon grew to cover other areas of cross-border crime within the European Community. In 1999, EUROPOL, the European Police Office, was established mainly as an intelligence broker for coordinated police work in the European Union.

In today’s Europe of open borders, the threats to our security are not diminishing. Organised crime groups, terrorist attacks, pan-European fraud networks and international drug cartels are only a few examples in this context. New dangers are emerging in the form of cybercrime, VAT fraud and other sophisticated crimes which abuse modern technology and the freedoms offered by the EU’s open borders.

To counter these threats and protect the internal security of the European Union and the safety and livelihood of its citizens, Europol and its more than 700 staff have been vested with unprecedented powers, competences and resources.

Europol is often perceived as some kind of ‘European FBI’.
However, Europol agents are not armed with guns, hunting criminals out on the streets. Its officers have no direct power of arrest. When Europol officials enter the field, they do so in a supportive function and under the leadership of national authorities.

Nevertheless, Europol has powerful weapons of its own. The agency is a hub of information, a centre of criminal intelligence and the working place of top analysts and experts from all 27 EU Member States. Like the spider’s web that is part of its logo, Europol interconnects the national law enforcement authorities of the European Union, receiving and distributing information and coordinating joint operations.

This booklet will briefly outline the agency’s capabilities, its tasks and powers, but the main focus will be on the responsibility that comes with the authority to collect substantial amounts of data. In a world where the ‘transparent citizen’ always seems just a step away, data protection plays an increasingly important role. The strong, tailor-made data protection regime at Europol is the main theme of this brochure.
Is Europol watching you?

With the collection and processing of data at the centre of Europol’s work and the corresponding means in place, it is implicit that large amounts of personal data are stored in Europol’s files, analysed by its experts and exchanged between the Europol units, Member States and even third parties. To some, this image might give cause for concern. Nowadays, we cannot even participate in a competition or join a gym without someone gaining access to our personal data and potentially using it for commercial purposes. A multi-national law enforcement agency with the power to collect and analyse large amounts of data might make even more sinister use of our personal information. Are we heading for ‘1984’ reloaded?

It is obvious that in the area of law enforcement, the highest standards of data protection and security are of the utmost importance. The unparalleled means of collecting and analysing data available in our day and age bring with them an obligation to respect each individual’s right to have their personal data duly protected. To live up to this responsibility, it is essential to minimise the danger of abuse and the risk of data leaks, whether intentional or unwitting.

The popular principle that ‘whatever is not forbidden is allowed’ must not apply: any processing of personal data has to be explicitly allowed and the requirements clearly defined.

The legal framework: tailor-made legislation

The extent of Europol’s competence is first of all determined by its mandate. A short introduction to the scope of Europol’s field of action is therefore indispensable before looking in detail at the specific data protection rules.
3.1. Europol’s mandate

Europol’s mandate is defined in the Europol Council Decision (1) (ECD) of 2009. According to Art. 4 (1) ECD, its competence covers terrorism and organised crime as well as other forms of serious crime as listed in the Annex to the ECD, such as trafficking in human beings, Euro counterfeiting or drug related crimes. It is further necessary that the crime concerns two or more Member States and requires them to take a common approach.

The type of action Europol may take is also clearly defined in the ECD. Europol is a European agency, not a self-serving organisation; its main objective therefore is to support and assist the Member States in their efforts to prevent and combat organised crime, terrorism and other forms of serious crime (2).

The core tasks (3) of the agency in providing that support are to

- Obtain, collate and analyse information and intelligence
- Facilitate the exchange of information between Member States
- Assist national investigations
- Help coordinate cooperative operations
- Prepare threat assessments, strategic analyses and general situation reports

Furthermore, since the beginning of 2013 Europol is also the home of the European Cybercrime Centre (EC3). 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 Europol (4).

(2) Art. 3 ECD.
(3) Art. 5 ECD.
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 (5).

