

e 2 0  
u 1 8  
• a t

Parliamentary  
Dimension  
Austrian Presidency  
of the Council of  
the European Union



REPUBLIC OF AUSTRIA  
Parliament

## **DRAFT AGENDA**

### **Joint Parliamentary Scrutiny Group on the European Union Agency for Law Enforcement Cooperation (Europol)**

*- 3rd meeting -*

**24-25 September 2018**

**European Parliament, Brussels**

Room:

24 September 2018: Hemicycle

25 September 2018: PHS 3C50



## **Joint Parliamentary Scrutiny Group on the European Union Agency for Law Enforcement Cooperation (Europol)**

*- 3rd meeting -*

### **Table of content**

1. Europol's Multiannual Programming 2019-2021
2. Contribution of the Cyprus delegation to the JPSG meeting
3. Contribution of the Romanian delegation to the JPSG meeting
4. Proceedings of the 107th Meeting of the Europol Management Board - Letter from Tsvetan TSVETANOV, Head of the Bulgarian Delegation to the JPSG
5. Europol Regulation
6. Rules Of Procedure of the Joint Parliamentary Scrutiny Group on Europol
7. Summary Conclusions by the JPSG Co-Chairs from the 2nd JPSG Meeting





A 000834 01.02.2018  
The Hague, 31 January 2018  
MBS 022.2018

## Management Board

Mr Antonio Tajani  
President of the European Parliament

### Consultation on Europol's draft Multiannual Programming 2019-2021

Dear President Tajani,

In accordance with Articles 12(1) and 51(2)(c) of the Europol Regulation I am pleased to transmit to the Joint Parliamentary Scrutiny Group (JPSG), for consultation, Europol's draft multiannual programming 2019-2021.

The draft multiannual programming sets out the overall strategic programming, including the objectives, expected results and performance indicators; the resource planning, including the multiannual budget and staff; and the strategy for relations with third countries and international organisations.

I look forward to the JPSG's input on Europol's draft multiannual programming 2019-2021 and remain at your disposal for any further information you may wish to obtain.

Yours sincerely,

A handwritten signature in blue ink, appearing to read "Pärkna".

Mr Priit Pärkna  
Chairperson

Attachments: draft Multiannual Programming 2019-2021 (#945558v2).



The Hague, 30 January 2018

EDOC# 945558v2

**Draft**

## **Europol Programming Document**

**2019 – 2021**

### **SECTION II –**

## **Multi-annual programming 2019 – 2021**

---

## **List of Acronyms**

ADEP	Automation of Data Exchange Processes
AFIS	Automated Fingerprint Identification System
AP	Analysis Project
ARO	Asset Recovery Office
CAR	Conflict Armament Research
CATS	Coordinating Committee in the area of police and judicial cooperation in criminal matters
CBRN	Chemical, Biological, Radiological and Nuclear
CGN	Carrier-grade network address translation
COM	European Commission
COSI	Standing Committee on Operational Cooperation on Internal Security
CT	Counter-Terrorism
EC3	Europol Cybercrime Centre
ECA	European Court of Auditors
ECD	Europol Council Decision
ECTC	European Counter Terrorism Centre
EEAS	European External Action Service
EMAST	EU Mobile Analysis Support Teams
EMIST	EU Mobile Investigation Support Teams
EMPACT	European Multidisciplinary Platform against Criminal Threats
EMSC	European Migrant Smuggling Centre
EPE	Europol Platform for Experts
ESOCC	European Serious and Organised Crime Centre
ETS	European Tracking Solution
EUIPO	European Union Intellectual Property Office
EU RTF	EU Regional Task Force
FIU	Financial Intelligence Unit
HR	Human Resource
IAC	Internal Audit Capability
IAS	Internal Audit Service
IDMC	Integrated Data Management Concept
IOCTA	Internet Organised Crime Threat Assessment
IRU	Internet Referral Unit
ISF	Internal Security Fund
J-CAT	Joint Cybercrime Action Taskforce
JHA	Justice and Home Affairs
JIT	Joint Investigation Team
JOT	Joint Operation Team
JSB	Joint Supervisory Board
LEA	Law Enforcement Authorities
MB	Management Board
MENA	Middle East and North Africa region
MS	Member State
MTIC	Excise and Missing Trader Intra Community
PIU	Passenger Information Unit
QUEST	Querying Europol's systems
PNR	Passenger Name Record
SIENA	Secure Information Exchange Network Application
SIS	Schengen Information System
SOCTA	Serious and Organized Crime Threat Assessment
TFTP	Terrorist Finance Tracking Programme
TP	Third Parties
UMF	Universal Message Format
US ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
VIS	Visa Information System

## SECTION II - Multi-annual programming 2019 – 2021

### 1. Multi-annual objectives

Based on the Financial Regulation and following Commission guidelines, Europol has prepared its Programming Document 2019-2021 containing multi-annual and annual programming components combined with indicative budget and resource allocations.

The multi-annual component of the Programming Document is largely based on the Europol Strategy 2016-2020 which was adopted by Europol's Management Board on 1 December 2015. The agreed strategic objectives are incorporated in the Programming Document as multi-annual objectives and are linked to the 2019 annual work programme, objectives and actions under Section III. A mid-term review of the Europol Strategy is envisaged for 2018, while the development of multi-annual strategic objectives covering the years 2020+ should take place in 2019.

In the next three years, Europol will continue to support law enforcement authorities in their fight against serious and organised crime and terrorism, but the strategic emphasis of the organisation will progressively shift from laying the foundation of increased capability to one based on full-scale delivery of operational service and impact. Europol, in its Multi-annual programming 2019-2021, focuses on consolidating all its capabilities and expertise, to deliver the most effective support to MS investigations. The focus of Europol's work will therefore be placed on two fundamental themes:

- a) making a significant contribution to criminal information management in the EU
- b) delivering maximum operational impact in its operational support to MS





## **2. Multi-annual programme**

### **Goal 1: Europol will be the EU criminal information hub, providing information sharing capabilities to law enforcement authorities in the MS**

The information management capabilities of Europol lie at the heart of its mandate, as they allow for increased cooperation between the Member States and Europol, and are crucial in obtaining the necessary intelligence to tackle cross-border crime. Information management includes the access to, collection and organisation of the structure, processing and delivery of information from multiple sources and in multiple formats to the Member States. To achieve its goal, Europol's work will focus on three axes: firstly on re-evaluating the information architecture of the organisation, in particular in the context of the new integrated data management concept afforded by the new Europol Regulation and in the context of improved EU interoperability of information systems; secondly, on the provision of fast, reliable and uninterrupted first line response and thirdly, on enhancing partnerships to develop a more comprehensive intelligence picture.

#### **1.1 Develop the necessary ICT capabilities to maximise the exchange and availability of criminal information**

Europol will exploit new technological developments and be a significant contributor to the increased integration and interoperability of law enforcement systems in Europe.

The new legal framework of Europol removes the emphasis from specific ICT systems and databases and introduces a new integrated data management concept (IDMC) which focuses, first and foremost, on placing the business needs of the law enforcement community as the main driver of obtaining, storing and disseminating the information available. In concrete terms, the rules for information processing are related to the data itself – rather than the systems or databases used to store it. As a consequence Europol, in close consultation with Member States, will have the opportunity to use this flexibility to modernise its systems architecture and information management strategy to ensure the best ways to manage criminal information and enhance the analytical capabilities of Europol based on MS' operational requirements. The integration of data will ensure that links across crime areas will be more easily identified and therefore, analytical support will be of increased value. The implementation of this new concept will lead to an evolution of existing systems such as the EIS and the development of new ICT solutions, including means of innovation such as, data science and 'smart' technologies.

Other major drivers behind information exchange capabilities will be the ever-increasing amount of available information and new technological trends such as de-centralised systems of information sharing. Europol will work towards providing Member States with optimal solutions by examining and applying the most appropriate topologies (e.g. central collecting or connecting data, ADEP concept) to ensure the necessary access to information and the provision of a complete intelligence picture. The access to and cross-checking of data in databases such as Prüm, SIS II and VIS will also be considerations of the new design. Travel intelligence such as PNR and ETIAS are expected to have a significant effect on the requirements of Europol's infrastructure.

Europol will build on the success of SIENA and further develop it as the system of first choice for secure law enforcement information exchange and communication.

#### **1.2. Provide effective and immediate first-line information exchange**

The information intake and data handling model will be reviewed in line with the new integrated data management concept and taking into account the increasing influx of high volume data.

Europol will respond to the needs of Member States for fast and uninterrupted service in a number of ways. A first-line 24/7 information hub is available to maximise intake, initial

processing and availability of information to Member States. In addition, Europol will work with Member States to increase the quality of their cooperation, in particular with regard to the quality of information exchanged and the speed of response (e.g. through increased usage of the Universal Message Format (UMF)).

Finally, Europol will further invest in standardisation, automation of cross-matching, optimisation of information flows and flexible resource allocation with a view to making more efficient use of human resources while managing to respond to all information processing requests in a timely manner.

### **1.3. Strategically enhance partnerships with cooperation partners**

An enhanced multi-disciplinary approach is becoming increasingly more relevant for Europol in delivering its mission, bringing together necessary expertise and information from an expanding range of partners.

Europol will continue to promote and further develop its cooperation with all competent law enforcement authorities including Customs and Counter-Terrorism services in the MS. At the same time, Europol will aim to further strengthen its partnership with third states (e.g. US, Mediterranean countries, the Western Balkans, Middle East and North African countries), through initiatives which preserve Europol's operational nature and its support function to Member States. In view of the global challenges the EU is facing, for example in the area of cybercrime, migration and terrorism, cooperation with Interpol will remain particularly relevant and will be enhanced through closer alignment and setting of common strategic actions.

EU agencies (e.g. Frontex, Eurojust) will remain important partners and cooperation will be further enhanced on the basis of complementarity. In particular, Europol and Frontex will closely cooperate in matters related to irregular migration while Europol and Eurojust will continue strengthening their cooperation through Joint Investigation Teams and in the area of cybercrime. The work of Europol on Intellectual property crime will be enhanced through the cooperation with EUIPO. Cooperation with other agencies, especially in the area of Justice and Home Affairs (e.g. CEPOL, eu-LISA, FRA), is being developed and implemented as needed for initiatives of common interest.

In addition, and more significantly than in the past, Europol's ability to cooperate with the private sector will be key in achieving the best operational results; the provisions of the new Europol Regulation will largely determine the extent to which Europol will cooperate with private partners.

The new External Strategy 2017-2020 as endorsed by Europol's Management Board at the end of 2016 has further defined the focus and steps to be taken towards enhancing cooperation with third countries and international organisations (please see next chapter).

### **Goal 2: Europol will provide the most effective operational support and expertise to MS investigations by developing and employing a comprehensive portfolio of services**

Europol will provide high quality operational support to MS investigations in three key priority areas, aligned with the European Agenda on Security, namely Serious and Organised Crime, Cybercrime and Counter-Terrorism.

In order to achieve maximum impact and operational results, Europol will dynamically adjust its operational delivery models and use of human resources. Existing and new operational capabilities and expertise will be employed as required to tackle the challenges in each of the key crime areas. Europol's Analysis Projects will support MS investigations in the area of Serious and Organised Crime within the priorities set in the EU Policy Cycle (2018-2021), while special focus will be placed in the area of facilitated irregular migration. The European Cybercrime centre will continue to drive and support intelligence-led actions and provide specialised forensic and technical support. In the area of counter-terrorism, Europol will focus on promoting and facilitating cooperation and information sharing with a view to improving the intelligence picture and increasing operational

## **Europol Unclassified – Basic Protection Level**

support to MS. In all priority areas Europol will provide an effective platform for the coordination of operations carried out by MS.

A number of cross-cutting operational capabilities will also be used to support the MS. Europol will further develop and adjust Europol's analytical products to match the needs of the MS. Europol will further support the EU Policy Cycle and aim to increase its impact on the set priorities. The embedment of FIU.net at Europol and the work on asset recovery will aim to increase the use of Financial Intelligence in all crime areas while access to PNR data will allow for identifying further criminal links. Europol will also continue sharing its expertise and building capacity at Member States through its training and special tactics capabilities.

Europol will continue delivering in selected areas and as required by the Member States, central capabilities and expertise that are not available widely at national level, to provide cost-effective and enhanced support where a common European response to threats is required.

Europol will be prepared to swiftly adjust its response as required by MS and work more closely with front-line investigators, providing on-the-spot, real-time information exchange and expertise. Europol will aim to support MS by using the most suitable, tailor-made operational delivery models. Based on the assessment of MS needs, Europol's response could include short and longer-term deployments of Europol experts (e.g. through EU mobile investigation support teams or through deployment of Europol experts to CSDP missions), forming a situation centre to coordinate a response to major security events and crises, creating a task force or supporting the formation of multi-national teams to intensify efforts and achieve immediate operational results in areas demanding attention. Finally, Europol will establish the required connections and develop standard operating procedures or protocols, to be able to respond to emerging incidents.

### **2.1. Support MS investigations in the area of Serious and Organised Crime**

Europol has largely embedded the principles of intelligence led policing in its structure, processes and resources. The EU Policy Cycle priorities will be the main driver for operational support provided to MS in the area of Serious and Organised Crime. Additionally, Europol will support Member States' efforts in tackling hierarchically structured, poly-crime Organised Crime Groups ("Mafia-type" groups). The work on Intellectual Property Crime will also be enhanced through a cooperation agreement with EUIPO. Europol will continue its work of providing operational analysis, coordination and funding of operational meetings. Large-scale operations and joint action days will be coordinated from Europol HQ with the aim of achieving operational results. The clustering and reduction of the number of Analysis Projects and the exchange of best practices between them will serve to achieve consistent results and optimum allocation of human resources. From 2018 onwards, Europol will support Member States in tackling the priorities defined in the new EU Policy Cycle 2018-2021.

As part of the EU efforts to respond to the migration crisis the European Migrant Smuggling Centre (EMSC) established in early 2016 provides increased operational support to MS in their fight against organised people smuggling networks. The EMSC utilises a combination of operational capabilities to ensure the best operational support; the pre-existing Analysis Projects, JOT-Mare and regional task forces deployed at Migration hotspots were strengthened with EU mobile investigation and analysis support teams, providing on-the-spot operational and analytical support. The expertise of the EU Internet Referral Unit is also used to identify and refer online content relating to the provision of irregular migration services.

## **2.2. Support MS investigations in the area of Cybercrime**

In the area of cybercrime, one of the most dynamic and challenging threats faced by MS, Europol will deliver operational support to cybercrime investigations, in particular addressing those crimes i) committed by organised groups, especially those generating large criminal profits such as online fraud, ii) which cause serious harm to their victims, such as online child sexual exploitation and iii) affecting critical infrastructure and information systems in the European Union.

The European Cybercrime Centre (EC3) will continue pioneering operational capabilities such as advanced digital forensic, technology tools and platforms supporting the MS in protecting society by providing a collective EU response to cybercrime. EC3 will also enhance its Victim Identification capabilities, in particular with regard to child sexual exploitation and continue its work in delivering prevention material.

EC3 will continue engaging with the law enforcement community, supporting the J-CAT and key partners, such as Interpol's ICGI, to identify, prioritise and coordinate operational action against cyber threats, becoming the EU reference for cybercrime investigators.

Increased cooperation with the private sector, academia and NGOs will be pivotal in acquiring multi-disciplinary expertise, promoting innovation and keeping up with the latest security and technological developments that act as facilitating factors for cybercrime.

EC3 will play an increasingly active role in the efforts of law enforcement against the use of encryption for criminal purposes.

## **2.3. Enhance cooperation in the area of Counter-Terrorism**

In the area of Counter-Terrorism, more work is required to achieve better cooperation and sharing of information. Europol will work towards an intelligence-led, user-driven and sustainable approach to collaboration amongst EU MS, partners and Europol on counter-terrorism issues.

The European Counter-Terrorism Centre (ECTC), operational from 2016 at Europol, brings together Europol's existing capabilities to promote and build the necessary infrastructure to enhance information exchange and the ability to provide analytical and operational support in major investigations. A key role for the centre is to support major CT investigations of Member States.

The EU IRU will be used to tackle online radicalisation, while the increased capabilities afforded by the TFTP and the FIU.net will be used to enhance the intelligence picture on terrorism financing. Trafficking in firearms continues to be an enabler of various forms of serious and organised crime and has also emerged as a key concern in the wake of recent terrorist attacks. Europol will increase its support to Member States in the fight against trafficking in firearms. Similarly, it will continue in its efforts to help MS to combat violent extremism, including in relation to the protection of vulnerable communities.

Europol will continue the effort to apply secure, tailored solutions within its EIS and SIENA systems to promote and enhance information exchange in the area of counter-terrorism. From 2017, a 24/7 CT service is available within the Front Office of Europol.

Additionally, in case of a major terrorist incident, Europol will be able to provide a First Response Network to best support Member States' investigations.

## **2.4. Develop and manage high quality analytical support and an evolving portfolio of cross-cutting operational capabilities**

Operational and strategic analysis will remain the basis of Europol's operational support. Analysis products will evolve in order to remain relevant with the aim to make best use of the information available to Europol to provide unique and valuable intelligence to Member States. This will include identifying the needs of Member States in terms of the type of analysis needed (e.g. tactical, strategic or operational), investing in the training of Europol analysts, further developing and maintaining quality standards for analytical support and

## **Europol Unclassified – Basic Protection Level**

exploring new methods such as big data analysis. Focus will also be placed on identifying and assessing future developments of crime. The new opportunities afforded by the integrated data management will ensure the provision of high quality value-adding analytical products.

Europol will step up its contribution in all stages of the EU Policy Cycle on organised and serious international crime. Europol will support the Policy Cycle priorities with the aim to improve the operational focus of operational actions and in addition, will provide Grants for the implementation of the actions. Finally, the coordination of cross-border investigations within the Policy Cycle priorities, including highly complex operations involving numerous operational actions, will be refined in order to identify the best ways to achieve operational impact.

The successful completion of the integration of FIU.net into Europol will present significant opportunities to increase the engagement of national FIUs in Europol's activities and to make better use of financial intelligence in national and international investigations in all priority areas.

Additionally, the use of financial intelligence in combination with other information such as PNR records can enhance the intelligence picture and provide the missing links to Member States in all priority areas; in this respect, Europol will assume an active role in PNR information exchange and gradually develop a travel intelligence capability.

### **Goal 3: Europol will be an efficient organisation with effective governance arrangements and a positive reputation**

As of 1 May 2017, a new Europol Regulation is applicable.

As any organisation, in particular in the continuing climate of economic austerity in the EU, Europol aims at achieving the most efficient and effective use of all its resources (human, financial, facilities, ICT infrastructure and services). As a public organisation, Europol will continue adhering to the highest accountability and governance standards and will strive to introduce further efficiency gains in its processes.

Europol will continue to build its profile as a trusted partner in EU policing and promote the results of cross-border law enforcement cooperation in the EU. Finally, Europol will continue advocating for the needs of the European law enforcement community.

#### **3.1. Ensure effective, efficient and accountable management of Europol's resources**

Europol will remain vigilant in managing its human and budgetary resources in the most efficient way with a view to providing maximum operational support to Member States.

Further efficiency gains will be introduced through streamlining of reporting, processes and monitoring of resource allocation (human resources and budget).

ICT and building requirements will be significantly adjusted to support the vision and strategy while, at the same time, adhering to the strict security and data protection standards of Europol. A new ICT delivery strategy will ensure the optimisation of the delivery of ICT systems in line with business needs.

Europol will maintain its high accountability standards by addressing audit and evaluation recommendations and by adhering to its internal control standards. As a consequence of the Europol Regulation, Europol will be subject to new supervision and oversight from the European Data Protection Supervisor (EDPS) and the Joint Parliamentary Scrutiny Group (JPSG). In line with the European Union's policy, Europol will continue enhancing the transparency of its activities by facilitating access to documents through a public access register.

In order to best support Member States, Europol will continue to identify and develop the right staff competencies and skills and strive to obtain the best resources.

**3.2. Promote the added value and achievements of EU law enforcement cooperation to stakeholders and EU citizens**

Europol will continue to build its profile as a trusted partner in EU policing and promote the benefits and the value added from cross-border law enforcement cooperation to relevant stakeholders.

Based on on-going efforts Europol will take further actions to raise awareness about its services and the advantages of cooperation to law enforcement actors, decision-makers in the area of police matters and partners from other sectors.

As an EU Agency fostering European cooperation and integration, Europol carries also the responsibility to communicate the added value of its activities to the wider European public.

The joint work of the law enforcement authorities in the EU delivers results which are hard evidence of the added value and benefits that EU cooperation offers to citizens. Success stories of EU police cooperation become indispensable contributions to the positive shaping of citizens' perceptions towards law enforcement, the European Union and its activities.

## Europol External Strategy 2017-2020

In order to strengthen Europol's contribution to consolidating the Security Union, in particular the fight against serious and organised crime and terrorism, Europol's activities in the external domain will focus on the following objectives:

- Optimising Europol's **partnerships**, operational and strategic;
- Strengthening Europol's role as the **preferred platform** for international law-enforcement cooperation against threats related to EU security;
- Reinforcing Europol's position within the **EU security architecture**;
- Promoting Europol's **successful cooperation model**.

### 1. Rationale

Article 12 of the Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol Regulation) explicitly stipulates the establishment of a strategy for relations with **third countries** and **international organisations**, which is also an element of the multiannual overall strategic programming.

Europol's External Strategy, reflecting the Europol Regulation, does not cover cooperation with EU agencies and other partners, such as the private sector.

The Global Strategy for the European Union's Foreign and Security Policy (EU Global Strategy), the European Agenda on Security, followed by the Communication from the Commission delivering on the European Agenda on Security to fight against terrorism and paving the way towards an effective and genuine Security Union and the European Agenda on Migration, represent the basis of Europol's External Strategy for the years 2017 to 2020.

### 2. Goals

The goal of the External Strategy is to guide Europol's cooperation with third countries and thereby fulfilling the agency's objectives set by the Europol Regulation, which is to support the competent authorities of the Member States and their mutual cooperation in preventing and combating serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy.

#### 2.1. Contributing to the implementation of the EU strategic framework

As stated in the EU Global Strategy, the internal and external security is ever more interlinked. The European Union is expected to play a major role in providing a global security. Europol is firmly embedded in this framework.

Europol's external cooperation with core partners from the third countries, like-minded countries and regional groups will be based on operational requirements and the recognised need for effective law enforcement cooperation based on the above mentioned strategic EU documents.

In accordance with the priorities set by the EU's strategic documents in the area of internal security, such as terrorism, hybrid threats, cyber and energy security, organised crime and external border management, **Europol's recognised operational priorities in the context of this strategy will be mainly in the area of serious organised crime, cybercrime and terrorism.** Hybrid threats are a new phenomenon which has to be further analysed in order to define Europol's role and the possible support it could provide in response to this global threat.

#### 2.2. Implementation of the Europol External Strategy

Europol's external relations should primarily focus on **strengthening Europol's contribution** to the fight against the three areas of crime identified in the European Agenda on Security: **Serious and Organised Crime, Cybercrime and Terrorism.**

## Europol Unclassified – Basic Protection Level

Among serious and organised crime challenges, **migrant smuggling** is of particular importance.

Europol's external activities are and will continue to be driven by **operational needs**. They should in particular serve the proper implementation of actions planned under the **Policy Cycle** and foster involvement and active participation of partners – third countries and organisations - in **EMPACT** activities.

Member States remain the leading participants of EMPACT and the mechanism itself primarily serves the internal security of the EU. However, its full and successful implementation, in particular at the operational level, is not possible without close partnership with third states and organisations. Europol will prioritise cooperation with partners that contribute to the implementation of the Policy Cycle.

At the same time, Europol will react flexibly to new or emerging security threats.

### 3. Objectives

Europol's objectives in the external relations domain are as follows:

#### 3.1. Optimising the **network of partnerships**, operational and strategic

Europol's primary objective is to ensure proper exchange of information and strengthening its role as the **EU criminal information hub**. This can be achieved through strategic and operational partnerships with external partners in accordance with the Art 23 and Art 25 of the Europol Regulation.

#### 3.2. Strengthening Europol's role as the **preferred platform** for international law-enforcement cooperation against threats related to EU security

Europol should continue to offer its partners an **attractive environment for cooperation**, both bilateral and multilateral.

The community of **liaison officers** attached to Europol plays a crucial role in facilitating proactive and coordinated activities against the serious crime. It will remain **one of Europol's unique features**. Europol's partners that contribute to its activities, in particular to its operational tasks, should have the opportunity to benefit from this unique feature and second their officers to Europol. Partners already having their officers seconded should be encouraged to develop their liaison bureaus further, involving various services that might benefit from and contribute to Europol's work. Secondment of counter-terrorism and cybercrime liaison officers should be particularly encouraged.

The development of the liaison officers' network should lead to better and more coordinated international police cooperation, bringing various states and regions closer together; the role of Europol in facilitating trans-Atlantic cooperation should be seen as an example in this regard.

Promoting **SIENA** and the **universal message format** will further contribute to secure and swift information exchange which, if necessary, might be combined with Europol's analytical capabilities.