As of its launch in 2013 the boundaries of EC3 operations are determined by the ECD and its implementing rules (6). Potential operational business needs beyond the current mandate will have to be reflected in the ongoing legislative process (7). 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.

3.2. The data protection regime

Recognising the importance of clear legislation in the area of data protection, the European Union implemented a strong legal framework tailored to safeguarding the fundamental rights of its citizens. The core data protection instrument within this framework is Directive 95/46/EC (8), which provides essential rules on the processing and movement of personal data. The European Commission proposed a comprehensive reform of the data protection rules on 25 January 2012 and this is currently under discussion (9).

However, just as the general importance of employing sound data protection safeguards is without question, there can be no doubt that effective police work requires top intelligence. The legislative challenge in the area of law enforcement is therefore to create a legal framework which balances the fundamental interests of freedom and security.

In the case of Europol, it was clear from the beginning that a tailor-made set of rules would have to be created which could effectively take into account both the operational needs of Europol and the individual’s right to effective data protection.

(8) 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.

(9) Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final and Proposal for a Directive of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purpose of prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final.
In response to this challenge, comprehensive specialised data protection legislation has been established: Europol has one of the strongest, most robust data protection frameworks in the world of law enforcement.

The centrepiece legislation in place to achieve this balancing act is the Europol Council Decision. With this Decision, the Member States recognised the need to provide special, tailor-made data protection rules for Europol. To stress this point, the legislator emphasised that ‘specific provisions on the protection of personal data’ were essential ‘because of the particular nature, functions and competences of Europol’ (10). Consequently, while the ECD reflects the same values as Directive 95/46/EC, it contains detailed Europol-specific and unique provisions.

The ECD is further complemented by a set of implementing rules, in particular the AWF Rules (11) which govern the handling of Europol’s analysis work files. Furthermore, Europol observes the principles of Regulation 45/2001 (12) with regard to the processing of staff data (13).

Europol’s standard of data protection as defined in Art. 27 ECD refers to the principles of Council of Europe Convention 108 (14) and Recommendation No R (87) 15 (15).

---

**Data protection legislation at Europol**

- The Europol Council Decision (ECD)
- Implementing rules (e.g. AWF Rules, Rules for relations with Third Parties, Rules on Confidentiality)
- Principles of Regulation (EC) 45/2001
- Council of Europe Convention 108 (1981)
- Council of Europe Recommendation R(87)15

---

(10) Recital 12 ECD.
(12) Regulation (EC) 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.
(13) Art. 39 (6) ECD.
(15) Recommendation No. R (87) 15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector, adopted on 17 September 1987.
3.3. Core definitions

One of the implications of this sophisticated regime is that personal data can only be processed if allowed by law. To ensure legal clarity and reliability in this sensitive area, the rules governing the processing of personal data have to be unequivocal and definitive.

The foundation for achieving this aim is clear terminology. Taking this into account, the ECD and its implementing rules make use of definitions that are common in the world of data protection. So, what exactly is personal data? What is encompassed by the term processing?

3.3.1. Personal data

In legal terms, personal data is

*any information relating to an identified or identifiable natural person.*

This definition raises the question: when is a person considered to be identifiable? The law says that an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors
specific to his physical, physiological, mental, economic, cultural or social identity (16).

However, whether or not a person ‘can be identified’ is certainly first and foremost a question of means. How much effort can realistically be invested in identifying a person?

Taking this into account, the rules further state that ‘an individual shall not be regarded as ‘identifiable’ if identification requires an unreasonable amount of time, cost and manpower.’ (17).

### 3.3.2. Data processing

Processing of personal data is much easier to define. Legally speaking, it is any operation … performed on personal data, whether or not by automated means, such as 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 (18).

In short: everything one can do, any kind of action performed on personal data is considered processing.

(17) Recommendation No. R (87) 15, Scope and Definitions, par. 2.
4 Methods and means

In practical terms, data processing at Europol is performed with the aid of specifically designed software, refined techniques and sophisticated structures. The following chapter will provide an insight into Europol’s main methods and means.

4.1. The Europol Information System

One of Europol’s core databases is the Europol Information System (EIS). Through this system, the Member States can share and retrieve information about persons, events and devices connected with a criminal case (e.g. suspects, weapons, phone numbers, number plates, passports).

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. 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 that fall within Europol’s mandate.

Art. 12 (2) ECD contains an exhaustive list of the type of data that may be stored and processed: name, date and place of birth, nationality, sex, place of residence, profession, identification documents, fingerprints and DNA profiles.

(19) Art. 12 (1) ECD.
Thanks to technical developments, data does not need to be entered manually into the EIS. Specifically designed dataloaders have been installed in many national databases to automatically upload relevant data to Europol. Organisational and technological safeguards ensure that only data that comply with Europol’s mandate are transmitted. This selective data loading is an example of ‘privacy by design’, in order to guarantee the high level of data protection in place at Europol.

Still, the amount of data running through the dataloaders is remarkable. More than 200,000 entries can be found in the EIS. Approximately 10,000 searches are carried out every month.

Data processed in the EIS cannot be kept indefinitely: Europol may only store data for well-defined periods of time \(^{(20)}\). In general, information shall only be held for as long as is necessary and must be reviewed no later than three years after insertion.

Review should in any case take 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 \(^{(21)}\).

### 4.2. Analysis work files

Criminal analysis at Europol is carried out by means of the Analysis Work Files (AWFs), which provide the framework for operational collaboration within the EU. In contrast to the EIS, the AWFs aim at focused analysis in a specific crime area. Dedicated phenomena can be individually targeted and tackled (e.g. Islamist terrorism, trafficking in human beings, money laundering), allowing the relevant data to be collected and analysed in one comprehensive environment.

\(^{(20)}\) Art. 20 ECD.
\(^{(21)}\) Art. 12 (5) ECD.
Accordingly, data in the AWFs may not only relate to suspects and (future) criminals, but also to contacts, associates, witnesses, victims and informants. The list of data categories (22) 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 in this environment.

Access to AWFs and the content of individual files are strictly limited by their respective Opening Orders (23). Firstly, the Opening Orders specify the purpose of the file. Information that does not fit the purpose description may not be inserted into an AWF. Data already contained in an AWF may not be used for any other purpose, such as training or administrative enquiries by tax authorities. 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’.

In addition, Art. 14 (1) ECD emphasises that 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.

Furthermore, the Opening Orders determine the nature of the data and the individuals on whom data may be stored, the conditions under which that data may be communicated to certain recipients and the appropriate procedure for doing so, as well as time limits for retaining the data. With regard to data retention the same principles apply as for the EIS (24).

(22) Art. 6 AWF Rules.
(23) Art. 5 AWF Rules.
(24) Art. 20 (1) ECD.
Participation in analysis activities is limited to an expressly nominated Analysis Group: in general, only 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.

At the same time, the members of the analysis group can set limits on the use of their data by assigning predefined handling codes. For instance they can determine or exclude potential recipients (25).

In order for the AWFs to function and allow for efficient analysis, the data in the files must be thoroughly checked: 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. As a result, Europol may only process data if accurate and up to date. After an initial check when inputting the data, regular reviews take place to ensure that the data continue to fulfil these requirements (26). Regular auditing is thus indispensable for the functioning of the AWFs.

4.3. Information security

Another important aspect in connection with Europol’s databases is information security. Data security safeguards are essential as soon as personal or sensitive strategic data are processed. Under the ECD, Europol has an obligation to implement ‘the necessary technological and organisational measures’ to protect its data (27). Accordingly, several technological safeguards have been implemented at Europol to prevent unauthorised access to and use of data. In addition, reliable protection against data loss or system malfunction is ensured.