**Europol's Platform for Experts** (EPE) should be promoted further in this context, as it offers a secure cooperation environment bringing together security experts. EPE should remain open to those partners with which Europol does not cooperate otherwise.

#### 3.3. **Reinforcing Europol's position within the EU security architecture** , in order to address external threats to the security of the EU

Europol is one of the key actors of the EU internal security architecture and an important part of a coherent European response to external security challenges like terrorism or migrant smuggling. Europol will strive to further develop its contribution to EU security, especially in the field of external relations.

Europol will further **strengthen cooperation with the European Commission and the European External Action Service** in order to ensure the proper exchange of strategic



information, to provide joint analysis of threats that have both an internal and external dimension and to facilitate contacts with third countries with which Europol doesn't cooperate yet.

Europol will further develop its cooperation with **EU operations and missions**, in particular those having executive functions and those operating in areas relevant for the internal security of the EU.

Europol will assess the potential of temporarily **deploying its staff outside of the EU, including to EU delegations, missions and operations**, which could contribute to gathering intelligence related to serious threats, such as migrant smuggling or terrorism.

Europol's role in **capacity building** in third countries will remain limited, focused on areas in which Europol has specific expertise and which are relevant for Europol's core business. Any capacity building activities should be carefully assessed and planned, with due consideration to available resources.

### 3.4. Promoting Europol's **successful cooperation model**

Regional entities that facilitate international police cooperation might benefit from Europol's successful cooperation model. Subject to available resources, Europol will promote and explain its functioning, its successful cooperation mechanisms and the lessons learned. The objective is to facilitate future cooperation between those regional entities and Europol.

## 4. Partners

The Europol Regulation gives Europol possibilities for effective and mutually beneficial cooperation with third countries and organisations. It gives Europol a global reach to serve the European law enforcement community.

When choosing cooperation partners, geographical criteria need to be combined with others, as for certain types of crime the geographical proximity of a cooperation partner is not the only criterion.

### 4.1. Third countries

As foreseen in the Regulation, agreements concluded before 1 May 2017 will remain the basis for future cooperation. Europol will strive to maintain and further develop the **already existing relationships** with all partners that are parties to agreements already in force.

The Europol Strategy states that Europol will aim to further strengthen its partnership with third states. The United States, Mediterranean countries and the Western Balkans are explicitly mentioned.

**The United States of America** will remain Europol's key partner. Mutual support and operational cooperation should be further reinforced, in particular through the increased exchange of information and active involvement in operational activities. Terrorism and cybercrime will remain main areas of common interest, notwithstanding continued cooperation in other fields, such as organised crime and migrant smuggling.

The migratory crisis and present terrorist threat call for closer cooperation between Europol and **Middle East and North African** countries. Each country of the region has its own specificities and a unique position in the security environment. In developing Europol's cooperation in this region, close cooperation with the European Union Action Service is of particular importance.

The **Western Balkans** will remain a region of particular relevance for Europol. Europol has been prioritising cooperation with the region for many years, which led to the conclusion of numerous operational agreements and successful strategic and operational cooperation. Further implementation of the agreements and full use of the already available mechanisms remain crucial. Migrant smuggling, organised crime and terrorism will remain key areas of common interest.

## Europol Unclassified – Basic Protection Level

Europol will continue supporting **regional initiatives in the Western Balkans**, as long as their activities supplement and enhance Europol's operational cooperation with the region.

The above mentioned areas will also require close cooperation with **Turkey**, the development of which depends on the general relations between the EU and Turkey.

Europol recognises the importance of cooperating with **Asian countries**, such as **India** and **Pakistan**, and will strive to strengthen cooperation with them.

Given the impact of Chinese organised crime on the EU and the high international profile of Chinese criminal groups, building cooperative relations with **China** will be of particular importance.

**South- and Central American states** will be important partners, in particular as regards drug-related crime. Furthermore, options available for cooperation under the Europol Regulation will be explored for the bilateral relations with **Israel** and **the Russian Federation**.

### 4.2. International organisations

**Interpol** will remain Europol's key partner. Respective capabilities and tools are complimentary and Europol remains **focused on supporting EU Members States** and ensuring **EU-wide** law enforcement cooperation. In view of the global challenges the EU is facing, cooperation with Interpol will remain particularly relevant and will be enhanced through closer alignment, increasing joint participation in operational activities and setting of common strategic activities.

Europol will make efforts to enhance its cooperation with **other international organisations** that play a role in the field of security, such as United Nations/ United Nations Office on Drugs and Crime (UN/UNODC), Organisation for Security and Co-operation in Europe (OSCE), World Customs Organisation (WCO) or North Atlantic Treaty Organization (NATO). Europol will strive to strengthen its cooperation in particular with the latter; counterterrorism and tackling migrant smuggling are detected to be the fields of common interest.

Europol is open for cooperation with **regional police cooperation organisations** such as Ameripol, Aseanapol and Afripol. Cooperation mechanisms should reflect operational needs as well as geographical and thematic priorities of Europol. Europol will strive to promote its successful cooperation model to foster regional cooperation.

## 5. Oversight mechanism – the role of the Management Board

The Management Board adopted guidelines on the implementation of the External Strategy in its meeting of 1 May 2017.

Information on the implementation of the External Strategy will be presented to the Management Board every six months. Moreover, Strategic Reviews concerning particular partners or regions will be submitted to the Management Board on a regular basis in order to present the on-going cooperation and seek guidance on further actions.

### 3. Human and financial resource outlook for the years 2019-2021

The Multi-annual Financial Framework (MFF) 2014-2020 of the EU had prescribed in 2013 a net reduction of Europol's resources for the years 2014-2020. In 2016, however, the political priorities of the EU made a necessary shift towards the establishment of a Security Union in order to address a number of pressing issues, particularly the increased migratory flows, the elevated terrorist threat, cybercrime or internet-facilitated crime and the fragmented EU information landscape.

Europol's role in the security landscape of the EU has been discussed with increasing intensity, with the Security Union being one of the latest examples. As a result, Europol was entrusted with a number of entirely new functions such as the European Cybercrime Centre, the European Migrant Smuggling Centre, the European Internet Referral Unit, the European Counter-Terrorism Centre and the FIU.net. Though some resources were provided to Europol to perform these new tasks, Europol has depended heavily on internal re-allocation of operational staff and on the shifting of posts from support functions to the Operations Department.

The discussion of Europol's role in the Security Union including on the latest topics such as innovation, interoperability<sup>1</sup> and decryption, calls for a continuous and comprehensive review of the agency's overall needs for human resources. In order to be able to perform the tasks assigned to it, Europol has to be reinforced with an appropriate level of staff.

Europol is an operational law enforcement agency, supporting the Member States by participating in their operations be it with expertise, analysis, on-the-spot deployments, cross-checking of data and operational meetings among other activities. Therefore, as criminal and terrorism threats are rising and EU cooperation becomes increasingly a vital success factor, the demand for Europol's services continues to grow and requires a corresponding increase in the agency's handling capacity.

Europol sees the necessity for further growth and development over the coming years (2019 – 2021). Factors which already have an impact or will have an impact during the following four years have to be taken into account. A small sample of the developments that most affect the security of EU citizens and for which Europol would require further development and resources are:

- Prevent or respond to terrorist attacks
- Take more terrorism propaganda offline
- Increase pressure on smuggling and trafficking networks, including via being present at migration hotspots in affected MS with Guest Officers
- Pioneer law enforcement information processing solutions of the next generation
- Increase capacity of centralised support for cyber forensics and decryption
- Increase the use of financial intelligence in investigations
- Develop a strong victim identification capability particularly to protect children from sexual abuse and exploitation

In its previous Programming Document Europol clearly defined its ambitions in a comprehensive plan for the years 2018-2020 in which an annual staff increase of approximately 70 Temporary Agent posts was foreseen. Eventually a more modest staff increase for 2018 was decided upon by the budgetary authority which amounted in a net staff increase of 26 Temporary Agent posts.

In the current Programming Document 2019-2021 Europol has based its planning on the modest approach taken by the budgetary authority for 2018 assuming that a bigger resource demand would not be met. The requested new posts would still allow for some increase in activities to enable continuation of Member States' support at an acceptable level, would boost to a certain extent the area of innovation and operational ICT and would also allow the agency to keep up with operational demand from Member States, for

---

<sup>1</sup> COM(2017) 794 final

## Europol Unclassified – Basic Protection Level

example to take into account a constant growth of support requests in the area of strategic and operational meetings that are organised for Member States.

From a high level perspective, for the next three years, Europol foresees the following Temporary Agent staff increases:

Area of the business	2019	2020	2021
Operations Directorate	+19	+19	+16
ICT Department	+20	+14	+12
Governance and Administration	+4	+4	+3
<b>Total</b>	<b>43</b>	<b>37</b>	<b>31</b>

It is important to stress the focus placed on augmentation of ICT resources. Information management capabilities are at the core of Europol's mandate and mission. In the last five years alone, Europol has been accepting at least 15% more contributions of operational data by MS each year, going from around 26,000 contributions in 2012 to more than 70,000 in 2017. During the same period the number of objects in the Europol Information System (EIS) has increased fivefold to containing more than 1 million objects in 2017. Member States have also intensified their usage of EIS – querying the system more than 2 million times in 2017- while more than 1,000 competent authorities are communicating through Europol's SIENA. Beyond the increased information exchange and number of users, technological solutions are continuously being developed and their services used to support the Member States, such as face recognition and victim identification solutions. Finally, Europol is committed to upgrading its information management and systems architecture and to introducing up-to-date, innovative capabilities to ensure that the information shared by Member States results in analysis products that provide the most accurate and comprehensive intelligence picture. This requires transformational as well as incremental change, and commensurate investments.

In past years, the budgetary process has resulted in Europol receiving additional resources specifically for its Operations Directorate, i.e. mainly analysts and specialists with crime analysis and investigation expertise. However, during the same period Europol's ICT capabilities did not see the investment that would be expected to keep up with the growth of demand for the organisation's products and technological developments in the field of information management. It is therefore imperative and long overdue to make a structural correction to the distribution of additional resources to the agency.

These staff increases, together with the necessary investments in the building and for operational and ICT initiatives, and the inclusion of funds to continue the secondary security checks at the hotspots via Europol's budget instead of via grants, lead to a necessary budget growth of € 21M in 2019 (total € 143.3M) compared to 2018. For future years there are smaller increases foreseen as in particular building related investments will be a lot less in 2020 (total € 146.1M) and 2021 (total €152.0M).

It needs to be taken into account that both the staff and budget figures in this Programming Document do not include the latest proposal from the Commission for a Regulation establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration). This proposal provides for a varying number of additional staff resources during the period 2019-2027 (5 extra TAs in 2019, varying numbers of CAs and TAs in the later years) and for varying additional budget amounts (overall almost € 49M over the period 2019-2027).

## HUMAN RESOURCES

### Temporary agents

Starting from the 2017 establishment plan of 550 posts the net number of posts increased by 26 and comes to 576 for 2018 (+ 4.7%). For 2019, 2020 and 2021 further increases are envisaged of 43, 37 and 31 additional Temporary Agent posts, respectively.

### **Contract Agents**

In response to business needs, the number of contract agents increased in 2017 to 165 full time equivalent (FTE) posts (153 heads at the end of 2017) which was possible as a consequence of budget availability. For 2018 the FTEs are envisaged to further increase to 212 also taking into consideration a switch from contractors (budgeted under Title 3) to Contract Agents (budgeted under Title 1) for certain ICT tasks (increase of 16 CA posts). From 2018 onwards the number of contract agents is expected to stabilise at 209.

### **Seconded National Experts**

The number of Seconded National Experts (SNEs) is foreseen to remain stable at 71. Considering the challenges that Member States have to make SNEs available and also taking into account the strong support by Member States for Guest Officer SNEs for deployments at hotspots, it is considered that going beyond the current levels is not feasible.

A breakdown of the areas of the business and what new posts will be specifically used for is provided in this section. For detailed data and numbers per staff category, see Annex III.

### **In Operations Directorate:**

#### **Horizontal Operational Services (incl. the 24/7 Operational Centre)**

The reinforcements for Horizontal Operational Services are foreseen for the 24/7 support, for the Financial Intelligence Group, for EMPACT and cross-cutting support, for analysis and training coordination and for additional analysis capacity. 2019 will be also a crucial year for the establishment of Europol's capabilities in the area of travel intelligence and the setting-up of the Europol Travel Intelligence Centre (ETIC).

#### **European Serious Organised Crime Centre (incl. EMSC)**

The posts for ESOCC are meant to reinforce the Weapons and Explosives clusters and the Drugs cluster in line with the ambition of the new Europol Drug Strategy. Specifically for the EMSC new posts will contribute to the delivery of the objectives of the Malta Implementation Plan and in particular to the strengthening of cooperation with the MENA countries, including the setting-up of a Clearing House and Regional Cooperation and Implementation Platforms. The provision of adequate support to MS in the framework of the EU Policy Cycle priorities and especially the new priorities will be also reinforced with additional resources.

#### **European Cyber Crime Centre (EC3)**

The posts for EC3 are focussing on digital forensics, big data analytics, black market sites (Dark Web and Open Web), cross-departmental encryption support, victim identification, child sexual exploitation, public-private cooperation, cyber bridge function towards global taskforces and further support towards the Joint Cybercrime Action Taskforce. In particular, Europol will aim at further developing and utilising its potential to perform as a European centre of expertise on decryption.

#### **European Counter Terrorism Centre (incl. EU/IRU)**

The posts for the ECTC will deal with Genocide and War Crimes, PNR, OSINT monitoring, IRU referrals and check the web, translations, analysis and R&D coordination. Specifically, the tasks arising for Europol from the EU Internet Forum Action Plan to Combat Terrorist Online Content will require the utilisation of additional resources.

### **In ICT Department:**

The posts are primarily envisaged for innovation profiles ranging from data-lake and cognitive computing operators, technical product managers, solution developers, smart capability testers to data enrichment scientists. In addition, software factory engagement managers and capacity for the implementation of IDMC and Business Product Management for the other operational systems are planned. New ICT posts remain crucial for delivering

on the mid-term ICT programmes (NEO for operational projects and nGage for optimisation and efficiency of corporate administration and support processes) established in 2017, which have been hit by a lack of new resources in both 2017 but particularly in 2018. As mentioned above, in addition to the requested posts, the posts envisioned in the Commission's proposal on interoperability, will be used to increase the performance of Europol's systems as to make them part of the interoperability landscape.

**In Governance and Administration:**

The posts will be used to ensure that the governance and administration capacity stays up to speed with the operations. Staff cuts from last years were for a large part taken by this area while at the same time the previous enlargements for EC3, the ECTC and the EMSC resulted in additional workload. Conversion of local staff into TAs and CAs is foreseen as well as the setting up of a new medical service.

**Rate of absorption of additional resources 2019-2021**

The sooner Europol is reinforced with the resources it needs to develop its current and future tasks, the bigger impact it can have by providing operational support to the MS. At the same time, Europol recognises that the resources required would be difficult to absorb in just one year and in all areas. The reinforcement of Europol should be done in a way in which there is flexibility to assign the posts within the organisation to best tackle the highest and most urgent priorities, while taking into account recruitment needs to replace existing posts (the turnover rate of Europol can be significant, given the policy of the Agency regarding restricted posts and the rotation principle).

As per best practice, the following principles on priority would continue to apply:

- Posts related to preparing the infrastructure of the organisation to handle the operational growth will be filled in first. These can include supporting posts needed for immediate handling of staff growth (e.g. recruitment, facilities) and ICT posts (e.g. implementing IDMC and interoperability changes, developing tools for operational support, responding to growing demand for support to operations i.e. more systems and more users).
- Operational posts:
  - Posts for vacancies (resignations, end of contract) where there is disruption of service;
  - Posts for new tasks at a rate that allows for swift absorption of staff;
  - Posts for growing tasks to allow for a balanced response to Member States demands.
- Other governance and administrative support posts will be filled at the rate dictated by the growth of the organisation.

**Staff cuts / redeployments**

The staff cuts for both the initial 5% and for the additional 5% for the re-deployment pool are implemented as planned. Out of a total of 45 posts to be reduced there were 36 posts cut at the end of 2017.

An important factor that was not taken into account in the requirement of staff cuts was that Europol, unlike other EU Institutions and Agencies, was already working on a 40hr week schedule, therefore not being able to recuperate some of the cuts by the increase in working time introduced in 2014 with the new Staff Regulation.

**Efficiency gains**

Europol continues to strive towards being a more operational agency. In 2017, the results of the job screening exercise show a small increase in the percentage of operational jobs and small decreases in the percentages for neutral and administrative/coordination jobs.

The job screening exercise was done for the fourth time in 2017, according to the guidelines defined by the EU Agencies Network and based on all people working at Europol's premises on 15 December 2017. This not only includes Temporary Agents,

## Europol Unclassified – Basic Protection Level

Contract Agents and SNEs but also Europol Liaison Officers, trainees and external service providers based at Europol's premises.

Compared to 2016, the Operational Jobs have increased by 1.6 points to 76%. On the other hand, the jobs dealing with administrative support and coordination have decreased by 1.3 points, to 19.6%. Neutral jobs have decreased by 0.3 points to 4.4%.

Job Type category	2016 Jobs	2016 (%)	2017 Jobs	2017 (%)	Δ 2017
<b>Administrative support and Coordination</b>	<b>227</b>	<b>21%</b>	<b>230</b>	<b>20%</b>	<b>-1.3%</b>
Administrative support	164	15%	166	14%	-1.0%
Coordination	63	6%	64	5%	-0.3%
<b>Operational</b>	<b>808</b>	<b>74%</b>	<b>891</b>	<b>76%</b>	<b>1.6%</b>
General Operational	591	54%	668	57%	2.5%
Programme Management	193	18%	200	17%	-0.7%
Top level Operational Coordination	24	2%	23	2%	-0.2%
<b>Neutral</b>	<b>50</b>	<b>5%</b>	<b>51</b>	<b>4%</b>	<b>-0.3%</b>
Finance	50	5%	51	4%	-0.3%
	<b>1085</b>		<b>1172</b>		

### Staff financed with ad hoc grants

For the year 2018 Europol will also have a number of Contract Agents and SNEs which are directly funded via ad hoc grants.

Grant from EUIPO: 6 SNEs and 2 Contract Agents

Grant from DG FPI: 5 Contract Agents

Still to be confirmed and clarified: Grant from DG Near for deployment of Liaison Officers in the Western Balkans

## FINANCIAL RESOURCES

### Revenue:

The total revenue for 2019 comes to € 143.3M. This amount includes the subsidy for the European School in The Hague (ESH) which has now been integrated under Item 9000 since the ESH has been completed with all schooling levels and the funding mechanism with the Commission is fully established.

Item	Heading	Revenue 2017	Revenue 2018	Draft Estimate 2019
9000	Regular subsidy from the Community	113,009,613	120,448,520	143,300,000
9001	Subsidy from Community for Type II School <sup>2</sup>	1,614,000	1,797,000	-
9010	Other subsidies and grants	-	P.M.	P.M.
9101	Denmark contribution <sup>3</sup>	-	P.M.	P.M.
9200	Other revenue	-	P.M.	P.M.
	<b>TITLE 1 – TOTAL</b>	<b>114,623,613</b>	<b>122,245,520</b>	<b>143,300,000</b>

<sup>2</sup> Since the school is fully established the subsidy will no longer be separately reflected in the budget

<sup>3</sup> It is envisaged that the budget will be amended later in the year with an additional contribution from Denmark via a separate procedure. Those funds will be handled as external assigned revenue (fund source R0).

## Europol Unclassified – Basic Protection Level

Item	Heading	Draft Budget outturn 2017	Budget 2018	Draft estimate 2019	2019/ 2018	% of the budget
1	Staff	71,864,946	79,421,520	87,045,000	110%	60.7%
2	Other Administrative Expenditure	9,782,622	12,805,100	17,418,200	136%	12.2%
3	Operational Activities	32,655,720	30,018,900	38,836,800	129%	27.1%
	<b>Total expenditure</b>	<b>114,303,288</b>	<b>122,245,520</b>	<b>143,300,000</b>	<b>117%</b>	<b>100.0%</b>

### **Title 1 – Staff expenditure:**

The estimated expenditure under Title 1 amounts to € 87M and represents 60.7% of the total budget. It reflects a 10% growth compared to 2018 which directly results from the requested growth in the number of Temporary Agents (+43) and the full year effect of the new 2018 posts (+26) in 2019.

The direct salary and allowances related budget (including recruitment expenditure and relocation allowances) for TAs and CAs (Chapter 11 – Staff in active employment) comes to € 79.7M. This is an increase of € 6.6M compared to the year 2018.

An increase of the budget (€ 1M compared to 2018) is also estimated for other staff related expenditure such as medical and PMO services, other external services (outsourced activities for removal and hospitality services, additional security officers and Audio-Visual (AV) support), interim services, training and the costs for the European school.

### **Title 2 – Other Administrative Expenditure:**

The estimated expenditure under Title 2 amounts to €17.4M. This is a 36% increase compared to the budget 2018 and this increase is largely a consequence of the necessary "one-off" activities related to the strategic housing roadmap and the upgrade of the AV systems in the meeting rooms.

The budget under Title 2 is planned for building related running costs, other facilities expenditure and investments concerning user elements of the building (€ 6.2M), for the continuation of the implementation of the strategic housing roadmap (€ 6.2M under this Title), for upgrade of AV systems which is a project that already started in 2017 (€ 484K), administrative ICT costs (€ 3M), other administrative governance expenditure (€ 829K) and for Statutory expenditure (e.g. Management Board and Internal Audit Capability amounting to € 732K).

Concerning the building, a significant part of the budget is foreseen for the implementation of the service level agreement with the Host State, including contractual maintenance to retain the current service environment and business continuity of the headquarters and involved infrastructure and for running costs (rent of the data recovery site, energy, cleaning, etc.), amounting to € 6.2M. In addition, an amount of € 6.7M is foreseen for "one-off" activities (Strategic Housing Roadmap (SHR) and AV upgrade).

For the SHR a range of activities and investments is included for both the existing headquarters and for the temporary satellite building that is needed to create swing-space to empty office floors during construction works at the headquarters. The main amounts budgeted are for construction costs for the user-elements and for the acquisition of furniture. In addition, costs for other external services such as removal and external security staff are taken into account as well as cleaning, catering and energy.

For administrative ICT the planned budget in 2019 amounts to € 3M. This is €600K higher than in 2018 when the budget allocated for administrative ICT was capped around the same as in 2017 due to budget limitations. A new initiative is the roll-out of Sysper II, the Commission's HR System. The budget for administrative ICT also includes continuation of IRIS (Intranet), FMIS (Facilities Management System), ABAC (the Commission's financial



## **Europol Unclassified – Basic Protection Level**

system) and E-Procurement initiatives. This also takes into account a necessary increase in telecom costs (for internet bandwidth).

An amount of € 0.8M is foreseen for other governance expenditure such as open source subscriptions, legal expenses, administrative expertise, security services, uniforms, etc.

The budget for the Management Board is estimated based on an expected increase in costs for interpretation and the hosting of two meetings in Member States. The total amount for MB activities comes to € 0.7M.

### **Title 3 – Operational activities:**

The estimated expenditure under Title 3 amounts to € 38.8M and represents 27% of the total budget (29% higher than in 2018). The budget under Title 3 is foreseen to cover for all Work Programme activities with a direct link to the core tasks. The following breakdown of activities under Title 3 is provided:

- A budget of € 11.3M for operations (including EMPACT) emphasises Europol's focus on operational activities and is foreseen to continue the high level of support to Member States. Overall a budget of € 4M is included for EMPACT activities of which 3.7M under Title 3. An amount of 2.7M is foreseen for EMPACT related grants for Member States.
- A budget of € 3.1M for the continuation of the guest officers' concept to provide secondary security checks at Hot Spots. This was included also in the original 2018 budget request from Europol but not provided by the Commission. In 2018 it will therefore need to be explored whether it can be funded by an amending budget otherwise Europol will face serious budgetary problems in 2018. During the years 2016 and 2017 this activity was funded via separate grants under ISF-Police EMAS (emergency assistance).
- A budget of € 20.4M is envisaged for operational information technology and telecommunications. This includes an increase of € 3.9M compared to 2018. This should allow for continuation of ongoing projects and for a minimum level of investments for innovation for which only very limited funds were available in 2018.
- The budget for Seconded National Experts amounting to € 4M covers the costs for 71 SNEs.
- The budget for high level external stakeholder meetings (HENUs and the annual Police Chiefs Convention) amounts to € 410K.

**Europol Unclassified – Basic Protection Level**

**Annex I: Resource allocation per Activity 2019-2021**

	Draft Budget 2019				Forecast 2020		Forecast 2021	
	Number of staff (TA,CA,SNE)	% of total staff	Budget allocation <sup>4</sup> €	% of total budget	Number of staff	Budget allocation €	Number of staff	Budget allocation €
A.1. Development of operational systems	159	18%	40,300,253	28%	173	41,844,300	185	43,952,743
A.2. Information Hub	68	8%	11,783,062	8%	69	11,783,349	70	12,031,183
A.3. Combating Serious Organised Crime	141	16%	19,228,984	13%	146	19,561,230	151	20,406,842
A.4. Combating Cyber Crime	95	11%	12,229,595	9%	101	12,677,504	105	13,454,279
A.5. Counter Terrorism	111	12%	12,716,798	9%	116	13,026,655	120	13,741,922
A.6. Provision of cross-cutting operational capabilities	76	8%	14,658,373	10%	78	14,871,147	80	15,279,858
A.7. Governance, support and administration	232	26%	29,543,176	21%	236	29,574,981	239	30,326,411
Independent functions: Data Protection Function Internal Audit Capability Management Board Accountancy Unit	17	2%	2,839,760	2%	17	2,792,834	17	2,820,762
<b>TOTAL</b>	<b>899</b>	<b>100%</b>	<b>143,300,000</b>	<b>100%</b>	<b>936</b>	<b>146,132,000</b>	<b>967</b>	<b>152,014,000</b>

<sup>4</sup> incl. salary.

**Annex II:****A. Human and Financial Resources 2019 – 2021****Table 1: Expenditure**

<b>Expenditure (Only C1 fund source)</b>	<b>Commitment / Payment appropriations</b>			
	<b>2018</b>	<b>2019</b>	<b>2020</b>	<b>2021</b>
Title 1 Staff Expenditure	79,421,520	87,045,000	93,115,000	98,468,000
Title 2 Other Administrative Expenditure	12,805,100	17,418,200	13,792,000	13,929,000
Title 3 Operational Activities	30,018,900	38,836,800	39,225,000	39,617,000
<b>Total expenditure</b>	<b>122,245,520</b>	<b>143,300,000</b>	<b>146,132,000</b>	<b>152,014,000</b>

**Table 2 – Revenue**

<b><u>REVENUES (only IC1)</u></b>	<b>Executed Budget 2017</b>	<b>Budget 2018</b>	<b>DB 2019 Agency request</b>	<b>DB 2019 Budget forecast</b>	<b>VAR 2019/ 2018</b>
<b>1 REVENUE FROM FEES AND CHARGES</b>		P.M.	P.M.		
<b>2. EU CONTRIBUTION</b>	<b>114,623,613</b>	<b>122,245,520</b>	<b>143,300,000</b>		<b>1.17</b>
Of which assigned revenues deriving from previous years' surpluses	2,669,000	1,868,000	1,158,000		
<b>3 THIRD COUNTRIES CONTRIBUTION (incl. EFTA and candidate countries)</b>	-	P.M.	P.M.		-
<b>4 OTHER CONTRIBUTIONS</b>	-	P.M.	P.M.		-
<b>5 ADMINISTRATIVE OPERATIONS</b>	-	P.M.	P.M.		-
Of which interest generated by funds paid by the Commission by way of the EU contribution (FFR Art. 58)	-	P.M.	P.M.		-
<b>6 REVENUES FROM SERVICES RENDERED AGAINST PAYMENT</b>	-	P.M.	P.M.		-
<b>7 CORRECTION OF BUDGETARY IMBALANCES</b>	-	P.M.	P.M.		-
<b>TOTAL REVENUES</b>	<b>114,623,613</b>	<b>122,245,520</b>	<b>143,300,000</b>		<b>1.17</b>

**Table 3 – Budget Outturn Cancellation of appropriations****Calculation Budget Outturn**

<b>BUDGET OUTTURN</b>	<b>2015</b>	<b>2016</b>	<b>2017</b>
Revenue actually received (+)	88,516,920	117,390,869	119,696,212
Payments made (-)	-74,639,953	-102,836,986	-110,402,762
Carry-over of appropriations (-)	-15,131,537	-18,977,641	-18,756,290
Cancellation of appropriations carried over (+)	3,563,930	1,612,811	834,972
Adjustment for carry-over of assigned revenue appropriations from previous year (+)	360,829	4,677,757	9,783,165
Exchange rate differences (+/-)	-1,318	1,439	3,595
<b>Total</b>	<b>2,668,872</b>	<b>1,868,249</b>	<b>1,158,893</b>

Budget Outturn

The overall draft budgetary outturn for the financial year 2017 comes to almost € 1.2M. This includes the following:

- An amount of € 320K of the 2017 budget was not committed and lapsed. The majority of the unused budget is within Operations (Chapter 30). This includes an amount of € 177K for EMPACT grants which remained unspent due to limited number of applications;
- An amount of € 835K of appropriations carried forward from 2016 to 2017 was not used;
- The exchange rate difference was € 3.6K (gain).

Cancellation of payment appropriations carried forward

The carry forward to 2017 came to a total of € 9.2M to cover existing commitments. The majority of this was carried forward from commitments taken under fund source C1 (€ 8.98M, representing 9% of the 2016 budget). An amount of € 219K was carried forward from the appropriations arising from internal assigned revenue (fund source C4 and C5).

The final implementation rate of the carry forward was 90.9% at the end of the year, which is 6.4% higher than in 2016. A total of € 835K was not used and is thus incorporated in the final budget outturn. Out of the € 835M not used:

- € 59K relates to Title 1, which is 10% of the carried forward under Title 1 (€ 590K);
- € 125K relates to Title 2, which is 3.4% of the carried forward under Title 2 (€ 3.66M);
- € 651K relates to Title 3, which is 13.2% of the carried forward under Title 3 (€ 4.95M).

Unused amounts related to:

- An amount of € 126K remained unspent for travel expenses after the final correction of the closure of the first grant for security checks at Hotspots;
- An amount of € 379K for various ICT consultancies and € 71K for other SW and HW related expenditure;
- An amount of € 57K for fixed telephone costs and € 22K for internet and mobile telecom costs;
- An amount of € 84K for various administrative and governance expenditure;
- An amount of € 60K for various operational expenditure; and
- An amount of € 35K for various facilities related expenditure.

## Europol Unclassified – Basic Protection Level

### Annex II:

#### B. Draft Estimate of Revenue and Expenditure 2019<sup>5</sup>

Draft Estimate of Revenue and Expenditure 2019

Draft Expenditure and revenue 2019	Budget Outturn 2017	Budget 2018	Draft Estimate 2019	VAR 2019/2018
<b>Title 1 Staff Expenditure</b>	<b>71,864,946</b>	<b>79,421,520</b>	<b>87,045,000</b>	<b>1.10</b>
11 Salaries & allowances	67,051,198	73,054,520	79,658,000	<b>1.09</b>
- of which establishment plan posts	57,399,939	62,130,520	68,009,000	<b>1.09</b>
- of which external personnel	9,651,260	10,924,000	11,649,000	<b>1.07</b>
13 Sociomedical infrastructure	934,138	1,003,000	1,313,000	<b>1.31</b>
14 Training	330,976	400,000	425,000	<b>1.06</b>
15 Other staff-related expenditure	3,468,959	4,881,000	5,550,000	<b>1.14</b>
16 Entertainment and representation expenses	79,674	83,000	99,000	<b>1.19</b>
<b>Title 2 Other administrative expenditure</b>	<b>9,782,622</b>	<b>12,805,100</b>	<b>17,418,200</b>	<b>1.36</b>
20 Rental of buildings and associated costs	5,716,491	8,456,000	11,290,000	<b>1.34</b>
21 Information and communication technology	1,697,421	1,776,000	2,226,000	<b>1.25</b>
22 Movable property and associated costs	734,914	919,000	1,855,000	<b>2.02</b>
23 Current administrative expenditure	337,512	384,100	484,200	<b>1.26</b>
24 Postal charges and telecommunications	633,567	680,000	831,000	<b>1.22</b>
25 Statutory expenditure	662,719	590,000	732,000	<b>1.24</b>
<b>Title 3 Operational activities</b>	<b>32,655,720</b>	<b>30,018,900</b>	<b>38,836,800</b>	<b>1.29</b>
30 Operations	8,472,018	9,667,900	14,409,800	<b>1.49</b>
31 Operational information technology	19,537,342	14,744,000	18,501,000	<b>1.25</b>
32 Telecommunication costs for operational activities	881,794	1,385,000	1,533,000	<b>1.11</b>
33 Seconded National Experts (Operational)	3,386,066	3,903,000	3,983,000	<b>1.02</b>
34 EPCC	268,500	229,000	300,000	<b>1.31</b>
35 Heads of Europol National Units	110,000	90,000	110,000	<b>1.22</b>
<b>TOTAL EXPENDITURE</b>	<b>114,303,288</b>	<b>122,245,520</b>	<b>143,300,000</b>	<b>1.17</b>

Quarterly estimate of cash payments and receipts:

Chapter	RECEIPTS	1 <sup>st</sup> Quarter	2 <sup>nd</sup> Quarter	3 <sup>rd</sup> Quarter	4 <sup>th</sup> Quarter	Total 2019
90	Regular subsidy from the Community	35,825,000	35,825,000	35,825,000	35,825,000	143,300,000
	<b>Total Receipts</b>	<b>35,825,000</b>	<b>35,825,000</b>	<b>35,825,000</b>	<b>35,825,000</b>	<b>143,300,000</b>

Title	PAYMENTS	1 <sup>st</sup> Quarter	2 <sup>nd</sup> Quarter	3 <sup>rd</sup> Quarter	4 <sup>th</sup> Quarter	Total 2019
1	Staff in active employment	21,543,638	21,543,638	21,543,638	21,543,638	86,174,550
2	Other administrative expenditure	2,830,458	2,830,458	2,830,458	2,830,458	11,321,830
3	Operational activities	7,767,360	7,767,360	7,767,360	7,767,360	31,069,440
	<b>Total Payments</b>	<b>32,141,455</b>	<b>32,141,455</b>	<b>32,141,455</b>	<b>32,141,455</b>	<b>128,565,820</b>

	1 <sup>st</sup> Quarter	2 <sup>nd</sup> Quarter	3 <sup>rd</sup> Quarter	4 <sup>th</sup> Quarter
Receipts - Payments	3,683,545	3,683,545	3,683,545	3,683,545
Cumulative	3,683,545	7,367,090	11,050,635	14,734,180

Draft Establishment Plan 2019 - The relevant information is to be found below in Annex III.

<sup>5</sup> Figures are rounded so the sum of the individual amounts may differ from the totals.

## Europol Unclassified – Basic Protection Level

### Annex III:

**Table 1 – Staff population and its evolution; Overview of all categories of staff**

Staff population [1]		Actually filled as of 31.12.2016 [2]	Authorised under EU Budget 2017 [3]	Actually filled as of 31.12.2017 [4]	Authorised under EU budget for year 2018 [5]	Draft Budget 2019	Envisaged in 2020 [6]	Envisaged in 2021 [7]
TA	AD	476	517	521	544	587	624	655
	AST	29	33	29	32	32	32	32
	AST /SC	0	0	0	0	0	0	0
<b>TOTAL TA [8]</b>		<b>505</b>	<b>550</b>	<b>550</b>	<b>576</b>	<b>619</b>	<b>656</b>	<b>687</b>
CA GF IV		30.41	43	34.66	55	55	55	55
CA GF III		70.02	82	86.06	113	110	110	110
CA GF II		32.50	40	32.50	44	44	44	44
CA GF I		0	0	0	0	0	0	0
<b>TOTAL CA [9]</b>		<b>132.93</b>	<b>165</b>	<b>153.22</b>	<b>212</b>	<b>209</b>	<b>209</b>	<b>209</b>
<b>SNE [10]</b>		<b>64.2</b>	<b>71</b>	<b>65.45</b>	<b>71</b>	<b>71</b>	<b>71</b>	<b>71</b>
<i>Structural service providers [11]</i>		31	50	41	50	50	50	50
<b>TOTAL</b>		<b>733.13</b>	<b>836</b>	<b>810</b>	<b>909</b>	<b>949</b>	<b>986</b>	<b>1017</b>
<i>External staff[12] for occasional replacement[13]</i>		9.33	10					

[1] This table provides all staff categories at Europol except trainees and Europol Liaison Officers. At the end of 2017 there were 32 trainees and around 220 Europol Liaison Officers

[2] The figures below include 42 TA posts (all in AD function group) that were not filled on 31.12.2016 but for which recruitment procedures were finalised and offer letters sent to selected candidates

[3] As authorised for officials and temporary agents (TA) and as estimated for contract agents (CA) and seconded national experts (SNE)

[4] The figures below include 15 TA posts (all in AD function group) that were not filled on 31.12.2017 but for which recruitment procedures were finalised and offer letters were sent to selected candidates

[5] As authorised for officials and temporary agents (TA) and as estimated for contract agents (CA) and seconded national experts (SNE)

[6] Tabular explanation of the effects on staff population is provided on the page below

[7] Ibid

[8] Headcounts

[9] FTE (annual averages)

[10] FTE (annual averages). The figure reported as of 31.12.2017 excludes FTE for SNE Guest Officers (30.78)

[11] FTE (annual averages)

[12] FTE (annual averages)

[13] Annual average FTE of CA's covering TA's on maternity leave, long-term sick leave and TA's working part-time. As these staff concern CAs the figure is from 2017 onwards fully integrated in the line for TOTAL CA.

**Europol Unclassified – Basic Protection Level**

**Annex III: Table 2 - Multi-annual staff policy plan 2019-2021**

Category and grade	Establishment plan in EU Budget 2017	Filled as of 31/12/2017	Modifications in year 2017 in application of flexibility rule [1]	Establishment plan in voted EU Budget 2018	Modifications in year 2018 in application of flexibility rule [2] [3]	Establishment plan in Draft EU Budget 2019	Establishment plan 2020	Establishment plan 2021
	TA only	TA only	TA only	TA only	TA only	TA only	TA only	TA only
AD 16								
AD 15	1	1	1	1	1	1	1	1
AD 14	1	1	1	1	1	1	2	2
AD 13	5	2	5	5	5	6	6	7
AD 12	11	6	11	11	11	12	13	14
AD 11	17	11	17	17	17	18	19	21
AD 10	30	10	30	28	28	31	35	38
AD 9	61	37	61	61	61	66	70	75
AD 8	97	75	97	100	90	94	99	104
AD 7	126	119	126	128	132	143	154	164
AD 6	139	247	139	158	177	196	208	214
AD 5	29	12	29	36	21	19	17	15
<b>Total AD</b>	<b>517</b>	<b>521</b>	<b>517</b>	<b>546</b>	<b>544</b>	<b>587</b>	<b>624</b>	<b>655</b>
AST 11	0	0	0	0	0	0	0	0
AST 10	0	0	0	0	0	0	0	0
AST 9	0	0	0	0	0	0	0	1
AST 8	2	0	2	3	3	4	5	4
AST 7	5	3	5	5	5	5	4	5
AST 6	6	4	6	6	6	6	7	7
AST 5	8	7	8	7	7	7	7	7
AST 4	8	10	8	5	8	7	6	5
AST 3	3	1	3	3	1	1	2	2
AST 2	1	4	1	1	2	2	1	1
AST 1	0	0	0	0	0	0	0	0
<b>Total AST</b>	<b>33</b>	<b>29</b>	<b>33</b>	<b>30</b>	<b>32</b>	<b>32</b>	<b>32</b>	<b>32</b>
AST/SC6	0	0	0	0	0	0	0	0
AST/SC5	0	0	0	0	0	0	0	0
AST/SC4	0	0	0	0	0	0	0	0
AST/SC3	0	0	0	0	0	0	0	0
AST/SC2	0	0	0	0	0	0	0	0
AST/SC1	0	0	0	0	0	0	0	0
<b>Total AST/SC</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>0</b>
<b>TOTAL</b>	<b>550</b>	<b>550</b>	<b>550</b>	<b>576</b>	<b>576</b>	<b>619</b>	<b>656</b>	<b>687</b>

[1] In line with Article 38(1) of the framework Financial Regulation, the management board may modify, under certain conditions, the establishment plan by in principle up to 10% TA only of posts authorised, unless the financial rules of the body concerned allows for a different % rate.

[2] Ibid

[3] Net modification and explanations for the modifications are provided on the page below

## Explanations on the modifications and changes in relation to the establishment plans from 2019 to 2021

*Modification to 2018 establishment plan using the flexibility contained with Article 38(1) of framework Financial Regulation.*

The modifications envisaged to the establishment plan 2018 can be summarised as follows:

Modification	Budgetary effect
4 AD8 downgraded to AD7	Savings
6 AD8 downgraded to AD6	Savings
13 AD5 converted to AD6	Increase
2 AD5 downgraded to AST4	Savings
1 AST3 converted to AST4	Increase
1 AST3 downgraded to AST2	Savings

In total the modifications involve 54 post movements which constitute around 9% of the total number of 576 established posts within the allowable 10% contained within Article 38 and expenditure impact of the total changes results in budget savings.

The staff turnover was 7.6% at the end of 2017 which is considerably lower than last year (14.2%). This difference can be partly explained by the number of staff for whom the second contract was ending in 2017 (fewer compared to 2016).

Replacement of staff occurs in many instances at entry level thus reducing the grade of many posts of long-serving staff. The modified establishment plan 2018 provides a more accurate reflection of the organisation in terms of actual grades allocated to staff and current and upcoming vacancies, taking into account the following factors:

- 38 staff members left Europol during 2017 with most of them being replaced or due to be replaced in lower grades;
- Similar profiles are replaced in entry grades, i.e. in most cases lower than those of leaving staff;
- In many cases when post profiles are reviewed and updated they are converted into lower level posts (e.g. Senior Specialist/Senior Analyst into Specialist/Analyst).

### *Reclassification adjustments in the Establishment plans for 2019, 2020 and 2021*

Europol implements reclassification on an annual basis. The establishment plans for 2018 to 2021 not only reflect the changes required in relation to new staff allocations but also changes to facilitate the reclassification process and potential changes to staff grades. At the end of the reclassification 2016 4% of staff (temporary agents) was reclassified. For future years depending on the grades the establishment plan foresees approximately 10% reclassification.



**From:** MB Secretariat <mbs@europol.europa.eu>  
**Sent:** 31 January 2018 16:54  
**To:** TAJANI Antonio, President  
**Cc:** CANGA FANO Diego; MB Secretariat  
**Subject:** @EXT: Europol's Programming Document 2018-2020; draft Programming Document 2019-2021; draft Multiannual Programming 2019-2021- EP  
**Attachments:** EDOC-#856927-v18-Europol\_Programming\_Document\_2018-2020.DOCX; EDOC-#945252-v1-Letter\_from\_the\_MB\_Chairperson\_transmitting\_Europol\_s\_Programming\_Document\_2018-2020\_to\_the\_JPSG.DOC; EDOC-#945349-v1-Letter\_from\_MB\_Chairperson\_consulting\_the\_JPSG\_on\_Europol\_s\_draft\_Multiannual\_Programming\_2019-2021.DOC; EDOC-#945538-v1-Letter\_from\_the\_MB\_Chairperson\_transmitting\_Europol\_s\_draft\_Programming\_Document\_2019-2021\_to\_the\_European\_Parliament.DOC; EDOC-#924131-v11A-Europol\_Programming\_Document\_2019-2021.PDF; EDOC-#945558-v2A-Europol\_Multi-Annual\_Programming\_2019-2021\_for\_consultation\_with\_JPSG.PDF

Dear colleagues,

On behalf of Mr Borja Barbosa, Secretary of the Management Board (MB) of Europol, please find attached the following documents:

Europol's Programming Document 2018-2020

- Letter from the MB Chairperson transmitting Europol's Programming Document 2018-2020 to the JPSG, MBS 020.2018
- Europol's Programming Document 2018-2020, #856927v18

Europol's draft Programming Document 2019-2021

- Letter from the MB Chairperson transmitting Europol's draft Programming Document 2019-2021 to the European Parliament, MBS 025.2018
- Europol's draft Programming Document 2019-2021, #924131v11

Europol's draft Multiannual Programming 2019-2021

- Letter from MB Chairperson consulting the JPSG on Europol's draft Multiannual Programming 2019-2021, MBS 022.2018

- Multi annual programming 2019-2021, #945558v2

Kind regards,

**Biljana Djukleska**

**EUROPOL** - Management Board Secretariat  
Eisenhowerlaan 73, 2517 KK  
The Hague, The Netherlands

Phone: +31 (0)70 353 1249  
E-mail: [Biljana.Djukleska@europol.europa.eu](mailto:Biljana.Djukleska@europol.europa.eu)  
[www.europol.europa.eu](http://www.europol.europa.eu)

\*\*\*\*\*

DISCLAIMER : This message is sent in confidence and is only intended for the named recipient. If you receive this message by mistake, you may not use, copy, distribute or forward this message, or any part of its contents or rely upon the information contained in it. Please notify the sender immediately by e-mail and delete the relevant e-mails from any computer. This message does not constitute a commitment by Europol unless otherwise indicated.

\*\*\*\*\*

## **Consultation on Europol's draft Multiannual Programming 2019-2021**

### **Input by the Cyprus delegation to the JPSG.**

Our general view is that the draft Multiannual Programming is a very coherent and well-structured document that describes clearly the Organisation's objectives in the period under review. We do, however, wish to bring up a few points.

-We consider corruption as a major enabler of a host of other criminal activities, as indicated also in the latest Threat Assessment. In spite of this, we notice it does not feature in the draft Multiannual Programming. How does Europol intend to deal with this issue in the period in question? Would the Management Board share the view that a reference should be included?

-Concerning the goal 1.3 to "Strategically enhance partnerships with cooperation partners", we are very skeptical with regard to the inclusion of Turkey in the Mediterranean countries with which an agreement for the exchange of personal data is considered as urgent and with which negotiations will be opened by the European Commission. The country has a particularly low record of data protection, further exacerbated under the current emergency status. Furthermore, the progress report on the Road Map for the liberalization of visas for Turkish citizens explicitly provides that "Turkey needs to revise its legislation and practices on terrorism in line with European standards, notably by better aligning the definition of terrorism in order to narrow the scope". In this light, the purpose of exchanging personal data regarding organized crime and terrorism before the amendment of the relevant legislation, brings into question the scope on which data exchanges between Europol and Turkey will occur.

Additionally, Turkey does not cooperate with Cyprus, inter alia, on issues of serious organized crime and counter-terrorism, compromising the overall efficiency of Europol's aims.

We also wonder how reliable an exchange of information on the part of the third party could be, particularly in the light of recent developments, which prove that radicalization efforts in EU Member States are actually directed by state structures of this country.

Under these circumstances, the upgrading and widening of Europol's conventional framework vis-à-vis this country, sends the wrong signal with regard to the real importance the EU in general, and Europol in particular, attach to the protection of the personal data of its citizens.

-While the role of the EU IRU to combat online radicalization is welcome, radicalization that occurs in mosques or other establishments should also perhaps form part of the wider counterterrorism strategy, particularly in cooperation with the Radicalisation Awareness Network.

25 June 2018

/EF



## Romanian Parliament

Bucharest, August 23<sup>rd</sup>, 2018

To the kind attention of Ms. Angela LUEGER and Mr. Claude MORAES,

Co-chairs of the Europol JPSG

Dear Colleagues,

The Chamber of Deputies and the Senate analyzed "Europol multiannual programming for 2019-2021" and decided to issue a joint document containing the contributions of both chambers of the Romanian Parliament.

After a thorough and in depth analysis, the Chamber of Deputies and the Senate, considers it a substantial document. However, we believe that some observations should be taken under consideration:

1. Europol should provide high quality operational support to Member States in three priority areas, in line with the European security agenda, namely organized crime, cybercrime and counter-terrorism;
2. In order to provide the most efficient operational support for illegal migration, Europol must re-enforce the capabilities of the EMSC (European Migrant Smuggling Center);
3. It is important to highlight the emphasis placed on the increase of ITC resources, having in view that information management capabilities are the main mission of Europol;
4. Particular attention should be paid to Europol's future budget in order to successfully complete the Agency's mandate, as well as seeing the impact of BREXIT on UK-Europol cooperation.

Please feel free to send this contribution to all the other national parliaments involved.

Yours faithfully,

On behalf of the Romanian delegation

Oana Consuela FLOREA

Member of the Romanian Chamber of Deputies

Head of the Romanian delegation on the Joint Parliamentary Scrutiny Group on  
Europol



parleu2018bg.bg

Parliamentary Dimension  
Bulgarian Presidency of the Council  
of the European Union

**Mr. Claude Moraes**

Co-Chair of the JPSG

Chairman of the Committee on Civil Liberties, Justice and Home Affairs

European Parliament

B-1047 Brussels

30 May 2018

**Dear Mr. Moraes,**

Dear Claude,

Herewith, I would like to inform you on the proceedings of the 107<sup>th</sup> Meeting of the Europol Management Board from 4 May 2018 in Sofia, Bulgaria that I attended in my capacity as Co-Chair of the JPSG during the agenda item, specifically devoted to hearing the JPSG input for the Europol Management Board. In my intervention, on behalf of the JPSG Co-Chairs, I raised the following issues presented here below.

I informed the Management Board of the adoption of the Rules of procedure by consensus at the Second Meeting of the JPSG on 18-19 March in Sofia, Bulgaria and the efforts that entailed this result.