(25) Art. 14 (6) ECD.
(26) Art. 27 ECD with Art. 5 Convention 108, Art. 29 (1) ECD.
(27) Art. 35 ECD.
Access to information and its handling is defined and restricted by the applicable classification. Europol distinguishes three types of Europol information: Europol Public Information; Europol Unclassified – Basic Protection Level information; and Europol classified information.

Europol classified information is further subdivided into four classification levels based on the potential impact caused by its unauthorised disclosure:

**RESTREINT UE / EU RESTRICTED**
**CONFIDENTIEL UE / EU CONFIDENTIAL**
**SECRET UE / EU SECRET**
**TRÈS SECRET UE / EU TOP SECRET**

Each type of information accords a different set of security measures to be applied in order to protect it against unauthorised disclosure. For instance, information classified EU Confidential or above may only be created or reproduced by duly authorised Confidentiality Officials using special secure equipment in order to ensure full traceability also as far as hardcopies are concerned.
4.4. SIENA

Having introduced Europol’s main systems for processing data and its general approach towards information security, it is worth considering how information finds its way into those systems.

In an organisation like Europol, with its main focus on information exchange, safe and swift transmission of data is essential. Information from a Member State must reach Europol without the risk of interception, and vice versa. In order to exchange information swiftly and securely, a tailor-made messaging system has been implemented at Europol: namely, the Secure Information Exchange Network Application – SIENA.

As is the case for the storage and analysis of data, transmission to and from Europol must follow data protection principles and information security safeguards. The state of the art SIENA infrastructure, hosted in the secure environment of Europol’s New Headquarters, allows Member States, third parties and Europol to communicate through a fast, secure and user-friendly channel.
Europol is obliged to keep a record of transmissions. Taking this into account, the SIENA system automatically documents all communication processes. To further ensure the responsible handling of personal data, information is only transmitted by Europol to other partners if “the recipient gives an undertaking that the data will be used only for the purpose for which they were transmitted” (28).

4.5. The liaison bureaux

The technical provisions for optimising information exchange are rounded out by the unique concept of the Europol Liaison Bureaux. Each Member State seconds at least one representative to Europol headquarters, providing every Member State with its own base on the Europol premises (29). In addition, third States with which Europol has

\[(28)\] Art. 24 (2) ECD.
\[(29)\] Art. 9 ECD.
concluded cooperation agreements are represented by at least one Liaison Officer, as is Interpol. As a result, officers from 36 countries plus Interpol are located in one spot, making communication between them and their respective national authorities easy and fast. The Liaison Bureaux are in 24/7 contact with their designated Europol National Unit (ENU) (30) via the SIENA system. Law enforcement officers in the participating countries address requests and messages to that National Unit which then forwards it to the Europol Liaison Bureau. In this way, language barriers are effectively overcome: officers can communicate with the National Unit in their mother tongue and will receive an answer in the same language.

These translation capabilities and office proximity are invaluable assets for any cross-border law enforcement operation. A striking feature in that regard is the human factor. Europol’s Liaison Officers are all neighbours, the next country always just a door away. This is a benefit that cannot be overestimated when it comes to ensuring that a national request is given the necessary priority in another State’s operations.

5 Reaching out: information acquisition beyond Europol

The data protection rules apply to all forms of personal data exchange between Europol and the Member States. However, Europol’s network of information extends far beyond that area. Recognising how beneficial information from third parties can be in certain cases, Europol maintains numerous external contacts and cooperation agreements. For each form of external data communication, robust rules have been implemented in the ECD to ensure that its standards are followed in all areas. For instance, data may not be transmitted to third entities without the owner’s prior consent (31).

Since external parties are not subject to the ECD data protection regime, Europol must ensure that adequate safeguards are in place. This concerns protection of the rights and freedoms of data subjects with regard to the processing of personal data as well as security risks related to the transfer of classified information.