I also presented to the Board our common desire as Co-Chairs that the provisions for JPSG participation in Management Board meetings (Recital 20 and Article 14(4) of Regulation (EU) 2016/794) be interpreted as broadly as possible. Drawing attention to Article 5 of the consensually adopted JPSG Rules of Procedure that regulate the framework for permanent JPSG representation at Management Board meetings, I highlighted that we expect on the one hand that the invitation will be extended in respect to all future Management Board meetings, on the other – that the JPSG representative will be invited to stay for other relevant agenda items, apart for the one specifically devoted to relations of the Management Board with the JPSG. In this respect, I also highlighted that the attendance of the JPSG representative at Management Board meetings should reflect the scope of Article 51 of the Europol Regulation in terms of content, of course with no prejudice to requirements of confidentiality.

In the same line of argument, I explained that the JPSG has still not selected its representative to the Management Board and that we



suggest to continue with the current practice of addressing future invitations to the Co-Chairs until such a representative is officially determined.

The issue of providing the Multiannual Programming document at least in both English and French was also mentioned in my intervention, with a view to the EU principle of linguistic diversity, the fact that both English and French are working languages for the JPSG, and in abidance with Article 12 of the Europol Regulation that stipulates that the Management Board should hold consultations with the JPSG on the multiannual programming document. The idea that the Management Board should propose a joint work calendar for the consultation process was also among the highlights in my presentation.

The situation created in respect to the confidentiality of some documents for the Second Meeting of the JPSG was also raised and I called for the Management Board Secretariat to establish a joint agreement with the JPSG Secretariat in this respect.

Last but not least, I noted that the JPSG meetings present a valuable opportunity to hold thematic discussions on a number of politically salient issues related to the work of Europol, including its external strategy and third partners. Thus, it gives the possibility for further guidance and feedback on the strategic orientation of the Agency. In the case of the Sofia JPSG meeting such a panel was the one on the Western Balkans.

I deem it important that in her intervention following my presentation, Europol Executive Director Ms. Catherine de Bolle noted that the Regulation has given parliamentarians a big role and this is a positive development for enhancing the transparency and legitimacy of the Agency through political monitoring and oversight. She also noted that for her it is a priority that Europol is in good contact with elected representatives and made the commitment that Europol will remain in full engagement with the JPSG.

Management Board Chairman Mr. Parkna, in turn, noted that this is the first time the Management Board hears the JPSG views about cooperation with the Management Board and that he welcomes my open and constructive intervention.



parleu2018bg.bg

Parliamentary Dimension  
Bulgarian Presidency of the Council  
of the European Union

In respect to the access to documents by the JPSG, the need to safeguard confidentiality was noted. It was highlighted that the JPSG should have understanding for the fact that some of the documents that the Management Board discusses are not to be made publicly available in order to safeguard the confidentiality of operations and sensitive information.

On JPSG representation to the Management Board, Mr. Parkna noted that Article 14 of the Regulation gives the Management Board considerable latitude, in particular when it comes to observers at its meetings. He underlined that it is necessary for the Management Board to decide together and called on national representatives to discuss the details with their respective national services and parliamentarians, starting this process immediately, so at the next Management Board meeting an informed debate on the matter can be held. The Management Board is to finalize its position at the October meeting and convey it to the JPSG Co-Chairs by letter.

In conclusion to my participation, I noted that parliamentary scrutiny should not be perceived as a potential impediment but as a contribution to the effectiveness of Europol. The meeting ended on the positive note that the relationship between the JPSG and the Management Board should be made constructive and fruitful so both bodies can fulfill their duties and at the same time facilitate the work of the Agency.

Kindest Regards,

**Tsvetan TSVETANOV**

Head of the Bulgarian Delegation to the JPSG  
Chairman of the Committee on Internal Security and Public Order  
National Assembly of Bulgaria

**CC: Mr. Raivo Aeg**



**REGULATION (EU) 2016/794 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL  
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**

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 88 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Acting in accordance with the ordinary legislative procedure <sup>(1)</sup>,

Whereas:

- (1) Europol was set up by Council Decision 2009/371/JHA <sup>(2)</sup> as an entity of the Union funded from the general budget of the Union to support and strengthen action by competent authorities of the Member States and their mutual cooperation in preventing and combating organised crime, terrorism and other forms of serious crime affecting two or more Member States. Decision 2009/371/JHA replaced the Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention) <sup>(3)</sup>.
- (2) Article 88 of the Treaty on the Functioning of the European Union (TFEU) provides for Europol to be governed by a regulation to be adopted in accordance with the ordinary legislative procedure. It also requires the establishment of procedures for the scrutiny of Europol's activities by the European Parliament, together with national parliaments, subject to point (c) of Article 12 of the Treaty on European Union (TEU) and Article 9 of Protocol No 1 on the role of National Parliaments in the European Union, annexed to the TEU and to the TFEU (Protocol No 1), in order to enhance the democratic legitimacy and accountability of Europol to the Union's citizens. Therefore, Decision 2009/371/JHA should be replaced by a regulation laying down, inter alia, rules on parliamentary scrutiny.
- (3) The 'Stockholm programme — An open and secure Europe serving and protecting citizens' <sup>(4)</sup> calls for Europol to evolve and become a hub for information exchange between the law enforcement authorities of the Member States, a service provider and a platform for law enforcement services. On the basis of an assessment of Europol's functioning, further enhancement of its operational effectiveness is needed to meet that objective.
- (4) Large-scale criminal and terrorist networks pose a significant threat to the internal security of the Union and to the safety and livelihood of its citizens. Available threat assessments show that criminal groups are becoming increasingly poly-criminal and cross-border in their activities. National law enforcement authorities therefore need to cooperate more closely with their counterparts in other Member States. In this context, it is necessary to equip Europol to better support Member States in Union-wide crime prevention, analyses and investigations. This was also confirmed in the evaluation of Decision 2009/371/JHA.

<sup>(1)</sup> Position of the European Parliament of 25 February 2014 (not yet published in the Official Journal) and position of the Council at first reading of 10 March 2016 (not yet published in the Official Journal). Position of the European Parliament of 11 May 2016 (not yet published in the Official Journal).

<sup>(2)</sup> Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol) (OJ L 121, 15.5.2009, p. 37).

<sup>(3)</sup> OJ C 316, 27.11.1995, p. 1.

<sup>(4)</sup> OJ C 115, 4.5.2010, p. 1.



- (5) This Regulation aims to amend and expand the provisions of Decision 2009/371/JHA and of Council Decisions 2009/934/JHA <sup>(1)</sup>, 2009/935/JHA <sup>(2)</sup>, 2009/936/JHA <sup>(3)</sup> and 2009/968/JHA <sup>(4)</sup> implementing Decision 2009/371/JHA. Since the amendments to be made are of a substantial number and nature, those Decisions should, in the interests of clarity, be replaced in their entirety in relation to the Member States bound by this Regulation. Europol as established by this Regulation should replace and assume the functions of Europol as established by Decision 2009/371/JHA, which, as a consequence, should be repealed.
- (6) As serious crime often occurs across internal borders, Europol should support and strengthen Member States' actions and their cooperation in preventing and combating serious crime affecting two or more Member States. Given that terrorism is one of the most significant threats to the security of the Union, Europol should assist Member States in facing common challenges in this regard. As the Union law enforcement agency, Europol should also support and strengthen actions and cooperation in tackling forms of crime that affect the interests of the Union. Among the forms of crime with which Europol is competent to deal, organised crime will continue to fall within the scope of Europol's main objectives, as, given its scale, significance and consequences, it also calls for a common approach by the Member States. Europol should also offer support in preventing and combating related criminal offences which are committed in order to procure the means of perpetrating acts in respect of which Europol is competent or to facilitate or perpetrate such acts or to ensure the impunity of committing them.
- (7) Europol should provide strategic analyses and threat assessments to assist the Council and the Commission in laying down strategic and operational priorities of the Union for fighting crime and in the operational implementation of those priorities. Where the Commission so requests in accordance with Article 8 of Council Regulation (EU) No 1053/2013 <sup>(5)</sup>, Europol should also carry out risk analyses, including in respect of organised crime, insofar as the risks concerned may undermine the application of the Schengen *acquis* by the Member States. Moreover, at the request of the Council or the Commission where appropriate, Europol should provide strategic analyses and threat assessments to contribute to the evaluation of states that are candidates for accession to the Union.
- (8) Attacks against information systems affecting Union bodies or two or more Member States are a growing menace in the Union, in particular in view of their speed and impact and the difficulty in identifying their sources. When considering requests by Europol to initiate an investigation into a serious attack of suspected criminal origin against information systems affecting Union bodies or two or more Member States, Member States should respond to Europol without delay, taking into account the fact that the rapidity of the response is a key factor in successfully tackling computer crime.
- (9) Given the importance of the inter-agency cooperation, Europol and Eurojust should ensure that necessary arrangements are established to optimise their operational cooperation, taking due account of their respective missions and mandates and of the interests of Member States. In particular, Europol and Eurojust should keep each other informed of any activity involving the financing of joint investigation teams.
- (10) When a joint investigation team is set up, the relevant agreement should determine the conditions relating to the participation of the Europol staff in the team. Europol should keep a record of its participation in such joint investigation teams targeting criminal activities falling within the scope of its objectives.
- (11) Europol should be able to request Member States to initiate, conduct or coordinate criminal investigations in specific cases where cross-border cooperation would add value. Europol should inform Eurojust of such requests.

<sup>(1)</sup> Council Decision 2009/934/JHA of 30 November 2009 adopting the implementing rules governing Europol's relations with partners, including the exchange of personal data and classified information (OJ L 325, 11.12.2009, p. 6).

<sup>(2)</sup> Council Decision 2009/935/JHA of 30 November 2009 determining the list of third States and organisations with which Europol shall conclude agreements (OJ L 325, 11.12.2009, p. 12).

<sup>(3)</sup> Council Decision 2009/936/JHA of 30 November 2009 adopting the implementing rules for Europol analysis work files (OJ L 325, 11.12.2009, p. 14).

<sup>(4)</sup> Council Decision 2009/968/JHA of 30 November 2009 adopting the rules on the confidentiality of Europol information (OJ L 332, 17.12.2009, p. 17).

<sup>(5)</sup> Council Regulation (EU) No 1053/2013 of 7 October 2013 establishing an evaluation and monitoring mechanism to verify the application of the Schengen *acquis* and repealing the Decision of the Executive Committee of 16 September 1998 setting up a Standing Committee on the evaluation and implementation of Schengen (OJ L 295, 6.11.2013, p. 27).

- (12) Europol should be a hub for information exchange in the Union. Information collected, stored, processed, analysed and exchanged by Europol includes criminal intelligence which relates to information about crime or criminal activities falling within the scope of Europol's objectives, obtained with a view to establishing whether concrete criminal acts have been committed or may be committed in the future.
- (13) In order to ensure Europol's effectiveness as a hub for information exchange, clear obligations should be laid down requiring Member States to provide Europol with the data necessary for it to fulfil its objectives. While implementing such obligations, Member States should pay particular attention to providing data relevant to the fight against crimes considered to be strategic and operational priorities within relevant policy instruments of the Union, in particular the priorities set by the Council in the framework of the EU Policy Cycle for organised and serious international crime. Member States should also endeavour to provide Europol with a copy of bilateral and multilateral exchanges of information with other Member States on crime falling within Europol's objectives. When supplying Europol with the necessary information, Member States should also include information about any alleged cyber attacks affecting Union bodies located in their territory. At the same time, Europol should increase the level of its support to Member States, so as to enhance mutual cooperation and the sharing of information. Europol should submit an annual report to the European Parliament, to the Council, to the Commission and to national parliaments on the information provided by the individual Member States.
- (14) To ensure effective cooperation between Europol and Member States, a national unit should be set up in each Member State (the 'national unit'). The national unit should be the liaison link between national competent authorities and Europol, thereby having a coordinating role in respect of Member States' cooperation with Europol, and thus helping to ensure that each Member State responds to Europol requests in a uniform way. To ensure a continuous and effective exchange of information between Europol and the national units, and to facilitate their cooperation, each national unit should designate at least one liaison officer to be attached to Europol.
- (15) Taking into account the decentralised structure of some Member States and the need to ensure rapid exchanges of information, Europol should be allowed to cooperate directly with competent authorities in Member States, subject to the conditions defined by Member States, while keeping the national units informed at the latter's request.
- (16) The establishment of joint investigation teams should be encouraged and Europol staff should be able to participate in them. To ensure that such participation is possible in every Member State, Council Regulation (Euratom, ECSC, EEC) No 549/69 <sup>(1)</sup> provides that Europol staff do not benefit from immunities while they are participating in joint investigation teams.
- (17) It is also necessary to improve the governance of Europol, by seeking efficiency gains and streamlining procedures.
- (18) The Commission and the Member States should be represented on the Management Board of Europol (the 'Management Board') to effectively supervise its work. The members and the alternate members of the Management Board should be appointed taking into account their relevant managerial, administrative and budgetary skills and knowledge of law enforcement cooperation. Alternate members should act as members in the absence of the member.
- (19) All parties represented on the Management Board should make efforts to limit the turnover of their representatives, with a view to ensuring the continuity of the Management Board's work. All parties should aim to achieve a balanced representation between men and women on the Management Board.
- (20) The Management Board should be able to invite non-voting observers whose opinion may be relevant for the discussion, including a representative designated by the Joint Parliamentary Scrutiny Group (JPSG).

<sup>(1)</sup> Regulation (Euratom, ECSC, EEC) No 549/69 of the Council of 25 March 1969 determining the categories of officials and other servants of the European Communities to whom the provisions of Article 12, the second paragraph of Article 13 and Article 14 of the Protocol on the Privileges and Immunities of the Communities apply (OJ L 74, 27.3.1969, p. 1).

- (21) The Management Board should be given the necessary powers, in particular to set the budget, verify its execution, and adopt the appropriate financial rules and planning documents, as well as adopt rules for the prevention and management of conflicts of interest in respect of its members, establish transparent working procedures for decision-making by the Executive Director of Europol, and adopt the annual activity report. It should exercise the powers of appointing authority vis-à-vis staff of the agency, including the Executive Director.
- (22) To ensure the efficient day-to-day functioning of Europol, the Executive Director should be its legal representative and manager, acting independently in the performance of his or her duties and ensuring that Europol carries out the tasks provided for by this Regulation. In particular, the Executive Director should be responsible for preparing budgetary and planning documents submitted for the decision of the Management Board and for implementing the multiannual programming and annual work programmes of Europol and other planning documents.
- (23) For the purposes of preventing and combating crime falling within the scope of its objectives, it is necessary for Europol to have the fullest and most up-to-date information possible. Therefore, Europol should be able to process data provided to it by Member States, Union bodies, third countries, international organisations and, under stringent conditions laid down by this Regulation, private parties, as well as data coming from publicly available sources, in order to develop an understanding of criminal phenomena and trends, to gather information about criminal networks, and to detect links between different criminal offences.
- (24) To improve Europol's effectiveness in providing accurate crime analyses to the competent authorities of the Member States, it should use new technologies to process data. Europol should be able to swiftly detect links between investigations and common *modi operandi* across different criminal groups, to check cross-matches of data and to have a clear overview of trends, while guaranteeing a high level of protection of personal data for individuals. Therefore, Europol databases should be structured in such a way as to allow Europol to choose the most efficient IT structure. Europol should also be able to act as a service provider, in particular by providing a secure network for the exchange of data, such as the secure information exchange network application (SIENA), aimed at facilitating the exchange of information between Member States, Europol, other Union bodies, third countries and international organisations. In order to ensure a high level of data protection, the purpose of processing operations and access rights as well as specific additional safeguards should be laid down. In particular, the principles of necessity and proportionality should be observed with regard to the processing of personal data.
- (25) Europol should ensure that all personal data processed for operational analyses are allocated a specific purpose. Nonetheless, in order for Europol to fulfil its mission, it should be allowed to process all personal data received to identify links between multiple crime areas and investigations, and should not be limited to identifying connections only within one crime area.
- (26) To respect the ownership of data and the protection of personal data, Member States, Union bodies, third countries and international organisations should be able to determine the purpose or purposes for which Europol may process the data they provide and to restrict access rights. Purpose limitation is a fundamental principle of personal data processing; in particular, it contributes to transparency, legal certainty and predictability and is particularly of high importance in the area of law enforcement cooperation, where data subjects are usually unaware when their personal data are being collected and processed and where the use of personal data may have a very significant impact on the lives and freedoms of individuals.
- (27) To ensure that data are accessed only by those needing access in order to perform their tasks, this Regulation should lay down detailed rules on different degrees of right of access to data processed by Europol. Such rules should be without prejudice to restrictions on access imposed by data providers, as the principle of ownership of data should be respected. In order to increase efficiency in the prevention and combating of crimes falling within the scope of Europol's objectives, Europol should notify Member States of information which concerns them.
- (28) To enhance operational cooperation between the agencies, and particularly to establish links between data already in the possession of the different agencies, Europol should enable Eurojust and the European Anti-Fraud Office (OLAF) to have access, on the basis of a hit/no hit system, to data available at Europol. Europol and Eurojust should be able to conclude a working arrangement ensuring, in a reciprocal manner within their respective mandates, access to, and the possibility of searching, all information that has been provided for the purpose of

cross-checking in accordance with specific safeguards and data protection guarantees provided for in this Regulation. Any access to data available at Europol should, by technical means, be limited to information falling within the respective mandates of those Union bodies.

- (29) Europol should maintain cooperative relations with other Union bodies, authorities of third countries, international organisations and private parties, to the extent required for the accomplishment of its tasks.
- (30) To ensure operational effectiveness, Europol should be able to exchange all relevant information, with the exception of personal data, with other Union bodies, authorities of third countries and international organisations, to the extent necessary for the performance of its tasks. Since companies, firms, business associations, non-governmental organisations and other private parties hold expertise and information of direct relevance to the prevention and combating of serious crime and terrorism, Europol should also be able to exchange such information with private parties. To prevent and combat cybercrime, as related to network and information security incidents, Europol should, pursuant to the applicable legislative act of the Union laying down measures to ensure a high common level of network and information security across the Union, cooperate and exchange information, with the exception of personal data, with national authorities competent for the security of network and information systems.
- (31) Europol should be able to exchange relevant personal data with other Union bodies to the extent necessary for the accomplishment of its or their tasks.
- (32) Serious crime and terrorism often have links beyond the territory of the Union. Europol should therefore be able to exchange personal data with authorities of third countries and with international organisations such as the International Criminal Police Organisation — Interpol to the extent necessary for the accomplishment of its tasks.
- (33) All Member States are affiliated to Interpol. To fulfil its mission, Interpol receives, stores and circulates data to assist competent law enforcement authorities to prevent and combat international crime. Therefore, it is appropriate to strengthen cooperation between Europol and Interpol by promoting an efficient exchange of personal data whilst ensuring respect for fundamental rights and freedoms regarding the automatic processing of personal data. When personal data is transferred from Europol to Interpol, this Regulation, in particular the provisions on international transfers, should apply.
- (34) To guarantee purpose limitation, it is important to ensure that personal data can be transferred by Europol to Union bodies, third countries and international organisations only if necessary for preventing and combating crime that falls within Europol's objectives. To this end, it is necessary to ensure that, when personal data are transferred, the recipient gives an undertaking that the data will be used by the recipient or transferred onward to a competent authority of a third country solely for the purpose for which they were originally transferred. Further onward transfer of the data should take place in compliance with this Regulation.
- (35) Europol should be able to transfer personal data to an authority of a third country or an international organisation on the basis of a Commission decision finding that the country or international organisation in question ensures an adequate level of data protection ('adequacy decision'), or, in the absence of an adequacy decision, an international agreement concluded by the Union pursuant to Article 218 TFEU, or a cooperation agreement allowing for the exchange of personal data concluded between Europol and the third country prior to the entry into force of this Regulation. In light of Article 9 of Protocol No 36 on transitional provisions, annexed to the TEU and to the TFEU, the legal effects of such agreements are to be preserved until those agreements are repealed, annulled or amended in the implementation of the Treaties. Where appropriate and in accordance with Regulation (EC) No 45/2001 of the European Parliament and of the Council <sup>(1)</sup>, the Commission should be able to consult the European Data Protection Supervisor (EDPS) before and during the negotiation of an international agreement. Where the Management Board identifies an operational need for cooperation with a third country or

<sup>(1)</sup> Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

an international organisation, it should be able to suggest to the Council that the latter draw the attention of the Commission to the need for an adequacy decision or for a recommendation for the opening of negotiations on an international agreement as referred to above.

- (36) Where a transfer of personal data cannot be based on an adequacy decision, an international agreement concluded by the Union or an existing cooperation agreement, the Management Board, in agreement with the EDPS, should be allowed to authorise a set of transfers, where specific conditions so require and provided that adequate safeguards are ensured. The Executive Director should be allowed to authorise the transfer of data in exceptional cases on a case-by-case basis, where such transfer is required, under specific strict conditions.
- (37) Europol should be able to process personal data originating from private parties and private persons only if those data are transferred to Europol by one of the following: a national unit in accordance with its national law; a contact point in a third country or an international organisation with which there is established cooperation through a cooperation agreement allowing for the exchange of personal data concluded in accordance with Article 23 of Decision 2009/371/JHA prior to the entry into force of this Regulation; an authority of a third country or an international organisation which is subject to an adequacy decision or with which the Union has concluded an international agreement pursuant to Article 218 TFEU. However, in cases where Europol receives personal data directly from private parties and the national unit, contact point or authority concerned cannot be identified, Europol should be able to process those personal data solely for the purpose of identifying those entities, and such data should be deleted unless those entities resubmit those personal data within four months after the transfer takes place. Europol should ensure by technical means that, during that period, such data would not be accessible for processing for any other purpose.
- (38) Taking into account the exceptional and specific threat posed to the internal security of the Union by terrorism and other forms of serious crime, especially when facilitated, promoted or committed using the internet, the activities that Europol should undertake on the basis of this Regulation, stemming from its implementation of the Council Conclusions of 12 March 2015 and the call by the European Council of 23 April 2015 in relation especially to those priority areas, in particular the corresponding practice of direct exchanges of personal data with private parties, should be evaluated by the Commission by 1 May 2019.
- (39) Any information which has clearly been obtained in obvious violation of human rights should not be processed.
- (40) Data protection rules at Europol should be strengthened and should draw on the principles underpinning Regulation (EC) No 45/2001 to ensure a high level of protection of individuals with regard to the processing of personal data. As Declaration No 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, attached to the TEU and the TFEU, recognises the specificity of personal data processing in the law enforcement context, the data protection rules of Europol should be autonomous while at the same time consistent with other relevant data protection instruments applicable in the area of police cooperation in the Union. Those instruments include, in particular, Directive (EU) 2016/680 of the European Parliament and of the Council<sup>(1)</sup>, as well as the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe and its Recommendation No R(87) 15<sup>(2)</sup>.
- (41) Any processing of personal data by Europol should be lawful and fair in relation to the data subjects concerned. The principle of fair processing requires transparency of processing allowing data subjects concerned to exercise their rights under this Regulation. It should be possible nevertheless to refuse or restrict access to their personal data if, with due regard to the interests of the data subjects concerned, such refusal or restriction constitutes a necessary measure to enable Europol to fulfil its tasks properly, to protect security and public order or to prevent crime, to guarantee that a national investigation will not be jeopardised or to protect the rights and freedoms of third parties. To enhance transparency, Europol should make publicly available a document setting out in an intelligible form the applicable provisions regarding the processing of personal data and the means available to data subjects to exercise their rights. Europol should also publish on its website a list of adequacy decisions,

<sup>(1)</sup> Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89).

<sup>(2)</sup> Council of Europe Committee of Ministers Recommendation No R(87) 15 to the Member States on regulating the use of personal data in the police sector, 17.9.1987.

agreements and administrative arrangements relating to the transfer of personal data to third countries and international organisations. Moreover, in order to increase Europol's transparency vis-à-vis Union citizens and its accountability, Europol should publish on its website a list of its Management Board members and, where appropriate, the summaries of the outcome of the meetings of the Management Board, while respecting data protection requirements.

- (42) As far as possible, personal data should be distinguished according to their degree of accuracy and reliability. Facts should be distinguished from personal assessments, in order to ensure both the protection of individuals and the quality and reliability of the information processed by Europol. In the case of information obtained from publicly available sources, particularly sources on the internet, Europol should as far as possible assess the accuracy of such information and the reliability of its source with particular diligence in order to address the risks associated with the internet as regards the protection of personal data and privacy.
- (43) Personal data relating to different categories of data subjects are processed in the area of law enforcement cooperation. Europol should make distinctions between personal data in respect of different categories of data subjects as clear as possible. Personal data concerning persons such as victims, witnesses and persons possessing relevant information, as well as personal data concerning minors, should in particular be protected. Europol should only process sensitive data if those data supplement other personal data already processed by Europol.
- (44) In the light of the fundamental right to the protection of personal data, Europol should not store personal data for longer than is necessary for the performance of its tasks. The need for continued storage of such data should be reviewed no later than three years after the start of its initial processing.
- (45) To guarantee the security of personal data, Europol and Member States should implement necessary technical and organisational measures.
- (46) Any data subject should have a right of access to personal data concerning him or her, a right to rectification if those data are inaccurate, and a right to erasure or restriction if those data are no longer required. The costs related to exercising the right of access to personal data should not represent a barrier to effectively exercising that right. The rights of the data subject and the exercise thereof should not affect the obligations incumbent upon Europol and should be subject to the restrictions laid down in this Regulation.
- (47) The protection of the rights and freedoms of data subjects requires a clear attribution of the responsibilities under this Regulation. In particular, Member States should be responsible for the accuracy of data, for keeping up to date the data they have transferred to Europol and for the legality of such data transfers. Europol should be responsible for the accuracy of data and for keeping up to date the data provided by other data suppliers or resulting from Europol's own analyses. Europol should ensure that data are processed fairly and lawfully, and are collected and processed for a specific purpose. Europol should also ensure that the data are adequate, relevant, not excessive in relation to the purpose for which they are processed, stored no longer than is necessary for that purpose, and processed in a manner that ensures appropriate security of personal data and confidentiality of data processing.
- (48) Europol should keep records of collection, alteration, access, disclosure, combination or erasure of personal data for the purposes of verifying the lawfulness of the data processing, self-monitoring and ensuring proper data integrity and security. Europol should be obliged to co-operate with the EDPS and to make logs or documentation available upon request, so that they can be used for monitoring processing operations.
- (49) Europol should designate a Data Protection Officer to assist it in monitoring compliance with this Regulation. The Data Protection Officer should be in a position to perform his or her duties and tasks independently and effectively, and should be provided with the necessary resources to do so.

- (50) Independent, transparent, accountable and effective structures for supervision are essential for the protection of individuals with regard to the processing of personal data as required by Article 8(3) of the Charter of Fundamental Rights of the European Union. National authorities competent for the supervision of the processing of personal data should monitor the lawfulness of personal data provided by Member States to Europol. The EDPS should monitor the lawfulness of data processing carried out by Europol, exercising his or her functions with complete independence. In this regard, the prior consultation mechanism is an important safeguard for new types of processing operations. This should not apply to specific individual operational activities, such as operational analysis projects, but to the use of new IT systems for the processing of personal data and any substantial changes thereto.
- (51) It is important to ensure strengthened and effective supervision of Europol and to guarantee that the EDPS can make use of appropriate law enforcement data protection expertise when he or she assumes responsibility for data protection supervision of Europol. The EDPS and national supervisory authorities should closely cooperate with each other on specific issues requiring national involvement and should ensure the consistent application of this Regulation throughout the Union.
- (52) In order to facilitate the cooperation between the EDPS and the national supervisory authorities, but without prejudice to the independence of the EDPS and his or her responsibility for data protection supervision of Europol, they should regularly meet within the Cooperation Board, which, as an advisory body, should deliver opinions, guidelines, recommendations and best practices on various issues requiring national involvement.
- (53) As Europol also processes non-operational personal data, unrelated to criminal investigations, such as personal data concerning staff of Europol, service providers or visitors, the processing of such data should be subject to Regulation (EC) No 45/2001.
- (54) The EDPS should hear and investigate complaints lodged by data subjects. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The national supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period.
- (55) Any individual should have the right to a judicial remedy against a decision of the EDPS concerning him or her.
- (56) Europol should be subject to the general rules on contractual and non-contractual liability applicable to Union institutions, agencies and bodies, save as regards the rules on liability for unlawful data processing.
- (57) It may be unclear for the individual concerned whether damage suffered as a result of unlawful data processing is a consequence of action by Europol or by a Member State. Europol and the Member State in which the event that gave rise to the damage occurred should therefore be jointly and severally liable.
- (58) While respecting the role of the European Parliament together with national parliaments in the scrutiny of Europol's activities, it is necessary that Europol be a fully accountable and transparent internal organisation. To that end, in light of Article 88 TFEU, procedures should be established for the scrutiny of Europol's activities by the European Parliament together with national parliaments. Such procedures should be subject to point (c) of Article 12 TEU and to Article 9 of Protocol No 1, providing that the European Parliament and national parliaments are together to determine the organisation and promotion of effective and regular interparliamentary cooperation within the Union. The procedures to be established for the scrutiny of Europol's activities should take due account of the need to ensure that the European Parliament and the national parliaments stand on an equal footing, as well as the need to safeguard the confidentiality of operational information. However, the way in which national parliaments scrutinise their governments in relation to the activities of the Union is a matter for the particular constitutional organisation and practice of each Member State.
- (59) The Staff Regulations of Officials of the European Union (the 'Staff Regulations') and the Conditions of Employment of Other Servants of the European Union (the 'Conditions of Employment of Other Servants') laid down in Council Regulation (EEC, Euratom, ECSC) No 259/68 <sup>(1)</sup> should apply to Europol staff. Europol should

<sup>(1)</sup> OJ L 56, 4.3.1968, p. 1.

be able to employ staff from the competent authorities of the Member States as temporary agents whose period of service should be limited in order to maintain the principle of rotation, as the subsequent reintegration of such staff members into the service of their competent authority facilitates close cooperation between Europol and the competent authorities of the Member States. Member States should take any measure necessary to ensure that staff engaged at Europol as temporary agents may, at the end of their term of service at Europol, return to the national civil service to which they belong.

- (60) Given the nature of the duties of Europol and the role of the Executive Director, the competent committee of the European Parliament should be able to invite the Executive Director to appear before it prior to his or her appointment, as well as prior to any extension of his or her term of office. The Executive Director should also present the annual report to the European Parliament and to the Council. Furthermore, the European Parliament and the Council should be able to invite the Executive Director to report on the performance of his or her duties.
- (61) To guarantee the full autonomy and independence of Europol, it should be granted an autonomous budget, with revenue coming essentially from a contribution from the general budget of the Union. The Union budgetary procedure should be applicable as far as the Union contribution and any other subsidies chargeable to the general budget of the Union are concerned. The auditing of accounts should be undertaken by the Court of Auditors.
- (62) Commission Delegated Regulation (EU) No 1271/2013 <sup>(1)</sup> should apply to Europol.
- (63) Given their specific legal and administrative powers and their technical competences in conducting cross-border information-exchange activities, operations and investigations, including in joint investigation teams, and in providing facilities for training, the competent authorities of the Member States should be able to receive grants from Europol without a call for proposals in accordance with point (d) of Article 190(1) of Commission Delegated Regulation (EU) No 1268/2012 <sup>(2)</sup>.
- (64) Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council <sup>(3)</sup> should apply to Europol.
- (65) Europol processes data that require particular protection as they include sensitive non-classified and EU classified information. Europol should therefore draw up rules on the confidentiality and processing of such information. The rules on the protection of EU classified information should be consistent with Council Decision 2013/488/EU <sup>(4)</sup>.
- (66) It is appropriate to evaluate the application of this Regulation regularly.
- (67) The necessary provisions regarding accommodation for Europol in The Hague, where it has its headquarters, and the specific rules applicable to all Europol's staff and members of their families should be laid down in a headquarters agreement. Furthermore, the host Member State should provide the necessary conditions for the smooth operation of Europol, including multilingual, European-oriented schooling and appropriate transport connections, so as to attract high-quality human resources from as wide a geographical area as possible.
- (68) Europol as established by this Regulation replaces and succeeds Europol as established by Decision 2009/371/JHA. It should therefore be the legal successor of all its contracts, including employment contracts, liabilities and properties acquired. International agreements concluded by Europol as established by Decision 2009/371/JHA and agreements concluded by Europol as established by the Europol Convention before 1 January 2010 should remain in force.

<sup>(1)</sup> Commission Delegated Regulation (EU) No 1271/2013 of 30 September 2013 on the framework financial regulation for the bodies referred to in Article 208 of Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council (OJ L 328, 7.12.2013, p. 42).

<sup>(2)</sup> Commission Delegated Regulation (EU) No 1268/2012 of 29 October 2012 on the rules of application of Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council on the financial rules applicable to the general budget of the Union (OJ L 362, 31.12.2012, p. 1).

<sup>(3)</sup> Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999 (OJ L 248, 18.9.2013, p. 1).

<sup>(4)</sup> Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information (OJ L 274, 15.10.2013, p. 1).



- (69) To enable Europol to continue to fulfil the tasks of Europol as established by Decision 2009/371/JHA to the best of its abilities, transitional measures should be laid down, in particular with regard to the Management Board, the Executive Director and staff employed under a contract of indefinite duration as a local staff member concluded by Europol as established by the Europol Convention, who should be offered the possibility of employment as a member of the temporary or contract staff under the Conditions of Employment of Other Servants.
- (70) The Council Act of 3 December 1998 <sup>(1)</sup> on Europol staff regulations has been repealed by Article 63 of Decision 2009/371/JHA. However, it should continue to apply to staff employed by Europol before the entry into force of Decision 2009/371/JHA. Therefore, transitional provisions should provide that contracts concluded in accordance with those staff regulations are to remain governed by them.
- (71) Since the objective of this Regulation, namely the establishment of an entity responsible for law enforcement cooperation at Union level, cannot be sufficiently achieved by the Member States but can rather, by reason of the scale and effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 TEU. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve that objective.
- (72) In accordance with Article 3 and Article 4a(1) of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the TEU and to the TFEU, Ireland has notified its wish to take part in the adoption and application of this Regulation.
- (73) In accordance with Articles 1 and 2 and Article 4a(1) of Protocol No 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice, annexed to the TEU and the TFEU, and without prejudice to Article 4 of that Protocol, the United Kingdom is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.
- (74) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the TEU and to the TFEU, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application.
- (75) The EDPS has been consulted and issued an opinion on 31 May 2013.
- (76) This Regulation respects the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union, in particular the right to the protection of personal data and the right to privacy as protected by Articles 8 and 7 of the Charter, as well as by Article 16 TFEU,

HAVE ADOPTED THIS REGULATION:

#### CHAPTER I

### GENERAL PROVISIONS, OBJECTIVES AND TASKS OF EUROPOL

#### *Article 1*

#### **Establishment of the European Union Agency for Law Enforcement Cooperation**

1. A European Union Agency for Law Enforcement Cooperation (Europol) is hereby established with a view to supporting cooperation among law enforcement authorities in the Union.
2. Europol as established by this Regulation shall replace and succeed Europol as established by Decision 2009/371/JHA.

<sup>(1)</sup> Council Act of 3 December 1998 laying down the staff regulations applicable to Europol employees (OJ C 26, 30.1.1999, p. 23).

*Article 2***Definitions**

For the purposes of this Regulation:

- (a) 'the competent authorities of the Member States' means all police authorities and other law enforcement services existing in the Member States which are responsible under national law for preventing and combating criminal offences. The competent authorities shall also comprise other public authorities existing in the Member States which are responsible under national law for preventing and combating criminal offences in respect of which Europol is competent;
- (b) 'strategic analysis' means all methods and techniques by which information is collected, stored, processed and assessed with the aim of supporting and developing a criminal policy that contributes to the efficient and effective prevention of, and the fight against, crime;
- (c) 'operational analysis' means all methods and techniques by which information is collected, stored, processed and assessed with the aim of supporting criminal investigations;
- (d) 'Union bodies' means institutions, bodies, missions, offices and agencies set up by, or on the basis of, the TEU and the TFEU;
- (e) 'international organisation' means an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;
- (f) 'private parties' means entities and bodies established under the law of a Member State or third country, in particular companies and firms, business associations, non-profit organisations and other legal persons that are not covered by point (e);
- (g) 'private persons' means all natural persons;
- (h) 'personal data' means any information relating to a data subject;
- (i) 'data subject' means an identified or identifiable natural person, an identifiable person being a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;
- (j) 'genetic data' means all personal data relating to the genetic characteristics of an individual that have been inherited or acquired, which give unique information about the physiology or the health of that individual, resulting in particular from an analysis of a biological sample from the individual in question;
- (k) 'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- (l) 'recipient' means a natural or legal person, public authority, agency or any other body to which data are disclosed, whether a third party or not;
- (m) 'transfer of personal data' means the communication of personal data, actively made available, between a limited number of identified parties, with the knowledge or intention of the sender to give the recipient access to the personal data;
- (n) 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

- (o) 'the data subject's consent' means any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to him or her being processed;
- (p) 'administrative personal data' means all personal data processed by Europol apart from those that are processed to meet the objectives laid down in Article 3.

### *Article 3*

## **Objectives**

1. Europol shall support and strengthen action by the competent authorities of the Member States and their mutual cooperation in preventing and combating serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy, as listed in Annex I.
2. In addition to paragraph 1, Europol's objectives shall also cover related criminal offences. The following shall be considered to be related criminal offences:
  - (a) criminal offences committed in order to procure the means of perpetrating acts in respect of which Europol is competent;
  - (b) criminal offences committed in order to facilitate or perpetrate acts in respect of which Europol is competent;
  - (c) criminal offences committed in order to ensure the impunity of those committing acts in respect of which Europol is competent.

### *Article 4*

## **Tasks**

1. Europol shall perform the following tasks in order to achieve the objectives set out in Article 3:
  - (a) collect, store, process, analyse and exchange information, including criminal intelligence;
  - (b) notify the Member States, via the national units established or designated pursuant to Article 7(2), without delay of any information and connections between criminal offences concerning them;
  - (c) coordinate, organise and implement investigative and operational actions to support and strengthen actions by the competent authorities of the Member States, that are carried out:
    - (i) jointly with the competent authorities of the Member States; or
    - (ii) in the context of joint investigation teams in accordance with Article 5 and, where appropriate, in liaison with Eurojust;
  - (d) participate in joint investigation teams, as well as propose that they be set up in accordance with Article 5;
  - (e) provide information and analytical support to Member States in connection with major international events;
  - (f) prepare threat assessments, strategic and operational analyses and general situation reports;

- (g) develop, share and promote specialist knowledge of crime prevention methods, investigative procedures and technical and forensic methods, and provide advice to Member States;
  - (h) support Member States' cross-border information exchange activities, operations and investigations, as well as joint investigation teams, including by providing operational, technical and financial support;
  - (i) provide specialised training and assist Member States in organising training, including with the provision of financial support, within the scope of its objectives and in accordance with the staffing and budgetary resources at its disposal in coordination with the European Union Agency for Law Enforcement Training (CEPOL);
  - (j) cooperate with the Union bodies established on the basis of Title V of the TFEU and with OLAF, in particular through exchanges of information and by providing them with analytical support in the areas that fall within their competence;
  - (k) provide information and support to EU crisis management structures and missions established on the basis of the TEU, within the scope of Europol's objectives as set out in Article 3;
  - (l) develop Union centres of specialised expertise for combating certain types of crime falling within the scope of Europol's objectives, in particular the European Cybercrime Centre;
  - (m) support Member States' actions in preventing and combating forms of crime listed in Annex I which are facilitated, promoted or committed using the internet, including, in cooperation with Member States, the making of referrals of internet content, by which such forms of crime are facilitated, promoted or committed, to the online service providers concerned for their voluntary consideration of the compatibility of the referred internet content with their own terms and conditions.
2. Europol shall provide strategic analyses and threat assessments to assist the Council and the Commission in laying down strategic and operational priorities of the Union for fighting crime. Europol shall also assist in the operational implementation of those priorities.
3. Europol shall provide strategic analyses and threat assessments to assist the efficient and effective use of the resources available at national and Union level for operational activities and the support of those activities.
4. Europol shall act as the Central Office for combating euro counterfeiting in accordance with Council Decision 2005/511/JHA <sup>(1)</sup>. Europol shall also encourage the coordination of measures carried out to fight euro counterfeiting by the competent authorities of the Member States or in the context of joint investigation teams, where appropriate in liaison with Union bodies and the authorities of third countries.
5. Europol shall not apply coercive measures in carrying out its tasks.

## CHAPTER II

### COOPERATION BETWEEN MEMBER STATES AND EUROPOL

#### *Article 5*

#### **Participation in joint investigation teams**

1. Europol staff may participate in the activities of joint investigation teams dealing with crime falling within Europol's objectives. The agreement setting up a joint investigation team shall determine the conditions relating to the participation of the Europol staff in the team, and shall include information on the rules on liability.

<sup>(1)</sup> Council Decision 2005/511/JHA of 12 July 2005 on protecting the euro against counterfeiting, by designating Europol as the Central Office for combating euro counterfeiting (OJ L 185, 16.7.2005, p. 35).

2. Europol staff may, within the limits of the laws of the Member States in which a joint investigation team is operating, assist in all activities and exchanges of information with all members of the joint investigation team.
3. Europol staff participating in a joint investigation team may, in accordance with this Regulation, provide all members of the team with necessary information processed by Europol for the purposes set out in Article 18(2). Europol shall at the same time inform the national units of the Member States represented in the team, as well as those of the Member States which provided the information.
4. Information obtained by Europol staff while part of the joint investigation team may, with the consent and under the responsibility of the Member State which provided the information, be processed by Europol for the purposes set out in Article 18(2), under the conditions laid down in this Regulation.
5. Where Europol has reason to believe that setting up a joint investigation team would add value to an investigation, it may propose this to the Member States concerned and take measures to assist them in setting up the joint investigation team.

#### *Article 6*

#### **Request by Europol for the initiation of a criminal investigation**

1. In specific cases where Europol considers that a criminal investigation should be initiated into a crime falling within the scope of its objectives, it shall request the competent authorities of the Member States concerned via the national units to initiate, conduct or coordinate such a criminal investigation.
2. The national units shall inform Europol without delay of the decision of the competent authorities of the Member States concerning any request made pursuant to paragraph 1.
3. If the competent authorities of a Member State decide not to accede to a request made by Europol pursuant to paragraph 1, they shall inform Europol of the reasons for their decision without undue delay, preferably within one month of receipt of the request. However, the reasons may be withheld if providing them would:
  - (a) be contrary to the essential interests of the security of the Member State concerned; or
  - (b) jeopardise the success of an ongoing investigation or the safety of an individual.
4. Europol shall immediately inform Eurojust of any request made pursuant to paragraph 1 and of any decision of a competent authority of a Member State pursuant to paragraph 2.

#### *Article 7*

#### **Europol national units**

1. The Member States and Europol shall cooperate with each other in the fulfilment of their respective tasks set out in this Regulation.
2. Each Member State shall establish or designate a national unit, which shall be the liaison body between Europol and the competent authorities of that Member State. Each Member State shall appoint an official as the head of its national unit.

3. Each Member State shall ensure that its national unit is competent under national law to fulfil the tasks assigned to national units in this Regulation, and in particular that it has access to national law enforcement data and other relevant data necessary for cooperation with Europol.

4. Each Member State shall determine the organisation and the staff of its national unit in accordance with its national law.

5. In accordance with paragraph 2, the national unit shall be the liaison body between Europol and the competent authorities of the Member States. However, subject to conditions determined by the Member States, including prior involvement of the national unit, the Member States may allow direct contacts between their competent authorities and Europol. The national unit shall at the same time receive from Europol any information exchanged in the course of direct contacts between Europol and the competent authorities, unless the national unit indicates that it does not need to receive such information.

6. Each Member State shall, via its national unit or, subject to paragraph 5, a competent authority, in particular:

- (a) supply Europol with the information necessary for it to fulfil its objectives, including information relating to forms of crime the prevention or combating of which is considered a priority by the Union;
- (b) ensure effective communication and cooperation of all relevant competent authorities with Europol;
- (c) raise awareness of Europol's activities;
- (d) in accordance with point (a) of Article 38(5), ensure compliance with national law when supplying information to Europol.

7. Without prejudice to the discharge by Member States of their responsibilities with regard to the maintenance of law and order and the safeguarding of internal security, Member States shall not in any particular case be obliged to supply information in accordance with point (a) of paragraph 6 that would:

- (a) be contrary to the essential interests of the security of the Member State concerned;
- (b) jeopardise the success of an ongoing investigation or the safety of an individual; or
- (c) disclose information relating to organisations or specific intelligence activities in the field of national security.

However, Member States shall supply information as soon as it ceases to fall within the scope of points (a), (b) or (c) of the first subparagraph.

8. Member States shall ensure that their financial intelligence units established pursuant to Directive 2005/60/EC of the European Parliament and of the Council <sup>(1)</sup> are allowed to cooperate with Europol via their national unit regarding analyses, within the limits of their mandate and competence.

9. The heads of the national units shall meet on a regular basis, in particular to discuss and resolve problems that occur in the context of their operational cooperation with Europol.

10. The costs incurred by national units in communications with Europol shall be borne by the Member States and, with the exception of the costs of connection, shall not be charged to Europol.

11. Europol shall draw up an annual report on the information provided by each Member State pursuant to point (a) of paragraph 6 on the basis of the quantitative and qualitative evaluation criteria defined by the Management Board. The annual report shall be sent to the European Parliament, the Council, the Commission and national parliaments.

---

<sup>(1)</sup> Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (OJ L 309, 25.11.2005, p. 15).

*Article 8***Liaison officers**

1. Each national unit shall designate at least one liaison officer to be attached to Europol. Except as otherwise laid down in this Regulation, the liaison officers shall be subject to the national law of the designating Member State.
2. Liaison officers shall constitute the national liaison bureaux at Europol and shall be instructed by their national units to represent the interests of the latter within Europol in accordance with the national law of the designating Member State and the provisions applicable to the administration of Europol.
3. Liaison officers shall assist in the exchange of information between Europol and their Member States.
4. Liaison officers shall, in accordance with their national law, assist in the exchange of information between their Member States and the liaison officers of other Member States, third countries and international organisations. Europol's infrastructure may be used, in accordance with national law, for such bilateral exchanges also to cover crimes falling outside the scope of the objectives of Europol. All such exchanges of information shall be in accordance with applicable Union and national law.
5. The Management Board shall determine the rights and obligations of liaison officers in relation to Europol. Liaison officers shall enjoy the privileges and immunities necessary for the performance of their tasks in accordance with Article 63(2).
6. Europol shall ensure that liaison officers are fully informed of and associated with all of its activities, in so far as necessary for the performance of their tasks.
7. Europol shall cover the costs of providing Member States with the necessary premises within the Europol building and adequate support for liaison officers to perform their duties. All other costs that arise in connection with the designation of liaison officers shall be borne by the designating Member State, including the costs of equipment for liaison officers, unless the European Parliament and the Council decide otherwise on the recommendation of the Management Board.

## CHAPTER III

**ORGANISATION OF EUROPOL***Article 9***Administrative and management structure of Europol**

The administrative and management structure of Europol shall comprise:

- (a) a Management Board;
- (b) an Executive Director;
- (c) where appropriate, other advisory bodies established by the Management Board in accordance with point (s) of Article 11(1).

## SECTION 1

**Management Board***Article 10***Composition of the Management Board**

1. The Management Board shall be composed of one representative from each Member State and one representative of the Commission. Each representative shall have a voting right.
2. The members of the Management Board shall be appointed taking into account their knowledge of law enforcement cooperation.
3. Each member of the Management Board shall have an alternate member who shall be appointed taking into account the criterion set out in paragraph 2. The alternate member shall represent the member in his or her absence.

The principle of a balanced gender representation on the Management Board shall also be taken into account.

4. Without prejudice to the right of the Member States and of the Commission to terminate the mandate of their respective member and alternate member, the membership of the Management Board shall be for a period of four years. That term shall be extendable.

*Article 11***Functions of the Management Board**

1. The Management Board shall:
  - (a) adopt each year, by a majority of two-thirds of its members and in accordance with Article 12, a document containing Europol's multiannual programming and its annual work programme for the following year;
  - (b) adopt, by a majority of two-thirds of its members, the annual budget of Europol and exercise other functions in respect of Europol's budget pursuant to Chapter X;
  - (c) adopt a consolidated annual activity report on Europol's activities and, by 1 July of the following year, send it to the European Parliament, the Council, the Commission, the Court of Auditors and the national parliaments. The consolidated annual activity report shall be made public;
  - (d) adopt the financial rules applicable to Europol in accordance with Article 61;
  - (e) adopt an internal anti-fraud strategy, proportionate to fraud risks, taking into account the costs and benefits of the measures to be implemented;
  - (f) adopt rules for the prevention and management of conflicts of interest in respect of its members, including in relation to their declaration of interests;
  - (g) in accordance with paragraph 2, exercise, with respect to the staff of Europol, the powers conferred by the Staff Regulations on the appointing authority and by the Conditions of Employment of Other Servants on the authority empowered to conclude a contract of employment of other servants ('the appointing authority powers');
  - (h) adopt appropriate implementing rules giving effect to the Staff Regulations and the Conditions of Employment of Other Servants in accordance with Article 110 of the Staff Regulations;



- (i) adopt internal rules regarding the procedure for the selection of the Executive Director, including rules on the composition of the selection committee which ensure its independence and impartiality;
- (j) propose to the Council a shortlist of candidates for the posts of Executive Director and Deputy Executive Directors and, where relevant, propose to the Council that their terms of office be extended or that they be removed from office in accordance with Articles 54 and 55;
- (k) establish performance indicators and oversee the Executive Director's performance, including the implementation of Management Board decisions;
- (l) appoint a Data Protection Officer, who shall be functionally independent in the performance of his or her duties;
- (m) appoint an accounting officer, who shall be subject to the Staff Regulations and the Conditions of Employment of Other Servants and functionally independent in the performance of his or her duties;
- (n) establish, where appropriate, an internal audit capability;
- (o) ensure adequate follow-up to findings and recommendations stemming from the internal or external audit reports and evaluations, as well as from investigations of OLAF and the EDPS;
- (p) define the evaluation criteria for the annual report in accordance with Article 7(11);
- (q) adopt guidelines further specifying the procedures for the processing of information by Europol in accordance with Article 18, after consulting the EDPS;
- (r) decide upon the conclusion of working and administrative arrangements in accordance with Article 23(4) and Article 25(1), respectively;
- (s) decide, taking into consideration both business and financial requirements, upon the establishment of Europol's internal structures, including Union centres of specialised expertise as referred to in point (l) of Article 4(1), upon a proposal of the Executive Director;
- (t) adopt its rules of procedure, including provisions concerning the tasks and the functioning of its secretariat;
- (u) adopt, where appropriate, other internal rules.