(30) Art. 8 ECD.
(31) Art. 24 (1) ECD.
5.1. EU institutions

As far as data exchange inside the European Union is concerned, Art. 22 ECD provides a basis for Europol to ‘establish and maintain cooperative relations’ with a (non-exhaustive) list of EU institutions and agencies, such as Eurojust, the European Central Bank or the European Anti-Fraud Office (OLAF). Where no agreement has yet been concluded, Europol can still exchange information, including personal data, provided that the exchange is necessary for the recipient’s tasks.

5.2. Third parties

Europol’s relations are not restricted to Member States and EU institutions. Since crime has no respect for borders, it is vital to cooperate with states or institutions outside the European area. These relations with third parties are regulated in Art. 23 ECD.

In general, there are two types of cooperation agreement that Europol can enter into with third states or entities: strategic and operational agreements.

Strategic agreements allowing for the exchange of general intelligence have been concluded with Albania, Bosnia-Herzegovina, Colombia, Moldova, Montenegro, Russia, Serbia, Turkey and Ukraine (32). Europol has also concluded an agreement with the UN Office on Drugs and Crime and the World Customs Organization.

Personal data may, however, only be exchanged where an operational agreement is in place. Europol may conclude such an agreement with third parties which have an adequate level of data protection.

(32) State of play as per November 2012. Art. 23 (8) ECD.
The process for concluding an operational cooperation agreement involves a prior data protection assessment of the third party to ensure that the necessary data protection and confidentiality rules are in place and in practice.

States with which an operational agreement has been concluded are Australia, Canada, Croatia, the former Yugoslav Republic of Macedonia, Iceland, Monaco, Norway, Switzerland and the USA. In addition, Europol has an operational cooperation agreement with Interpol and Eurojust. An operational cooperation agreement has been concluded with Columbia, pending ratification in accordance with national law (33).

Exceptionally, and in the absence of a cooperation agreement, personal data may only be transmitted under the strictest conditions. One scenario is that of the ‘ticking bomb’: what if Europol learns about a threat and cannot react in time because information cannot be exchanged without an operational cooperation agreement?

Europol’s data protection regime takes account of such situations as specific exemptions have been implemented for cases of imminent threats. Europol may transmit personal data where the Director deems it ‘absolutely necessary to safeguard the essential interests of the Member States concerned within the scope of Europol’s objectives or in the interests of preventing imminent danger associated with crime or terrorist offences’ (34).

(33) State of play as per October 2011.
(34) Art. 23 (8) ECD.
It is also noteworthy that the receipt of data as a one-way flow of information from third parties to Europol can be allowed prior to the entry into force of a cooperation agreement. However, the third party in question at least needs to be included in a predefined Council list of potential future cooperation partners of Europol.

### 5.3. Private parties

In addition to states and institutions such as Interpol and Eurojust, Europol can receive information from private parties, i.e. bodies governed by private law, such as companies, business associations or non-profit organisations \(^{(35)}\).

As with any transfer of personal data, this process is subject to data protection controls. In particular, the possibility to route information from a private party to Europol depends on what type of law is involved.

If the private party is established under the law of a Member State (for example, a German *GmbH* or a British *Ltd*), personal data from that party may only be processed if it has been transmitted via the respective Europol National Unit (in this case, the German *Bundeskriminalamt* or British *Serious Organised Crime Agency*). This practice ensures that the respective underlying national law is applied, including any data protection safeguards.

\(^{(35)}\) Art. 25 (1) (a) ECD.
Correspondingly, where a private party has been established under the law of a third state with which Europol has concluded an operational cooperation agreement, personal data may only be routed via the designated contact point of that state.

Where there is no such agreement in place, Europol may only process the data on the basis of a memorandum of understanding which itself is subject to a number of requirements and safeguards.

The option to obtain information from private parties is a significant asset for Europol in the context of concrete ongoing investigations.

Furthermore, the organisation can increase its expertise and knowledge and explore new methods and approaches. Cooperation with external specialists from such diverse areas as academia, trade associations and private companies, as foreseen by Europol’s Outreach programme, present invaluable benefits to the ever-developing agency.
5.4. Publicly available sources

Under the ECD, Europol may also ‘directly retrieve and process information including personal data, from publicly available sources, such as media and public data and commercial intelligence providers’ (36).