2. If the Management Board considers it necessary for the performance of Europol's tasks, it may suggest to the Council that it draw the attention of the Commission to the need for an adequacy decision as referred to in point (a) of Article 25(1) or for a recommendation for a decision authorising the opening of negotiations with a view to the conclusion of an international agreement as referred to in point (b) of Article 25(1).

3. The Management Board shall, in accordance with Article 110 of the Staff Regulations, adopt a decision based on Article 2(1) of the Staff Regulations and on Article 6 of the Conditions of Employment of Other Servants delegating the relevant appointing authority powers to the Executive Director and establishing the conditions under which such delegation of powers may be suspended. The Executive Director shall be authorised to subdelegate those powers.

Where exceptional circumstances so require, the Management Board may, by way of a decision, temporarily suspend the delegation of the appointing authority powers to the Executive Director and any subdelegation of such powers and exercise them itself or delegate those powers to one of its members or to a staff member other than the Executive Director.

## Article 12

### **Multiannual programming and annual work programmes**

1. The Management Board shall, by 30 November each year, adopt a document containing Europol's multiannual programming and annual work programme, based on a draft put forward by the Executive Director, taking into account the opinion of the Commission and, as regards the multiannual programming, after having consulted the JPSG. The Management Board shall forward that document to the Council, the Commission and the JPSG.

2. The multiannual programming shall set out the overall strategic programming, including the objectives, expected results and performance indicators. It shall also set out the resource planning, including the multiannual budget and staff. It shall include the strategy for relations with third countries and international organisations.

The multiannual programming shall be implemented by means of annual work programmes and shall, where appropriate, be updated following the outcome of external and internal evaluations. The conclusion of those evaluations shall also be reflected, where appropriate, in the annual work programme for the following year.

3. The annual work programme shall comprise detailed objectives, expected results and performance indicators. It shall also contain a description of the actions to be financed and an indication of the financial and human resources allocated to each action, in accordance with the principles of activity-based budgeting and management. The annual work programme shall be consistent with the multiannual programming. It shall clearly indicate tasks that have been added, changed or deleted compared to the previous financial year.

4. Where, after adoption of an annual work programme, a new task is assigned to Europol, the Management Board shall amend the annual work programme.

5. Any substantial amendment to the annual work programme shall be adopted by the same procedure as that applicable to the adoption of the initial annual work programme. The Management Board may delegate to the Executive Director the power to make non-substantial amendments to the annual work programme.

#### *Article 13*

### **Chairperson and Deputy Chairperson of the Management Board**

1. The Management Board shall elect a Chairperson and a Deputy Chairperson from within the group of three Member States that have jointly prepared the Council's 18-month programme. They shall serve for the 18-month period corresponding to that Council programme. If, however, the Chairperson's or the Deputy Chairperson's membership of the Management Board ends at any time during their term of office as Chairperson or Deputy Chairperson, their term of office shall automatically expire at the same time.

2. The Chairperson and the Deputy Chairperson shall be elected by a majority of two-thirds of the members of the Management Board.

3. Where the Chairperson is unable to carry out his or her duties, he or she shall automatically be replaced by the Deputy Chairperson.

#### *Article 14*

### **Meetings of the Management Board**

1. The Chairperson shall convene the meetings of the Management Board.

2. The Executive Director shall take part in the deliberations of the Management Board.

3. The Management Board shall hold at least two ordinary meetings a year. In addition, it shall meet on the initiative of its Chairperson, or at the request of the Commission or of at least one-third of its members.

4. The Management Board may invite any person whose opinion may be relevant for the discussion, including, where appropriate, a representative of the JPSG, to attend its meeting as a non-voting observer.

5. The members and the alternate members of the Management Board may, subject to its rules of procedure, be assisted at the meetings by advisers or experts.
6. Europol shall provide the secretariat for the Management Board.

#### *Article 15*

### **Voting rules of the Management Board**

1. Without prejudice to points (a) and (b) of Article 11(1), Article 13(2), Article 50(2), Article 54(8) and Article 64, the Management Board shall take decisions by a majority of its members.
2. Each member shall have one vote. In the absence of a voting member, his or her alternate shall be entitled to exercise his or her right to vote.
3. The Executive Director shall not take part in the vote.
4. The Management Board's rules of procedure shall establish more detailed voting arrangements, in particular the circumstances in which a member may act on behalf of another member, and any quorum requirements, where necessary.

#### *SECTION 2*

### ***Executive Director***

#### *Article 16*

### **Responsibilities of the Executive Director**

1. The Executive Director shall manage Europol. He or she shall be accountable to the Management Board.
2. Without prejudice to the powers of the Commission or the Management Board, the Executive Director shall be independent in the performance of his or her duties and shall neither seek nor take instructions from any government or any other body.
3. The Council may invite the Executive Director to report on the performance of his or her duties.
4. The Executive Director shall be the legal representative of Europol.
5. The Executive Director shall be responsible for the implementation of the tasks assigned to Europol by this Regulation, in particular:
  - (a) the day-to-day administration of Europol;
  - (b) making proposals to the Management Board as regards the establishment of Europol's internal structures;
  - (c) implementing decisions adopted by the Management Board;
  - (d) preparing the draft multiannual programming and annual work programmes and submitting them to the Management Board, after having consulted the Commission;

- (e) implementing the multiannual programming and the annual work programmes and reporting to the Management Board on their implementation;
- (f) preparing appropriate draft implementing rules to give effect to the Staff Regulations and the Conditions of Employment of Other Servants in accordance with Article 110 of the Staff Regulations;
- (g) preparing the draft consolidated annual report on Europol's activities and presenting it to the Management Board for adoption;
- (h) preparing an action plan following up conclusions of internal or external audit reports and evaluations, as well as investigation reports and recommendations from investigations by OLAF and the EDPS, and reporting on progress twice a year to the Commission and regularly to the Management Board;
- (i) protecting the financial interests of the Union by applying measures to prevent fraud, corruption and any other illegal activity and, without prejudice to the investigative competence of OLAF, by effective checks and, if irregularities are detected, by recovering amounts wrongly paid and, where appropriate, by effective, proportionate and dissuasive administrative and financial penalties;
- (j) preparing a draft internal anti-fraud strategy for Europol and presenting it to the Management Board for adoption;
- (k) preparing draft internal rules for the prevention and management of conflicts of interest in respect of the members of the Management Board and presenting those draft rules to the Management Board for adoption;
- (l) preparing draft financial rules applicable to Europol;
- (m) preparing Europol's draft statement of estimates of revenue and expenditure and implementing its budget;
- (n) supporting the Chairperson of the Management Board in preparing Management Board meetings;
- (o) informing the Management Board on a regular basis regarding the implementation of Union strategic and operational priorities for fighting crime;
- (p) performing other tasks pursuant to this Regulation.

#### CHAPTER IV

### PROCESSING OF INFORMATION

#### *Article 17*

#### **Sources of information**

1. Europol shall only process information that has been provided to it:
  - (a) by Member States in accordance with their national law and Article 7;
  - (b) by Union bodies, third countries and international organisations in accordance with Chapter V;
  - (c) by private parties and private persons in accordance with Chapter V.
2. Europol may directly retrieve and process information, including personal data, from publicly available sources, including the internet and public data.
3. In so far as Europol is entitled under Union, international or national legal instruments to gain computerised access to data from Union, international or national information systems, it may retrieve and process information, including personal data, by such means if that is necessary for the performance of its tasks. The applicable provisions of such Union, international or national legal instruments shall govern access to, and the use of, that information by Europol, in so far as they provide for stricter rules on access and use than those laid down by this Regulation. Access to such information systems shall be granted only to duly authorised staff of Europol and only in so far as this is necessary and proportionate for the performance of their tasks.

## Article 18

**Purposes of information processing activities**

1. In so far as is necessary for the achievement of its objectives as laid down in Article 3, Europol may process information, including personal data.
2. Personal data may be processed only for the purposes of:
  - (a) cross-checking aimed at identifying connections or other relevant links between information related to:
    - (i) persons who are suspected of having committed or taken part in a criminal offence in respect of which Europol is competent, or who have been convicted of such an offence;
    - (ii) persons regarding whom there are factual indications or reasonable grounds to believe that they will commit criminal offences in respect of which Europol is competent;
  - (b) analyses of a strategic or thematic nature;
  - (c) operational analyses;
  - (d) facilitating the exchange of information between Member States, Europol, other Union bodies, third countries and international organisations.
3. Processing for the purpose of operational analyses as referred to in point (c) of paragraph 2 shall be performed by means of operational analysis projects, in respect of which the following specific safeguards shall apply:
  - (a) for every operational analysis project, the Executive Director shall define the specific purpose, categories of personal data and categories of data subjects, participants, duration of storage and conditions for access, transfer and use of the data concerned, and shall inform the Management Board and the EDPS thereof;
  - (b) personal data may only be collected and processed for the purpose of the specified operational analysis project. Where it becomes apparent that personal data may be relevant for another operational analysis project, further processing of that personal data shall only be permitted insofar as such further processing is necessary and proportionate and the personal data are compatible with the provisions set out in point (a) that apply to the other analysis project;
  - (c) only authorised staff may access and process the data of the relevant project.
4. The processing referred to in paragraphs 2 and 3 shall be carried out in compliance with the data protection safeguards provided for in this Regulation. Europol shall duly document those processing operations. The documentation shall be made available, upon request, to the Data Protection Officer and to the EDPS for the purpose of verifying the lawfulness of the processing operations.
5. Categories of personal data and categories of data subjects whose data may be collected and processed for each purpose referred to in paragraph 2 are listed in Annex II.
6. Europol may temporarily process data for the purpose of determining whether such data are relevant to its tasks and, if so, for which of the purposes referred to in paragraph 2. The Management Board, acting on a proposal from the Executive Director and after consulting the EDPS, shall further specify the conditions relating to the processing of such data, in particular with respect to access to and use of the data, as well as time limits for the storage and deletion of the data, which may not exceed six months, having due regard to the principles referred to in Article 28.
7. The Management Board, after consulting the EDPS, shall, as appropriate, adopt guidelines further specifying procedures for the processing of information for the purposes listed in paragraph 2 in accordance with point (q) of Article 11(1).

*Article 19***Determination of the purpose of, and restrictions on, the processing of information by Europol**

1. A Member State, a Union body, a third country or an international organisation providing information to Europol shall determine the purpose or purposes for which it is to be processed, as referred to in Article 18. If it has not done so, Europol, in agreement with the provider of the information concerned, shall process the information in order to determine the relevance of such information as well as the purpose or purposes for which it is to be further processed. Europol may process information for a purpose different from that for which information has been provided only if authorised so to do by the provider of the information.
2. Member States, Union bodies, third countries and international organisations may indicate, at the moment of providing information to Europol, any restriction on access thereto or the use to be made thereof, in general or specific terms, including as regards its transfer, erasure or destruction. Where the need for such restrictions becomes apparent after the information has been provided, they shall inform Europol accordingly. Europol shall comply with such restrictions.
3. In duly justified cases Europol may assign restrictions to access or use by Member States, Union bodies, third countries and international organisations of information retrieved from publicly available sources.

*Article 20***Access by Member States and Europol's staff to information stored by Europol**

1. Member States shall, in accordance with their national law and Article 7(5), have access to, and be able to search, all information which has been provided for the purposes of points (a) and (b) of Article 18(2). This shall be without prejudice to the right of Member States, Union bodies, third countries and international organisations to indicate any restrictions in accordance with Article 19(2).
2. Member States shall, in accordance with their national law and Article 7(5), have indirect access on the basis of a hit/no hit system to information provided for the purposes of point (c) of Article 18(2). This shall be without prejudice to any restrictions indicated by the Member States, Union bodies and third countries or international organisations providing the information, in accordance with Article 19(2).

In the case of a hit, Europol shall initiate the procedure by which the information that generated the hit may be shared, in accordance with the decision of the provider of the information to Europol.

3. In accordance with national law, the information referred to in paragraphs 1 and 2 shall be accessed and further processed by Member States only for the purpose of preventing and combating:

- (a) forms of crime in respect of which Europol is competent; and
- (b) other forms of serious crime, as set out in Council Framework Decision 2002/584/JHA <sup>(1)</sup>.

4. Europol staff duly empowered by the Executive Director shall have access to information processed by Europol to the extent required for the performance of their duties and without prejudice to Article 67.

---

<sup>(1)</sup> Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190, 18.7.2002, p. 1).

*Article 21***Access by Eurojust and OLAF to information stored by Europol**

1. Europol shall take all appropriate measures to enable Eurojust and OLAF, within their respective mandates, to have indirect access on the basis of a hit/no hit system to information provided for the purposes of points (a), (b) and (c) of Article 18(2), without prejudice to any restrictions indicated by the Member State, Union body, third country or international organisation providing the information in question, in accordance with Article 19(2).

In the case of a hit, Europol shall initiate the procedure by which the information that generated the hit may be shared, in accordance with the decision of the provider of the information to Europol, and only to the extent that the data generating the hit are necessary for the performance of Eurojust's or OLAF's tasks.

2. Europol and Eurojust may conclude a working arrangement ensuring, in a reciprocal manner and within their respective mandates, access to, and the possibility of searching, all information that has been provided for the purpose specified in point (a) of Article 18(2). This shall be without prejudice to the right of Member States, Union bodies, third countries and international organisations to indicate restrictions on access to, and the use of, such data, and shall be in accordance with the data protection guarantees provided for in this Regulation.

3. Searches of information in accordance with paragraphs 1 and 2 shall be carried out only for the purpose of identifying whether information available at Eurojust or OLAF matches with information processed at Europol.

4. Europol shall allow searches in accordance with paragraphs 1 and 2 only after obtaining from Eurojust information on which National Members, Deputies and Assistants, as well as Eurojust staff members, and from OLAF information on which OLAF staff members, have been designated as authorised to perform such searches.

5. If, during Europol's information-processing activities in respect of an individual investigation, Europol or a Member State identifies the need for coordination, cooperation or support in accordance with the mandate of Eurojust or OLAF, Europol shall notify them to that effect and shall initiate the procedure for sharing the information, in accordance with the decision of the Member State providing the information. In such a case, Eurojust or OLAF shall consult with Europol.

6. Eurojust, including the College, the National Members, Deputies and Assistants, as well as Eurojust staff members, and OLAF, shall respect any restriction on access or use, in general or specific terms, indicated by Member States, Union bodies, third countries and international organisations in accordance with Article 19(2).

7. Europol, Eurojust and OLAF shall inform each other if, after consulting each other's data in accordance with paragraph 2 or as a result of a hit in accordance with paragraph 1, there are indications that data may be incorrect or may conflict with other data.

*Article 22***Duty to notify Member States**

1. Europol shall, in accordance with point (b) of Article 4(1), notify a Member State without delay of any information concerning it. If such information is subject to access restrictions pursuant to Article 19(2) that would prohibit its being shared, Europol shall consult with the provider of the information stipulating the access restriction and seek its authorisation for sharing.

In such a case, the information shall not be shared without an explicit authorisation by the provider.

2. Irrespective of any access restrictions, Europol shall notify a Member State of any information concerning it if this is absolutely necessary in the interest of preventing an imminent threat to life.

In such a case, Europol shall at the same time notify the provider of the information about the sharing of the information and justify its analysis of the situation.

## CHAPTER V

### RELATIONS WITH PARTNERS

#### SECTION 1

##### *Common provisions*

##### *Article 23*

##### **Common provisions**

1. In so far as necessary for the performance of its tasks, Europol may establish and maintain cooperative relations with Union bodies in accordance with the objectives of those bodies, the authorities of third countries, international organisations and private parties.
2. Subject to any restriction pursuant to Article 19(2) and without prejudice to Article 67, Europol may directly exchange all information, with the exception of personal data, with entities referred to in paragraph 1 of this Article, in so far as such an exchange is relevant for the performance of Europol's tasks.
3. The Executive Director shall inform the Management Board about any regular cooperative relations which Europol intends to establish and maintain in accordance with paragraphs 1 and 2, and about the development of such relations once established.
4. For the purposes set out in paragraphs 1 and 2, Europol may conclude working arrangements with entities referred to in paragraph 1. Such working arrangements shall not allow the exchange of personal data and shall not bind the Union or its Member States.
5. Europol may receive and process personal data from entities referred to in paragraph 1 insofar as necessary and proportionate for the legitimate performance of its tasks and subject to the provisions of this Chapter.
6. Without prejudice to Article 30(5), personal data shall only be transferred by Europol to Union bodies, third countries and international organisations if necessary for preventing and combating crime falling within the scope of Europol's objectives and in accordance with this Regulation, and if the recipient gives an undertaking that the data will be processed only for the purpose for which they were transferred. If the data to be transferred have been provided by a Member State, Europol shall seek that Member State's consent, unless the Member State has granted its prior authorisation to such onward transfer, either in general terms or subject to specific conditions. Such consent may be withdrawn at any time.
7. Onward transfers of personal data held by Europol by Member States, Union bodies, third countries and international organisations shall be prohibited, unless Europol has given its prior explicit authorisation.
8. Europol shall ensure that detailed records of all transfers of personal data and of the grounds for such transfers are recorded in accordance with this Regulation.
9. Any information which has clearly been obtained in obvious violation of human rights shall not be processed.



## SECTION 2

*Transfer and exchange of personal data*

## Article 24

**Transfer of personal data to Union bodies**

Subject to any possible restrictions pursuant to Article 19(2) or (3) and without prejudice to Article 67, Europol may directly transfer personal data to a Union body, insofar as such transfer is necessary for the performance of its tasks or those of the recipient Union body.

## Article 25

**Transfer of personal data to third countries and international organisations**

1. Subject to any possible restrictions pursuant to Article 19(2) or (3) and without prejudice to Article 67, Europol may transfer personal data to an authority of a third country or to an international organisation, insofar as such transfer is necessary for the performance of Europol's tasks, on the basis of one of the following:

- (a) a decision of the Commission adopted in accordance with Article 36 of Directive (EU) 2016/680, finding that the third country or a territory or a processing sector within that third country or the international organisation in question ensures an adequate level of protection ('adequacy decision');
- (b) an international agreement concluded between the Union and that third country or international organisation pursuant to Article 218 TFEU adducing adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals;
- (c) a cooperation agreement allowing for the exchange of personal data concluded, before 1 May 2017, between Europol and that third country or international organisation in accordance with Article 23 of Decision 2009/371/JHA.

Europol may conclude administrative arrangements to implement such agreements or adequacy decisions.

2. The Executive Director shall inform the Management Board about exchanges of personal data on the basis of adequacy decisions pursuant to point (a) of paragraph 1.

3. Europol shall publish on its website and keep up to date a list of adequacy decisions, agreements, administrative arrangements and other instruments relating to the transfer of personal data in accordance with paragraph 1.

4. By 14 June 2021, the Commission shall assess the provisions contained in the cooperation agreements referred to in point (c) of paragraph 1, in particular those concerning data protection. The Commission shall inform the European Parliament and the Council about the outcome of that assessment, and may, if appropriate, submit to the Council a recommendation for a decision authorising the opening of negotiations for the conclusion of international agreements referred to in point (b) of paragraph (1).

5. By way of derogation from paragraph 1, the Executive Director may authorise the transfer of personal data to third countries or international organisations on a case-by-case basis if the transfer is:

- (a) necessary in order to protect the vital interests of the data subject or of another person;
- (b) necessary to safeguard legitimate interests of the data subject where the law of the Member State transferring the personal data so provides;

- (c) essential for the prevention of an immediate and serious threat to the public security of a Member State or a third country;
- (d) necessary in individual cases for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal sanctions; or
- (e) necessary in individual cases for the establishment, exercise or defence of legal claims relating to the prevention, investigation, detection or prosecution of a specific criminal offence or the execution of a specific criminal sanction.

Personal data shall not be transferred if the Executive Director determines that fundamental rights and freedoms of the data subject concerned override the public interest in the transfer referred to in points (d) and (e).

Derogations may not be applicable to systematic, massive or structural transfers.

6. By way of derogation from paragraph 1, the Management Board may, in agreement with the EDPS, authorise for a period not exceeding one year, which shall be renewable, a set of transfers in accordance with points (a) to (e) of paragraph 5, taking into account the existence of adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals. Such authorisation shall be duly justified and documented.

7. The Executive Director shall as soon as possible inform the Management Board and the EDPS of the cases in which paragraph 5 has been applied.

8. Europol shall keep detailed records of all transfers made pursuant to this Article.

## Article 26

### Exchanges of personal data with private parties

1. Insofar as is necessary in order for Europol to perform its tasks, Europol may process personal data obtained from private parties on condition that they are received via:

- (a) a national unit in accordance with national law;
- (b) the contact point of a third country or an international organisation with which Europol has concluded, before 1 May 2017, a cooperation agreement allowing for the exchange of personal data in accordance with Article 23 of Decision 2009/371/JHA; or
- (c) an authority of a third country or an international organisation which is the subject of an adequacy decision as referred to in point (a) of Article 25(1) of this Regulation or with which the Union has concluded an international agreement pursuant to Article 218 TFEU.

2. In cases where Europol nonetheless receives personal data directly from private parties and where the national unit, contact point or authority concerned, as referred to in paragraph 1, cannot be identified, Europol may process those personal data solely for the purpose of such identification. Subsequently, the personal data shall be forwarded immediately to the national unit, contact point or authority concerned and shall be deleted unless the national unit, contact point or authority concerned resubmits those personal data in accordance with Article 19(1) within four months after the transfer takes place. Europol shall ensure by technical means that, during that period, the data in question are not accessible for processing for any other purpose.

3. Following the transfer of personal data in accordance with point (c) of paragraph 5 of this Article, Europol may in connection therewith receive personal data directly from a private party which that private party declares it is legally allowed to transmit in accordance with the applicable law, in order to process such data for the performance of the task set out in point (m) of Article 4(1).

4. If Europol receives personal data from a private party in a third country with which there is no agreement concluded either on the basis of Article 23 of Decision 2009/371/JHA or on the basis of Article 218 TFEU, or which is not the subject of an adequacy decision as referred to in point (a) of Article 25(1) of this Regulation, Europol may forward those data only to a Member State, or to a third country concerned with which such an agreement has been concluded.

5. Europol may not transfer personal data to private parties except where, on a case-by-case basis where strictly necessary and subject to any possible restrictions stipulated pursuant to Article 19(2) or (3) and without prejudice to Article 67:

- (a) the transfer is undoubtedly in the interests of the data subject, and either the data subject's consent has been given or the circumstances allow a clear presumption of consent; or
- (b) the transfer is absolutely necessary in the interests of preventing the imminent perpetration of a crime, including terrorism, for which Europol is competent; or
- (c) the transfer of personal data which are publicly available is strictly necessary for the performance of the task set out in point (m) of Article 4(1) and the following conditions are met:
  - (i) the transfer concerns an individual and specific case; and
  - (ii) no fundamental rights and freedoms of the data subjects concerned override the public interest necessitating the transfer in the case at hand.

6. With regard to points (a) and (b) of paragraph 5 of this Article, if the private party concerned is not established within the Union or in a country with which Europol has a cooperation agreement allowing for the exchange of personal data, with which the Union has concluded an international agreement pursuant to Article 218 TFEU or which is the subject of an adequacy decision as referred to in point (a) of Article 25(1) of this Regulation, the transfer shall only be authorised if the transfer is:

- (a) necessary in order to protect the vital interests of the data subject or another person; or
- (b) necessary in order to safeguard legitimate interests of the data subject; or
- (c) essential for the prevention of an immediate and serious threat to public security of a Member State or a third country; or
- (d) necessary in individual cases for the purposes of the prevention, investigation, detection or prosecution of criminal offences for which Europol is competent; or
- (e) necessary in individual cases for the establishment, exercise or defence of legal claims relating to the prevention, investigation, detection or prosecution of a specific criminal offence for which Europol is competent.

7. Europol shall ensure that detailed records of all transfers of personal data and the grounds for such transfers are recorded in accordance with this Regulation and communicated upon request to the EDPS pursuant to Article 40.

8. If the personal data received or to be transferred affect the interests of a Member State, Europol shall immediately inform the national unit of the Member State concerned.

9. Europol shall not contact private parties to retrieve personal data.

10. The Commission shall evaluate the practice of direct exchanges of personal data with private parties by 1 May 2019.

*Article 27***Information from private persons**

1. Insofar as is necessary in order for Europol to perform its tasks, Europol may receive and process information originating from private persons. Personal data originating from private persons may only be processed by Europol on condition that they are received via:

- (a) a national unit in accordance with national law;
- (b) the contact point of a third country or an international organisation with which Europol has concluded, before 1 May 2017, a cooperation agreement allowing for the exchange of personal data in accordance with Article 23 of Decision 2009/371/JHA; or
- (c) an authority of a third country or an international organisation which is the subject of an adequacy decision as referred to in point (a) of Article 25(1) or with which the Union has concluded an international agreement pursuant to Article 218 TFEU.

2. If Europol receives information, including personal data, from a private person residing in a third country with which there is no international agreement concluded either on the basis of Article 23 of Decision 2009/371/JHA or on the basis of Article 218 TFEU, or which is not the subject of an adequacy decision as referred to in point (a) of Article 25(1) of this Regulation, Europol may only forward that information to a Member State or to a third country concerned with which such an international agreement has been concluded.

3. If the personal data received affect the interests of a Member State, Europol shall immediately inform the national unit of the Member State concerned.

4. Europol shall not contact private persons to retrieve information.

5. Without prejudice to Articles 36 and 37, Europol may not transfer personal data to private persons.

## CHAPTER VI

**DATA PROTECTION SAFEGUARDS***Article 28***General data protection principles**

1. Personal data shall be:

- (a) processed fairly and lawfully;
- (b) collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes. Further processing of personal data for historical, statistical or scientific research purposes shall not be considered incompatible provided that Europol provides appropriate safeguards, in particular to ensure that data are not processed for any other purposes;
- (c) adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed;
- (d) accurate and kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

- (e) kept in a form which permits identification of data subjects for no longer than necessary for the purposes for which the personal data are processed; and
  - (f) processed in a manner that ensures appropriate security of personal data.
2. Europol shall make publicly available a document setting out in an intelligible form the provisions regarding the processing of personal data and the means available for the exercise of the rights of data subjects.

#### Article 29

##### **Assessment of reliability of the source and accuracy of information**

1. The reliability of the source of information originating from a Member State shall be assessed as far as possible by the providing Member State using the following source evaluation codes:

(A): where there is no doubt as to the authenticity, trustworthiness and competence of the source, or if the information is provided by a source which has proved to be reliable in all instances;

(B): where the information is provided by a source which has in most instances proved to be reliable;

(C): where the information is provided by a source which has in most instances proved to be unreliable;

(X): where the reliability of the source cannot be assessed.

2. The accuracy of information originating from a Member State shall be assessed as far as possible by the providing Member State using the following information evaluation codes:

(1): information the accuracy of which is not in doubt;

(2): information known personally to the source but not known personally to the official passing it on;

(3): information not known personally to the source but corroborated by other information already recorded;

(4): information not known personally to the source and which cannot be corroborated.

3. Where Europol, on the basis of information already in its possession, comes to the conclusion that the assessment provided for in paragraphs 1 or 2 needs to be corrected, it shall inform the Member State concerned and seek to agree on an amendment to the assessment. Europol shall not change the assessment without such agreement.

4. Where Europol receives information from a Member State without an assessment in accordance with paragraphs 1 or 2, it shall attempt to assess the reliability of the source or the accuracy of information on the basis of information already in its possession. The assessment of specific data and information shall take place in agreement with the providing Member State. A Member State may also agree with Europol in general terms on the assessment of specified types of data and specified sources. If no agreement is reached in a specific case, or no agreement in general terms exists, Europol shall assess the information or data and shall attribute to such information or data the evaluation codes (X) and (4) referred to in paragraphs 1 and 2 respectively.

5. This Article shall apply *mutatis mutandis* where Europol receives data or information from a Union body, third country, international organisation or private party.

6. Information from publicly available sources shall be assessed by Europol using the evaluation codes set out in paragraphs 1 and 2.

7. Where information is the result of an analysis made by Europol in the performance of its tasks, Europol shall assess such information in accordance with this Article, and in agreement with the Member States participating in the analysis.

#### *Article 30*

### **Processing of special categories of personal data and of different categories of data subjects**

1. Processing of personal data in respect of victims of a criminal offence, witnesses or other persons who can provide information concerning criminal offences, or in respect of persons under the age of 18, shall be allowed if it is strictly necessary and proportionate for preventing or combating crime that falls within Europol's objectives.

2. Processing of personal data, by automated or other means, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership and processing of genetic data or data concerning a person's health or sex life shall be prohibited, unless it is strictly necessary and proportionate for preventing or combating crime that falls within Europol's objectives and if those data supplement other personal data processed by Europol. The selection of a particular group of persons solely on the basis of such personal data shall be prohibited.

3. Only Europol shall have direct access to personal data as referred to in paragraphs 1 and 2. The Executive Director shall duly authorise a limited number of Europol officials to have such access if it is necessary for the performance of their tasks.

4. No decision by a competent authority which produces adverse legal effects concerning a data subject shall be based solely on automated processing of data as referred to in paragraph 2, unless the decision is expressly authorised pursuant to national or Union legislation.

5. Personal data as referred to in paragraphs 1 and 2 shall not be transmitted to Member States, Union bodies, third countries or international organisations unless such transmission is strictly necessary and proportionate in individual cases concerning crime that falls within Europol's objectives and in accordance with Chapter V.

6. Every year Europol shall provide to the EDPS a statistical overview of all personal data as referred to in paragraph 2 which it has processed.

#### *Article 31*

### **Time-limits for the storage and erasure of personal data**

1. Personal data processed by Europol shall be stored by Europol only for as long as is necessary and proportionate for the purposes for which the data are processed.

2. Europol shall in any event review the need for continued storage no later than three years after the start of initial processing of personal data. Europol may decide on the continued storage of personal data until the following review, which shall take place after another period of three years, if continued storage is still necessary for the performance of Europol's tasks. The reasons for the continued storage shall be justified and recorded. If no decision is taken on the continued storage of personal data, that data shall be erased automatically after three years.

3. If personal data as referred to in Article 30(1) and (2) are stored for a period exceeding five years, the EDPS shall be informed accordingly.
4. Where a Member State, a Union body, a third country or an international organisation has indicated any restriction as regards the earlier erasure or destruction of the personal data at the moment of transfer in accordance with Article 19(2), Europol shall erase the personal data in accordance with those restrictions. If continued storage of the data is deemed necessary, on the basis of information that is more extensive than that possessed by the data provider, in order for Europol to perform its tasks, Europol shall request the authorisation of the data provider to continue storing the data and shall present a justification for such request.
5. Where a Member State, a Union body, a third country or an international organisation erases from its own data files personal data provided to Europol, it shall inform Europol accordingly. Europol shall erase the data unless the continued storage of the data is deemed necessary, on the basis of information that is more extensive than that possessed by the data provider, in order for Europol to perform its tasks. Europol shall inform the data provider of the continued storage of such data and present a justification of such continued storage.
6. Personal data shall not be erased if:
  - (a) this would damage the interests of a data subject who requires protection. In such cases, the data shall be used only with the express and written consent of the data subject;
  - (b) their accuracy is contested by the data subject, for a period enabling Member States or Europol, where appropriate, to verify the accuracy of the data;
  - (c) they have to be maintained for purposes of proof or for the establishment, exercise or defence of legal claims; or
  - (d) the data subject opposes their erasure and requests the restriction of their use instead.

## Article 32

### Security of processing

1. Europol shall implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction, accidental loss or unauthorised disclosure, alteration and access or any other unauthorised form of processing.
2. In respect of automated data processing, Europol and each Member State shall implement measures designed to:
  - (a) deny unauthorised persons access to data-processing equipment used for processing personal data (equipment access control);
  - (b) prevent the unauthorised reading, copying, modification or removal of data media (data media control);
  - (c) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data (storage control);
  - (d) prevent the use of automated data-processing systems by unauthorised persons using data-communication equipment (user control);
  - (e) ensure that persons authorised to use an automated data-processing system have access only to data covered by their access authorisation (data access control);

- (f) ensure that it is possible to verify and establish to which bodies personal data may be or have been transmitted using data-communication equipment (communication control);
  - (g) ensure that it is possible to verify and establish which personal data have been input into automated data-processing systems and when and by whom the data were input (input control);
  - (h) ensure that it is possible to verify and establish what data have been accessed by which member of personnel and at what time (access log);
  - (i) prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during the transportation of data media (transport control);
  - (j) ensure that it is possible, in the event of interruption, to restore installed systems immediately (recovery); and
  - (k) ensure that the functions of the system perform faultlessly, that the occurrence of faults in the functions is immediately reported (reliability) and that stored data cannot be corrupted by system malfunctions (integrity).
3. Europol and Member States shall establish mechanisms to ensure that security needs are taken on board across information system boundaries.

#### *Article 33*

### **Data protection by design**

Europol shall implement appropriate technical and organisational measures and procedures in such a way that the data processing will comply with this Regulation and protect the rights of the data subjects concerned.

#### *Article 34*

### **Notification of a personal data breach to the authorities concerned**

1. In the event of a personal data breach, Europol shall without undue delay notify the EDPS, as well as the competent authorities of the Member States concerned, of that breach, in accordance with the conditions laid down in Article 7(5), as well as the provider of the data concerned.
2. The notification referred to in paragraph 1 shall, as a minimum:
  - (a) describe the nature of the personal data breach including, where possible and appropriate, the categories and number of data subjects concerned and the categories and number of data records concerned;
  - (b) describe the likely consequences of the personal data breach;
  - (c) describe the measures proposed or taken by Europol to address the personal data breach; and
  - (d) where appropriate, recommend measures to mitigate the possible adverse effects of the personal data breach.
3. Europol shall document any personal data breaches, including the facts surrounding the breach, its effects and the remedial action taken, thereby enabling the EDPS to verify compliance with this Article.



*Article 35***Communication of a personal data breach to the data subject**

1. Subject to paragraph 4 of this Article, where a personal data breach as referred to in Article 34 is likely to severely and adversely affect the rights and freedoms of the data subject, Europol shall communicate the personal data breach to the data subject without undue delay.
2. The communication to the data subject referred to in paragraph 1 shall describe, where possible, the nature of the personal data breach, recommend measures to mitigate the possible adverse effects of the personal data breach, and contain the identity and contact details of the Data Protection Officer.
3. If Europol does not have the contact details of the data subject concerned, it shall request the provider of the data to communicate the personal data breach to the data subject concerned and to inform Europol about the decision taken. Member States providing the data shall communicate the breach to the data subject concerned in accordance with the procedures of their national law.
4. The communication of a personal data breach to the data subject shall not be required if:
  - (a) Europol has applied to the personal data concerned by that breach appropriate technological protection measures that render the data unintelligible to any person who is not authorised to access it;
  - (b) Europol has taken subsequent measures which ensure that the data subject's rights and freedoms are no longer likely to be severely affected; or
  - (c) such communication would involve disproportionate effort, in particular owing to the number of cases involved. In such a case, there shall instead be a public communication or similar measure informing the data subjects concerned in an equally effective manner.
5. The communication to the data subject may be delayed, restricted or omitted where this constitutes a necessary measure with due regard for the legitimate interests of the person concerned:
  - (a) to avoid obstructing official or legal inquiries, investigations or procedures;
  - (b) to avoid prejudicing the prevention, detection, investigation and prosecution of criminal offences or for the execution of criminal penalties;
  - (c) to protect public and national security;
  - (d) to protect the rights and freedoms of third parties.

*Article 36***Right of access for the data subject**

1. Any data subject shall have the right, at reasonable intervals, to obtain information on whether personal data relating to him or her are processed by Europol.
2. Without prejudice to paragraph 5, Europol shall provide the following information to the data subject:
  - (a) confirmation as to whether or not data related to him or her are being processed;
  - (b) information on at least the purposes of the processing operation, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed;

- (c) communication in an intelligible form of the data undergoing processing and of any available information as to their sources;
- (d) an indication of the legal basis for processing the data;
- (e) the envisaged period for which the personal data will be stored;
- (f) the existence of the right to request from Europol rectification, erasure or restriction of processing of personal data concerning the data subject.

3. Any data subject wishing to exercise the right of access to personal data relating to him or her may make a request to that effect, without incurring excessive costs, to the authority appointed for that purpose in the Member State of his or her choice. That authority shall refer the request to Europol without delay, and in any case within one month of receipt.

4. Europol shall confirm receipt of the request under paragraph 3. Europol shall answer it without undue delay, and in any case within three months of receipt by Europol of the request from the national authority.

5. Europol shall consult the competent authorities of the Member States, in accordance with the conditions laid down in Article 7(5), and the provider of the data concerned, on a decision to be taken. A decision on access to personal data shall be conditional on close cooperation between Europol and the Member States and the provider of the data directly concerned by the access of the data subject to such data. If a Member State or the provider of the data objects to Europol's proposed response, it shall notify Europol of the reasons for its objection in accordance with paragraph 6 of this Article. Europol shall take the utmost account of any such objection. Europol shall subsequently notify its decision to the competent authorities concerned, in accordance with the conditions laid down in Article 7(5), and to the provider of the data.

6. The provision of information in response to any request under paragraph 1 may be refused or restricted if such refusal or restriction constitutes a measure that is necessary in order to:

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

When the applicability of an exemption is assessed, the fundamental rights and interests of the data subject shall be taken into account.

7. Europol shall inform the data subject in writing of any refusal or restriction of access, of the reasons for such a decision and of his or her right to lodge a complaint with the EDPS. Where the provision of such information would deprive paragraph 6 of its effect, Europol shall only notify the data subject concerned that it has carried out the checks, without giving any information which might reveal to him or her whether or not personal data concerning him or her are processed by Europol.

#### *Article 37*

### **Right to rectification, erasure and restriction**

1. Any data subject having accessed personal data concerning him or her processed by Europol in accordance with Article 36 shall have the right to request Europol, through the authority appointed for that purpose in the Member State of his or her choice, to rectify personal data concerning him or her held by Europol if they are incorrect or to complete or update them. That authority shall refer the request to Europol without delay and in any case within one month of receipt.

2. Any data subject having accessed personal data concerning him or her processed by Europol in accordance with Article 36 shall have the right to request Europol, through the authority appointed for that purpose in the Member State of his or her choice, to erase personal data relating to him or her held by Europol if they are no longer required for the purposes for which they are collected or are further processed. That authority shall refer the request to Europol without delay and in any case within one month of receipt.
3. Europol shall restrict rather than erase personal data as referred to in paragraph 2 if there are reasonable grounds to believe that erasure could affect the legitimate interests of the data subject. Restricted data shall be processed only for the purpose that prevented their erasure.
4. If personal data as referred to in paragraphs 1, 2 and 3 held by Europol have been provided to it by third countries, international organisations or Union bodies, have been directly provided by private parties or have been retrieved by Europol from publicly available sources or result from Europol's own analyses, Europol shall rectify, erase or restrict such data and, where appropriate, inform the providers of the data.
5. If personal data as referred to in paragraphs 1, 2 and 3 held by Europol have been provided to Europol by Member States, the Member States concerned shall rectify, erase or restrict such data in collaboration with Europol, within their respective competences.
6. If incorrect personal data have been transferred by another appropriate means or if the errors in the data provided by Member States are due to faulty transfer or transfer in breach of this Regulation or if they result from data being input, taken over or stored in an incorrect manner or in breach of this Regulation by Europol, Europol shall rectify or erase such data in collaboration with the provider of the data concerned.
7. In the cases referred to in paragraphs 4, 5 and 6, all addressees of the data concerned shall be notified forthwith. In accordance with the rules applicable to them, the addressees shall then rectify, erase or restrict those data in their systems.
8. Europol shall inform the data subject in writing without undue delay, and in any case within three months of receipt of a request in accordance with paragraph 1 or 2, that data concerning him or her have been rectified, erased or restricted.
9. Within three months of receipt of a request in accordance with paragraph 1 or 2, Europol shall inform the data subject in writing of any refusal of rectification, erasure or restricting, of the reasons for such a refusal and of the possibility of lodging a complaint with the EDPS and of seeking a judicial remedy.

#### *Article 38*

#### **Responsibility in data protection matters**

1. Europol shall store personal data in a way that ensures that their source, as referred to in Article 17, can be established.
2. The responsibility for the quality of personal data as referred to in point (d) of Article 28(1) shall lie with:
  - (a) the Member State or the Union body which provided the personal data to Europol;
  - (b) Europol in respect of personal data provided by third countries or international organisations or directly provided by private parties; of personal data retrieved by Europol from publicly available sources or resulting from Europol's own analyses; and of personal data stored by Europol in accordance with Article 31(5).

3. If Europol becomes aware that personal data provided pursuant to points (a) and (b) of Article 17(1) are factually incorrect or have been unlawfully stored, it shall inform the provider of those data accordingly.

4. Europol shall be responsible for compliance with the principles referred to in points (a), (b), (c), (e) and (f) of Article 28(1).

5. The responsibility for the legality of a data transfer shall lie with:

(a) the Member State which provided the personal data to Europol;

(b) Europol in the case of personal data provided by it to Member States, third countries or international organisations.

6. In the case of a transfer between Europol and a Union body, the responsibility for the legality of the transfer shall lie with Europol.

Without prejudice to the first subparagraph, where the data are transferred by Europol following a request from the recipient, both Europol and the recipient shall be responsible for the legality of such a transfer.

7. Europol shall be responsible for all data processing operations carried out by it, with the exception of the bilateral exchange of data using Europol's infrastructure between Member States, Union bodies, third countries and international organisations to which Europol has no access. Such bilateral exchanges shall take place under the responsibility of the entities concerned and in accordance with their law. The security of such exchanges shall be ensured in accordance with Article 32.

#### *Article 39*

#### **Prior consultation**

1. Any new type of processing operations to be carried out shall be subject to prior consultation where:

(a) special categories of data as referred to in Article 30(2) are to be processed;

(b) the type of processing, in particular using new technologies, mechanisms or procedures, presents specific risks for the fundamental rights and freedoms, and in particular the protection of personal data, of data subjects.

2. The prior consultation shall be carried out by the EDPS following receipt of a notification from the Data Protection Officer that shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address those risks, safeguards and security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of the data subjects and other persons concerned.

3. The EDPS shall deliver his or her opinion to the Management Board within two months following receipt of the notification. That period may be suspended until the EDPS has obtained any further information that he or she may have requested.

If the opinion has not been delivered after four months it shall be deemed to be favourable.

If the opinion of the EDPS is that the notified processing may involve a breach of any provision of this Regulation, he or she shall, where appropriate, make proposals to avoid such a breach. Where Europol does not modify the processing operation accordingly, the EDPS may exercise the powers granted to him or her under Article 43(3).

4. The EDPS shall keep a register of all processing operations that have been notified to him or her pursuant to paragraph 1. The register shall not be made public.

#### *Article 40*

### **Logging and documentation**

1. For the purpose of verifying the lawfulness of data processing, self-monitoring and ensuring proper data integrity and security, Europol shall keep records of the collection, alteration, access, disclosure, combination or erasure of personal data. Such logs or documentation shall be deleted after three years, unless the data which they contain are further required for ongoing control. There shall be no possibility of modifying the logs.

2. Logs or documentation prepared pursuant to paragraph 1 shall be communicated upon request to the EDPS, to the Data Protection Officer and, if required for a specific investigation, to the national unit concerned. The information thus communicated shall only be used for the control of data protection and for ensuring proper data processing as well as data integrity and security.

#### *Article 41*

### **Data Protection Officer**

1. The Management Board shall appoint a Data Protection Officer, who shall be a member of the staff. In the performance of his or her duties, he or she shall act independently.

2. The Data Protection Officer shall be selected on the basis of his or her personal and professional qualities and, in particular, the expert knowledge of data protection.

It shall be ensured in the selection of the Data Protection Officer that no conflict of interest may result from the performance of his or her duty in that capacity and from any other official duties, in particular those relating to the application of this Regulation.

3. The Data Protection Officer shall be appointed for a term of four years. He or she shall be eligible for reappointment up to a maximum total term of eight years. He or she may be dismissed from his or her function as Data Protection Officer by the Management Board only with the consent of the EDPS, if he or she no longer meets the conditions required for the performance of his or her duties.

4. After his or her appointment, the Data Protection Officer shall be registered with the EDPS by the Management Board.

5. With respect to the performance of his or her duties, the Data Protection Officer shall not receive any instructions.

6. The Data Protection Officer shall, in particular, have the following tasks with regard to personal data, with the exception of administrative personal data:

- (a) ensuring, in an independent manner, the internal application of this Regulation concerning the processing of personal data;
- (b) ensuring that a record of the transfer and receipt of personal data is kept in accordance with this Regulation;

- (c) ensuring that data subjects are informed of their rights under this Regulation at their request;
- (d) cooperating with Europol staff responsible for procedures, training and advice on data processing;
- (e) cooperating with the EDPS;
- (f) preparing an annual report and communicating that report to the Management Board and to the EDPS;
- (g) keeping a register of personal data breaches.

7. The Data Protection Officer shall also carry out the functions provided for by Regulation (EC) No 45/2001 with regard to administrative personal data.

8. In the performance of his or her tasks, the Data Protection Officer shall have access to all the data processed by Europol and to all Europol premises.

9. If the Data Protection Officer considers that the provisions of this Regulation concerning the processing of personal data have not been complied with, he or she shall inform the Executive Director and shall require him or her to resolve the non-compliance within a specified time.

If the Executive Director does not resolve the non-compliance of the processing within the time specified, the Data Protection Officer shall inform the Management Board. The Data Protection Officer and the Management Board shall agree a specified time for a response by the latter. If the Management Board does not resolve the non-compliance within the time specified, the Data Protection Officer shall refer the matter to the EDPS.

10. The Management Board shall adopt implementing rules concerning the Data Protection Officer. Those implementing rules shall, in particular, concern the selection procedure for the position of the Data Protection Officer and his or her dismissal, tasks, duties and powers, and safeguards ensuring the independence of the Data Protection Officer.

11. Europol shall provide the Data Protection Officer with the staff and resources needed in order for him or her to be able to carry out his or her duties. Those staff members shall have access to all the data processed at Europol and to Europol premises only to the extent necessary for the performance of their tasks.

12. The Data Protection Officer and his or her staff shall be bound by the obligation of confidentiality in accordance with Article 67(1).

#### *Article 42*

### **Supervision by the national supervisory authority**

1. Each Member State shall designate a national supervisory authority. The national supervisory authority shall have the task of monitoring independently, in accordance with its national law, the permissibility of the transfer, the retrieval and any communication to Europol of personal data by the Member State concerned, and of examining whether such transfer, retrieval or communication violates the rights of the data subjects concerned. For that purpose, the national supervisory authority shall have access, at the national unit or at the liaison officers' premises, to data submitted by its Member State to Europol in accordance with the relevant national procedures and to logs and documentation as referred to in Article 40.

2. For the purpose of exercising their supervisory function, national supervisory authorities shall have access to the offices and documents of their respective liaison officers at Europol.

3. National supervisory authorities shall, in accordance with the relevant national procedures, supervise the activities of national units and the activities of liaison officers, insofar as such activities are relevant to the protection of personal data. They shall also keep the EDPS informed of any actions they take with respect to Europol.

4. Any person shall have the right to request the national supervisory authority to verify the legality of any transfer or communication to Europol of data concerning him or her in any form and of access to those data by the Member State concerned. That right shall be exercised in accordance with the national law of the Member State in which the request is made.

#### *Article 43*

### **Supervision by the EDPS**

1. The EDPS shall be responsible for monitoring and ensuring the application of the provisions of this Regulation relating to the protection of fundamental rights and freedoms of natural persons with regard to the processing of personal data by Europol, and for advising Europol and data subjects on all matters concerning the processing of personal data. To that end, he or she shall fulfil the duties set out in paragraph 2 and exercise the powers laid down in paragraph 3, while closely cooperating with the national supervisory authorities in accordance with Article 44.

2. The EDPS shall have the following duties:

- (a) hearing and investigating complaints, and informing the data subject of the outcome within a reasonable period;
- (b) conducting inquiries either on his or her own initiative or on the basis of a complaint, and informing the data subject of the outcome within a reasonable period;
- (c) monitoring and ensuring the application of this Regulation and any other Union act relating to the protection of natural persons with regard to the processing of personal data by Europol;
- (d) advising Europol, either on his or her own initiative or in response to a consultation, on all matters concerning the processing of personal data, in particular before it draws up internal rules relating to the protection of fundamental rights and freedoms with regard to the processing of personal data;
- (e) keeping a register of new types of processing operations notified to him or her by virtue of Article 39(1) and registered in accordance with Article 39(4);
- (f) carrying out a prior consultation on processing notified to him or her.