While the first image that comes to mind might be one of Europol agents browsing Wikipedia or Google for information, the main asset of this new provision lies elsewhere: criminals, especially terrorist groups, often communicate through public websites. These groups will issue threats, claim credit for attacks or spread indoctrination material over the internet. So-called ‘terror manuals’ offer detailed instructions on how to organise attacks or build weapons and bombs.

Europol may monitor those websites and analyse their information. From a European Union perspective, this adds significant value, since the evaluation of large amounts of data and the scrutiny of innumerable web pages in many different languages requires considerable technical and human resources that would not be available to a single Member State. The agency has therefore added the Check the Web portal to its AWFs, where relevant information is gathered and processed in order to gain an overview of worldwide Islamist terrorist activity. Similar initiatives regarding other crime phenomena are under consideration.

Exercising the rules or: who watches the watchdog?

The data protection framework in place at Europol is one of the strongest in the world. Nevertheless, simply having a robust set of rules and regulations does not suffice to ensure effective data protection in practice. Therefore, several entities monitor and ensure compliance with the data protection rules at Europol.

(36) Art. 25 (4) ECD.
6.1. The Data Protection Officer – an independent insider

The Data Protection Office (DPO) is an integral part of Europol and the initial point of contact for all data protection issues. The unit is headed by the Data Protection Officer, who is appointed by Europol’s Management Board on a proposal by the Director.

The Data Protection Officer’s main task is to ensure lawfulness and compliance with the ECD as far as data protection is concerned (37). A central part of this role is to provide guidance and independent advice, in particular to the Operations Department. Applying the framework can sometimes be a complex and legally difficult task; for example when determining whether or not data may be sent to third parties, or when negotiating operational cooperation agreements. Furthermore, the DPO is the main contact point to its external data protection supervisors.

Its unique status within the Europol architecture enables the DPO to get involved in planning processes from the very beginning: in that way, the DPO not only provides ex post monitoring, but participates in the development of systems, the execution of ongoing operations and the training of staff members.

(37) Art. 28 ECD.
At the same time, the DPO is also a functionally independent part of the organisation. It operates as an informed but independent advisor. In cases of non-compliance the DPO can escalate the matter in a predefined procedure, addressing first the Director, then the Management Board and subsequently the external supervisory authority if necessary (38).

What appears to be a contradiction at first glance is in fact a very effective concept: the DPO as part of the organisation works on enabling operational business in accordance with the applicable data protection legal framework. In this setting, the DPO provides professional, reliable and solution-oriented advice to all units. It is in the interest of the organisation to have an internal – yet independent – judgement on where a line needs to be drawn between operational demands and the constitutional right of protection of personal data. Europol cannot and does not have an interest in performing outside the applicable data protection framework.

To ensure lawfulness and compliance with the ECD, the DPO can employ various methods and tools. For example, a central feature of the work related to data protection is to conduct regular audits on Europol’s databases. To this end, the DPO has access to all data processed by Europol and to all Europol premises. Incorrect data, outdated information or unnecessary entries are recorded so they can subsequently be rectified by the data owner. Again, high standard technology plays an important part in this aspect of Europol’s work. State of the art analysis software is used for carrying out audits; additionally, logs of access or other action performed within the files are automatically created. By means of these logs, any retrieval or modification of personal data can be traced back to its originator, allowing the DPO to verify the necessity and legality of the process (39).

(38) Art. 28(4) ECD.
(39) Art. 18 (ECD).
Furthermore, the DPO’s specialists regularly examine measures of information security for planned and existing projects. Wherever personal data are being processed, a risk assessment is essential and the necessary safeguards have to be determined and implemented. This includes privacy by design for any new technical infrastructure. The implementation has to be monitored, verified and maintained throughout the lifecycle of the database.

Since these projects often involve complex technological processes, DPO staff also comprises expertise in computer sciences.

Furthermore, the DPO is involved in an advisory capacity in negotiations with third States and, in particular, in verifying whether the future partner can guarantee an adequate level of data protection. For example, DPO officials will not only scrutinise the obligatory reports on the respective national data protection provisions, but will also undertake study visits and assess their implementation on-site.

The DPO also documents all operations processing personal information, including staff data. All units are obliged to notify the DPO of any such operation. This notification enables the DPO to be aware of all ongoing and planned processes to ensure that the appropriate data protection safeguards are in place. In particular in the sensitive area of investigations into serious and organised crime or terrorism, protecting staff data is, in the very sense of the word, vital. Data protection rules shield staff from having information about them and their families accessed freely within the organisation or leaked to unauthorised persons outside. In particular, law enforcement staff depend on their information to be kept private.

The DPO consequently raises awareness on the risks associated to careless handling of personal details.
Another task the DPO is entrusted with is to ensure that data subjects are informed of their rights. An individual can obtain information on whether personal data relating to him or her are processed in Europol’s systems and to have such data communicated to him or her, or checked under the conditions laid down in the ECD (40). To this end, the data subject can submit a request to Europol via the competent authority of any Member State. Checks of the Europol systems are carried out by the DPO. Decisions on access to data are conditional upon close cooperation between Europol and the Member States directly concerned by a communication of such data.

The ECD affords exemptions on the provision of information only if refusal is necessary to:

- enable Europol to fulfil its tasks properly;
- protect security and public order in the Member States or to prevent crime;
- guarantee that any national investigation will not be jeopardised;
- protect the rights and freedoms of third parties (41).

In such cases the agency will notify the person concerned that it has carried out the checks, but will not reveal the result. If the individual making the request is not satisfied with Europol’s reply, he or she can appeal to the Joint Supervisory Body (42).

If data that are incorrect or processed in breach of the ECD were transmitted directly to Europol by Member States, the Member States concerned shall correct or delete such data in collaboration with Europol. Moreover, Europol has an obligation to immediately notify the Member State or other source of the data in question, as well as any recipients (43).

(40) Art. 30 ECD.
(41) Art. 30 (5) ECD.
(42) Art. 32 ECD.
(43) Art. 31 ECD.
Additionally, the data subject has a right to obtain compensation for damages suffered as a consequence of unauthorised or incorrect data processing at Europol (44). This rule is yet another safeguard for ensuring that Europol and the Member States adhere to the data protection regime. Effective data protection can correspondingly also be regarded as a viable instrument to shield the organisation and its Member States from such claims.

In its first years, Europol received a relatively low number of requests, with an average of about 15 cases per year. In 2007, however, there was a marked increase in the number of requests, with more than 120 requests: this trend continued, peaking at 560 requests in 2012.

Citizens have clearly become more aware of their rights: for example, the websites of Member States’ data protection authorities contain information on how to exercise such a right; campaigns run by groups or individuals provide advice on how to approach organisations in this regard; the Europol Joint Supervisory Body’s website highlights the rights of the individual under the ECD.

The DPO also acts as a link to the Joint Supervisory Body (see below). In this function, the DPO informs the relevant authorities bodies about Europol’s activities in the field of data protection measures and fosters a productive exchange of views on these matters.

(44) Art. 52 ECD.
6.2. The Joint Supervisory Body

While the DPO, though independent in the performance of tasks, is an integral part of the organisation, the Joint Supervisory Body (JSB) provides external control (45).

The JSB consists of representatives of the national data protection authorities of all 27 Member States. These dedicated experts have broad experience in the particular field of data processing in a law enforcement environment. Their task is to review the activities of Europol from a data protection perspective. To this end, the JSB has the power to inspect all Europol files at any time. It invokes that right at least once a year by performing a thorough inspection visit at the Europol premises in close cooperation with the DPO. Such an inspection covers all Europol’s processing operations and results in the delivery of an extensive and detailed report, including findings and recommendations. Ad hoc inspections are carried out if deemed necessary.

So far, these inspection visits have been a useful tool to further develop Europol’s data protection framework, demonstrating the fruitful and productive cooperation between both institutions. According to the JSB, Europol has ‘recognised the importance of data protection, not just as a necessary element of meeting its human rights obligations, but also a means of providing reassurance to contributing Member States’ (46).

6.3. National supervisory bodies

In addition to the internal control provided by the DPO and the external control performed by the JSB, each Member State has its own national supervisory body. These national authorities monitor independently, in accordance with the respective national law, the communication of personal data to and from

(45) Art. 34 ECD.
(46) Mr. David Smith, Chairman of the JSB, 28th January 2008.
Europol (47). Members of these supervisory bodies also have access to the documents and premises of their Liaison Officers at Europol.

Further to the rights of data subjects referred to previously, each individual can request their national supervisory body to ensure that the input or communication of their data to Europol as well as the consultation of that data by the Member State is compliant with applicable national law.

To return to the very beginning of this brochure: Are we heading for ‘1984’ reloaded?

The answer can only be a clear ‘No’. The previous chapters have illustrated the solid data protection regime at Europol on paper as well as in practice. Ultimately, what Europol strives to protect is an Area of Freedom, Security and Justice. The aims of preventing and combating crime and terrorism are balanced against the goal of safeguarding the freedom of individuals. In fact, they go hand in hand: at Europol, it is widely recognised that the data protection rules in place are essential for the success of operations.

Data protection directly contributes to Europol’s analysis and operational work. The rules in place ensure a high level of data quality which is a precondition for high quality analysis. Europol’s analysis reports directly influence operations in Member States often leading to the arrest of persons involved in serious crime.

(47) Art. 33 ECD.
However, making an arrest is not the end of the story. Data that is obtained or processed unlawfully may not be admitted as evidence in court. Information provided by Europol must be beyond doubt in the interest of data subjects and law enforcement.

Europol’s aim is to serve operational business needs in the best possible way while maintaining a high standard of data protection and security. Europol and its partners are united by one vision: making Europe safer.
PHOTO CREDITS

Review and Cover Jan Ellermann, Maarten Daman | Page 5 © Marinos Markides
Page 6 © Europol | Page 7 © Shutterstock | Page 9 © Europol | Pages 10 © Fotolia
Page 12 © Spanish Police | Page 13 © Alexandra Wegner | Page 14 © Europol/Fotolia
Page 15 © Fotolia | Page 16 © Europol | Pages 17 © Fotolia | Page 18 © Fotolia
Page 19 © Europol/Shutterstock | Page 20 © Europol | Page 22 © shutterstock
Page 27 © Jaakko Suomela; © Antte Lauhamaa-Wikstrom | Page 28 © Shutterstock
Page 29 © Europol | Page 30 © Europol | Page 31 © Europol | Page 33 © Shutterstock

Europol would like to thank the law enforcement photographers whose photographs feature in this publication.
Europol

Data Protection at Europol

Luxembourg: Publications Office of the European Union

2011 – 34 pp. – 14.8 x 21 cm

ISBN 978-92-95078-31-4
doi:10.2813/38585
HOW TO OBTAIN EU PUBLICATIONS

Free publications:
• via EU Bookshop (http://bookshop.europa.eu);
• at the European Union’s representations or delegations. You can obtain their contact details on the Internet (http://ec.europa.eu) or by sending a fax to +352 2929-42758.

Priced publications:
• via EU Bookshop (http://bookshop.europa.eu).

Priced subscriptions (e.g. annual series of the *Official Journal of the European Union* and reports of cases before the Court of Justice of the European Union):
• via one of the sales agents of the Publications Office of the European Union (http://publications.europa.eu/others/agents/index_en.htm).
DATA PROTECTION OFFICE

data protection
at europol