3. The EDPS may pursuant to this Regulation:

- (a) give advice to data subjects on the exercise of their rights;
- (b) refer a matter to Europol in the event of an alleged breach of the provisions governing the processing of personal data, and, where appropriate, make proposals for remedying that breach and for improving the protection of the data subjects;
- (c) order that requests to exercise certain rights in relation to data be complied with where such requests have been refused in breach of Articles 36 and 37;
- (d) warn or admonish Europol;

- (e) order Europol to carry out the rectification, restriction, erasure or destruction of personal data which have been processed in breach of the provisions governing the processing of personal data and to notify such actions to third parties to whom such data have been disclosed;
- (f) impose a temporary or definitive ban on processing operations by Europol which are in breach of the provisions governing the processing of personal data;
- (g) refer a matter to Europol and, if necessary, to the European Parliament, the Council and the Commission;
- (h) refer a matter to the Court of Justice of the European Union under the conditions provided for in the TFEU;
- (i) intervene in actions brought before the Court of Justice of the European Union.

4. The EDPS shall have the power to:

- (a) obtain from Europol access to all personal data and to all information necessary for his or her enquiries;
- (b) obtain access to any premises in which Europol carries on its activities when there are reasonable grounds for presuming that an activity covered by this Regulation is being carried out there.

5. The EDPS shall draw up an annual report on the supervisory activities of Europol, after consulting the national supervisory authorities. That report shall be part of the annual report of the EDPS referred to in Article 48 of Regulation (EC) No 45/2001.

The report shall include statistical information regarding complaints, inquiries, and investigations carried out in accordance with paragraph 2, as well as regarding transfers of personal data to third countries and international organisations, cases of prior consultation, and the use of the powers laid down in paragraph 3.

6. The EDPS, the officials and the other staff members of the EDPS's Secretariat shall be bound by the obligation of confidentiality laid down in Article 67(1).

#### *Article 44*

### **Cooperation between the EDPS and national supervisory authorities**

1. The EDPS shall act in close cooperation with the national supervisory authorities on issues requiring national involvement, in particular if the EDPS or a national supervisory authority finds major discrepancies between the practices of Member States or potentially unlawful transfers in the use of Europol's channels for exchanges of information, or in the context of questions raised by one or more national supervisory authorities on the implementation and interpretation of this Regulation.

2. The EDPS shall use the expertise and experience of the national supervisory authorities in carrying out his or her duties as set out in Article 43(2). In carrying out joint inspections together with the EDPS, members and staff of national supervisory authorities shall, taking due account of the principles of subsidiarity and proportionality, have powers equivalent to those laid down in Article 43(4) and be bound by an obligation equivalent to that laid down in Article 43(6). The EDPS and the national supervisory authorities shall, each acting within the scope of their respective competences, exchange relevant information and assist each other in carrying out audits and inspections.

3. The EDPS shall keep national supervisory authorities fully informed of all issues directly affecting or otherwise relevant to them. Upon the request of one or more national supervisory authorities, the EDPS shall inform them of specific issues.



4. In cases relating to data originating from one or more Member States, including the cases referred to in Article 47(2), the EDPS shall consult the national supervisory authorities concerned. The EDPS shall not decide on further action to be taken before those national supervisory authorities have informed the EDPS of their position, within a deadline specified by him or her which shall not be shorter than one month and not longer than three months. The EDPS shall take the utmost account of the respective positions of the national supervisory authorities concerned. In cases where the EDPS intends not to follow the position of a national supervisory authority, he or she shall inform that authority, provide a justification and submit the matter for discussion to the Cooperation Board established by Article 45(1).

In cases which the EDPS considers to be extremely urgent, he or she may decide to take immediate action. In such cases, the EDPS shall immediately inform the national supervisory authorities concerned and justify the urgent nature of the situation as well as the action he or she has taken.

#### *Article 45*

### **Cooperation Board**

1. A Cooperation Board with an advisory function is hereby established. It shall be composed of a representative of a national supervisory authority of each Member State and of the EDPS.

2. The Cooperation Board shall act independently when performing its tasks pursuant to paragraph 3 and shall neither seek nor take instructions from any body.

3. The Cooperation Board shall have the following tasks:

- (a) discussing general policy and strategy of data protection supervision of Europol and the permissibility of the transfer, the retrieval and any communication to Europol of personal data by the Member States;
- (b) examining difficulties of interpretation or application of this Regulation;
- (c) studying general problems relating to the exercise of independent supervision or the exercise of the rights of data subjects;
- (d) discussing and drawing up harmonised proposals for joint solutions on matters referred to in Article 44(1);
- (e) discussing cases submitted by the EDPS in accordance with Article 44(4);
- (f) discussing cases submitted by any national supervisory authority; and
- (g) promoting awareness of data protection rights.

4. The Cooperation Board may issue opinions, guidelines, recommendations and best practices. The EDPS and the national supervisory authorities shall, without prejudice to their independence and each acting within the scope of their respective competences, take the utmost account of them.

5. The Cooperation Board shall meet whenever necessary, and at least twice a year. The costs and servicing of its meetings shall be borne by the EDPS.

6. Rules of procedure of the Cooperation Board shall be adopted at its first meeting by a simple majority of its members. Further working methods shall be developed jointly as necessary.

*Article 46***Administrative personal data**

Regulation (EC) No 45/2001 shall apply to all administrative personal data held by Europol.

## CHAPTER VII

**REMEDIES AND LIABILITY***Article 47***Right to lodge a complaint with the EDPS**

1. Any data subject shall have the right to lodge a complaint with the EDPS if he or she considers that the processing by Europol of personal data relating to him or her does not comply with this Regulation.
2. Where a complaint relates to a decision as referred to in Article 36 or 37, the EDPS shall consult the national supervisory authorities of the Member State that provided the data or the Member State directly concerned. In adopting his or her decision, which may extend to a refusal to communicate any information, the EDPS shall take into account the opinion of the national supervisory authority.
3. Where a complaint relates to the processing of data provided by a Member State to Europol, the EDPS and the national supervisory authority of the Member State that provided the data shall, each acting within the scope of their respective competences, ensure that the necessary checks on the lawfulness of the processing of the data have been carried out correctly.
4. Where a complaint relates to the processing of data provided to Europol by Union bodies, third countries or international organisations, or of data retrieved by Europol from publicly available sources or resulting from Europol's own analyses, the EDPS shall ensure that Europol has correctly carried out the necessary checks on the lawfulness of the processing of the data.

*Article 48***Right to a judicial remedy against the EDPS**

Any action against a decision of the EDPS shall be brought before the Court of Justice of the European Union.

*Article 49***General provisions on liability and the right to compensation**

1. Europol's contractual liability shall be governed by the law applicable to the contract in question.
2. The Court of Justice of the European Union shall have jurisdiction to give judgment pursuant to any arbitration clause in a contract concluded by Europol.

3. Without prejudice to Article 49, in the case of non-contractual liability, Europol shall, in accordance with the general principles common to the laws of the Member States, make good any damage caused by its departments or by its staff in the performance of their duties.
4. The Court of Justice of the European Union shall have jurisdiction in disputes relating to compensation for damage as referred to in paragraph 3.
5. The personal liability of Europol staff vis-à-vis Europol shall be governed by the provisions laid down in the Staff Regulations or in the Conditions of Employment of Other Servants applicable to them.

#### *Article 50*

### **Liability for incorrect personal data processing and the right to compensation**

1. Any individual who has suffered damage as a result of an unlawful data processing operation shall have the right to receive compensation for damage suffered, either from Europol in accordance with Article 340 TFEU or from the Member State in which the event that gave rise to the damage occurred, in accordance with its national law. The individual shall bring an action against Europol before the Court of Justice of the European Union, or against the Member State before a competent national court of that Member State.
2. Any dispute between Europol and Member States over the ultimate responsibility for compensation awarded to an individual in accordance with paragraph 1 shall be referred to the Management Board, which shall decide by a majority of two-thirds of its members, without prejudice to the right to challenge that decision in accordance with Article 263 TFEU.

#### CHAPTER VIII

### **JOINT PARLIAMENTARY SCRUTINY**

#### *Article 51*

### **Joint Parliamentary scrutiny**

1. Pursuant to Article 88 TFEU, the scrutiny of Europol's activities shall be carried out by the European Parliament together with national parliaments. This shall constitute a specialised Joint Parliamentary Scrutiny Group (JPSG) established together by the national parliaments and the competent committee of the European Parliament. The organisation and the rules of procedure of the JPSG shall be determined together by the European Parliament and the national parliaments in accordance with Article 9 of Protocol No 1.
2. The JPSG shall politically monitor Europol's activities in fulfilling its mission, including as regards the impact of those activities on the fundamental rights and freedoms of natural persons.

For the purposes of the first subparagraph:

- (a) the Chairperson of the Management Board, the Executive Director or their Deputies shall appear before the JPSG at its request to discuss matters relating to the activities referred to in the first subparagraph, including the budgetary aspects of such activities, the structural organisation of Europol and the potential establishment of new units and specialised centres, taking into account the obligations of discretion and confidentiality. The JPSG may decide to invite to its meetings other relevant persons, where appropriate;

- (b) the EDPS shall appear before the JPSG at its request, and at least once a year, to discuss general matters relating to the protection of fundamental rights and freedoms of natural persons, and in particular the protection of personal data, with regard to Europol's activities, taking into account the obligations of discretion and confidentiality;
  - (c) the JPSG shall be consulted in relation to the multiannual programming of Europol in accordance with Article 12(1).
3. Europol shall transmit the following documents, for information purposes, to the JPSG, taking into account the obligations of discretion and confidentiality:
- (a) threat assessments, strategic analyses and general situation reports relating to Europol's objective as well as the results of studies and evaluations commissioned by Europol;
  - (b) the administrative arrangements concluded pursuant to Article 25(1);
  - (c) the document containing the multiannual programming and the annual work programme of Europol, referred to in Article 12(1);
  - (d) the consolidated annual activity report on Europol's activities, referred to in point (c) of Article 11(1);
  - (e) the evaluation report drawn up by the Commission, referred to in Article 68(1).
4. The JPSG may request other relevant documents necessary for the fulfilment of its tasks relating to the political monitoring of Europol's activities, subject to Regulation (EC) No 1049/2001 of the European Parliament and of the Council <sup>(1)</sup> and without prejudice to Articles 52 and 67 of this Regulation.
5. The JPSG may draw up summary conclusions on the political monitoring of Europol's activities and submit those conclusions to the European Parliament and national parliaments. The European Parliament shall forward them, for information purposes, to the Council, the Commission and Europol.

#### *Article 52*

### **Access by the European Parliament to information processed by or through Europol**

1. For the purpose of enabling it to exercise parliamentary scrutiny of Europol's activities in accordance with Article 51, access by the European Parliament to sensitive non-classified information processed by or through Europol, upon the European Parliament's request, shall comply with the rules referred to in Article 67(1).
2. Access by the European Parliament to EU classified information processed by or through Europol shall be consistent with the Interinstitutional Agreement of 12 March 2014 between the European Parliament and the Council concerning the forwarding to and the handling by the European Parliament of classified information held by the Council on matters other than those in the area of the common foreign and security policy <sup>(2)</sup>, and shall comply with the rules referred to in Article 67(2) of this Regulation.
3. The necessary details regarding access by the European Parliament to the information referred to in paragraphs 1 and 2 shall be governed by working arrangements concluded between Europol and the European Parliament.

<sup>(1)</sup> Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ L 145, 31.5.2001, p. 43).

<sup>(2)</sup> OJ C 95, 1.4.2014, p. 1.

## CHAPTER IX

## STAFF

*Article 53***General provisions**

1. The Staff Regulations, the Conditions of Employment of Other Servants and the rules adopted by agreement between the institutions of the Union for giving effect to the Staff Regulations and to the Conditions of Employment of Other Servants shall apply to the staff of Europol with the exception of staff who, on 1 May 2017, are employed pursuant to a contract concluded by Europol as established by the Europol Convention without prejudice to Article 73(4) of this Regulation. Such contracts shall continue to be governed by the Council Act of 3 December 1998.

2. Europol staff shall consist of temporary staff and/or contract staff. The Management Board shall be informed on a yearly basis of contracts of an indefinite duration granted by the Executive Director. The Management Board shall decide which temporary posts provided for in the establishment plan can be filled only by staff from the competent authorities of the Member States. Staff recruited to occupy such posts shall be temporary agents and may be awarded only fixed-term contracts, renewable once for a fixed period.

*Article 54***Executive Director**

1. The Executive Director shall be engaged as a temporary agent of Europol under point (a) of Article 2 of the Conditions of Employment of Other Servants.

2. The Executive Director shall be appointed by the Council from a shortlist of candidates proposed by the Management Board, following an open and transparent selection procedure.

The shortlist shall be drawn up by a selection committee set up by the Management Board and composed of members designated by Member States and a Commission representative

For the purpose of concluding a contract with the Executive Director, Europol shall be represented by the Chairperson of the Management Board.

Before appointment, the candidate selected by the Council may be invited to appear before the competent committee of the European Parliament, which shall subsequently give a non-binding opinion.

3. The term of office of the Executive Director shall be four years. By the end of that period, the Commission, in association with the Management Board, shall undertake an assessment taking into account:

(a) an evaluation of the Executive Director's performance, and

(b) Europol's future tasks and challenges.

4. The Council, acting on a proposal from the Management Board that takes into account the assessment referred to in paragraph 3, may extend the term of office of the Executive Director once and for no more than four years.

5. The Management Board shall inform the European Parliament if it intends to propose to the Council that the Executive Director's term of office be extended. Within the month before any such extension, the Executive Director may be invited to appear before the competent committee of the European Parliament.
6. An Executive Director whose term of office has been extended shall not participate in another selection procedure for the same post at the end of the overall period.
7. The Executive Director may be removed from office only pursuant to a decision of the Council acting on a proposal from the Management Board. The European Parliament shall be informed about that decision.
8. The Management Board shall reach decisions regarding proposals to be made to the Council on the appointment, extension of the term of office, or removal from office, of the Executive Director by a majority of two-thirds of its members with voting rights.

#### *Article 55*

### **Deputy Executive Directors**

1. Three Deputy Executive Directors shall assist the Executive Director. The Executive Director shall define their tasks.
2. Article 54 shall apply to the Deputy Executive Directors. The Executive Director shall be consulted prior to their appointment, any extension of their term of office or their removal from office.

#### *Article 56*

### **Seconded national experts**

1. Europol may make use of seconded national experts.
2. The Management Board shall adopt a decision laying down rules on the secondment of national experts to Europol.

## CHAPTER X

### **FINANCIAL PROVISIONS**

#### *Article 57*

### **Budget**

1. Estimates of all revenue and expenditure for Europol shall be prepared each financial year, which shall correspond to the calendar year, and shall be shown in Europol's budget.
2. Europol's budget shall be balanced in terms of revenue and of expenditure.

3. Without prejudice to other resources, Europol's revenue shall comprise a contribution from the Union entered in the general budget of the Union.
4. Europol may benefit from Union funding in the form of delegation agreements or ad hoc grants in accordance with its financial rules referred to in Article 61 and with the provisions of the relevant instruments supporting the policies of the Union.
5. Europol's expenditure shall include staff remuneration, administrative and infrastructure expenses, and operating costs.
6. Budgetary commitments for actions relating to large-scale projects extending over more than one financial year may be broken down into several annual instalments.

#### *Article 58*

#### **Establishment of the budget**

1. Each year the Executive Director shall draw up a draft statement of estimates of Europol's revenue and expenditure for the following financial year, including an establishment plan, and shall send it to the Management Board.
2. The Management Board shall, on the basis of the draft statement of estimates, adopt a provisional draft estimate of Europol's revenue and expenditure for the following financial year and shall send it to the Commission by 31 January each year.
3. The Management Board shall send the final draft estimate of Europol's revenue and expenditure, which shall include a draft establishment plan, to the European Parliament, the Council and the Commission by 31 March each year.
4. The Commission shall send the statement of estimates to the European Parliament and the Council, together with the draft general budget of the Union.
5. On the basis of the statement of estimates, the Commission shall enter in the draft general budget of the Union the estimates that it considers necessary for the establishment plan and the amount of the contribution to be charged to the general budget, which it shall place before the European Parliament and the Council in accordance with Articles 313 and 314 TFEU.
6. The European Parliament and the Council shall authorise the appropriations for the contribution from the Union to Europol.
7. The European Parliament and the Council shall adopt Europol's establishment plan.
8. Europol's budget shall be adopted by the Management Board. It shall become final following the final adoption of the general budget of the Union. Where necessary, it shall be adjusted accordingly.
9. For any building projects likely to have significant implications for Europol's budget, Delegated Regulation (EU) No 1271/2013 shall apply.

*Article 59***Implementation of the budget**

1. The Executive Director shall implement Europol's budget.
2. Each year the Executive Director shall send to the European Parliament and the Council all information relevant to the findings of any evaluation procedures.

*Article 60***Presentation of accounts and discharge**

1. Europol's accounting officer shall send the provisional accounts for the financial year (year N) to the Commission's accounting officer and to the Court of Auditors by 1 March of the following financial year (year N + 1).
2. Europol shall send a report on the budgetary and financial management for year N to the European Parliament, the Council and the Court of Auditors by 31 March of year N + 1.
3. The Commission's accounting officer shall send Europol's provisional accounts for year N, consolidated with the Commission's accounts, to the Court of Auditors by 31 March of year N + 1.
4. On receipt of the Court of Auditors' observations on Europol's provisional accounts for year N pursuant to Article 148 of Regulation (EU, Euratom) No 966/2012 of the European Parliament and of the Council <sup>(1)</sup>, Europol's accounting officer shall draw up Europol's final accounts for that year. The Executive Director shall submit them to the Management Board for an opinion.
5. The Management Board shall deliver an opinion on Europol's final accounts for year N.
6. Europol's accounting officer shall, by 1 July of year N + 1, send the final accounts for year N to the European Parliament, the Council, the Commission, the Court of Auditors and national parliaments, together with the Management Board's opinion referred to in paragraph 5.
7. The final accounts for year N shall be published in the *Official Journal of the European Union* by 15 November of year N + 1.
8. The Executive Director shall send to the Court of Auditors, by 30 September of year N + 1, a reply to the observations made in its annual report. He or she shall also send the reply to the Management Board.
9. The Executive Director shall submit to the European Parliament, at the latter's request, any information required for the smooth application of the discharge procedure for year N, as laid down in Article 109(3) of Delegated Regulation (EU) No 1271/2013.
10. On a recommendation from the Council acting by a qualified majority, the European Parliament shall, before 15 May of year N + 2, grant a discharge to the Executive Director in respect of the implementation of the budget for year N.

<sup>(1)</sup> Regulation (EU, Euratom) 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 and repealing Council Regulation (EC, Euratom) No 1605/2002 (OJ L 298, 26.10.2012, p. 1).



*Article 61***Financial rules**

1. The financial rules applicable to Europol shall be adopted by the Management Board after consultation with the Commission. They shall not depart from Delegated Regulation (EU) No 1271/2013 unless such a departure is specifically required for the operation of Europol and the Commission has given its prior consent.
2. Europol may award grants related to the fulfilment of tasks as referred to in Article 4.
3. Europol may award grants without a call for proposals to Member States for performance of their cross-border operations and investigations and for the provision of training relating to the tasks referred to in points (h) and (i) of Article 4(1).
4. In respect of the financial support to be given to joint investigation teams' activities, Europol and Eurojust shall jointly establish the rules and conditions upon which applications for such support are to be processed.

## CHAPTER XI

**MISCELLANEOUS PROVISIONS***Article 62***Legal status**

1. Europol shall be an agency of the Union. It shall have legal personality.
2. In each Member State Europol shall enjoy the most extensive legal capacity accorded to legal persons under national law. Europol may, in particular, acquire and dispose of movable and immovable property and be a party to legal proceedings.
3. In accordance with Protocol No 6 on the location of the seats of the institutions and of certain bodies, agencies and departments of the European Union, annexed to the TEU and to the TFEU ('Protocol No 6'), Europol shall have its seat in The Hague.

*Article 63***Privileges and immunities**

1. Protocol No 7 on the privileges and immunities of the European Union, annexed to the TEU and to the TFEU, shall apply to Europol and its staff.
2. Privileges and immunities of liaison officers and members of their families shall be subject to an agreement between the Kingdom of Netherlands and the other Member States. That agreement shall provide for such privileges and immunities as are necessary for the proper performance of the tasks of liaison officers.

*Article 64***Language arrangements**

1. The provisions laid down in Regulation No 1 <sup>(1)</sup> shall apply to Europol.
2. The Management Board shall decide by a majority of two-thirds of its members on the internal language arrangements of Europol.
3. The translation services required for the functioning of Europol shall be provided by the Translation Centre for the bodies of the European Union.

*Article 65***Transparency**

1. Regulation (EC) No 1049/2001 shall apply to documents held by Europol.
2. By 14 December 2016, the Management Board shall adopt the detailed rules for applying Regulation (EC) No 1049/2001 with regard to Europol documents.
3. Decisions taken by Europol under Article 8 of Regulation (EC) No 1049/2001 may be the subject of a complaint to the European Ombudsman or of an action before the Court of Justice of the European Union, in accordance with Articles 228 and 263 TFEU respectively.
4. Europol shall publish on its website a list of the Management Board members and summaries of the outcome of the meetings of the Management Board. The publication of those summaries shall be temporarily or permanently omitted or restricted if such publication would risk jeopardising the performance of Europol's tasks, taking into account its obligations of discretion and confidentiality and the operational character of Europol.

*Article 66***Combating fraud**

1. In order to facilitate the fight against fraud, corruption and any other illegal activities under Regulation (EU, Euratom) No 883/2013, Europol shall, by 30 October 2017, accede to the Interinstitutional Agreement of 25 May 1999 between the European Parliament, the Council of the European Union and the Commission of the European Communities concerning internal investigations by the European Anti-Fraud Office (OLAF) <sup>(2)</sup> and shall adopt appropriate provisions applicable to all employees of Europol, using the template set out in the Annex to that Agreement.
2. The Court of Auditors shall have a power of audit, on the basis of documents and on-the-spot checks, over all grant beneficiaries, contractors and subcontractors who have received Union funds from Europol.

<sup>(1)</sup> Regulation No 1 determining the languages to be used by the European Economic Community (OJ 17, 6.10.1958, p. 385/58).

<sup>(2)</sup> OJ L 136, 31.5.1999, p. 15.

3. OLAF may carry out investigations, including on-the-spot checks and inspections, with a view to establishing whether there has been fraud, corruption or any other illegal activity affecting the financial interests of the Union in connection with a grant or a contract awarded by Europol. Such investigations shall be carried out in accordance with the provisions and procedures laid down in Regulation (EU, Euratom) No 883/2013 and in Council Regulation (Euratom, EC) No 2185/96 <sup>(1)</sup>.

4. Without prejudice to paragraphs 1, 2 and 3, working arrangements with Union bodies, authorities of third countries, international organisations and private parties, contracts, grant agreements and grant decisions of Europol shall contain provisions expressly empowering the Court of Auditors and OLAF to conduct the audits and investigations referred to in paragraphs 2 and 3, in accordance with their respective competences.

#### *Article 67*

### **Rules on the protection of sensitive non-classified and classified information**

1. Europol shall establish rules on the obligations of discretion and confidentiality and on the protection of sensitive non-classified information.

2. Europol shall establish rules on the protection of EU classified information which shall be consistent with Decision 2013/488/EU in order to ensure an equivalent level of protection for such information.

#### *Article 68*

### **Evaluation and review**

1. By 1 May 2022 and every five years thereafter, the Commission shall ensure that an evaluation assessing, in particular, the impact, effectiveness and efficiency of Europol and of its working practices is carried out. The evaluation may, in particular, address the possible need to modify the structure, operation, field of action and tasks of Europol, and the financial implications of any such modification.

2. The Commission shall submit the evaluation report to the Management Board. The Management Board shall provide its observations on the evaluation report within three months from the date of receipt. The Commission shall then submit the final evaluation report, together with the Commission's conclusions, and the Management Board's observations in an annex thereto, to the European Parliament, the Council, the national parliaments and the Management Board. Where appropriate, the main findings of the evaluation report shall be made public.

#### *Article 69*

### **Administrative inquiries**

The activities of Europol shall be subject to inquiries by the European Ombudsman in accordance with Article 228 TFEU.

<sup>(1)</sup> Council Regulation (Euratom, EC) No 2185/96 of 11 November 1996 concerning on-the-spot checks and inspections carried out by the Commission in order to protect the European Communities' financial interests against fraud and other irregularities (OJ L 292, 15.11.1996, p. 2).

*Article 70***Headquarters**

The necessary arrangements concerning the accommodation to be provided for Europol in the Kingdom of the Netherlands and the facilities to be made available by the Kingdom of the Netherlands, together with the specific rules applicable there to the Executive Director, members of the Management Board, Europol's staff and members of their families, shall be laid down in a headquarters agreement between Europol and the Kingdom of the Netherlands, in accordance with Protocol No 6.

## CHAPTER XII

**TRANSITIONAL PROVISIONS***Article 71***Legal succession**

1. Europol as established by this Regulation shall be the legal successor in respect of all contracts concluded by, liabilities incumbent upon and properties acquired by Europol as established by Decision 2009/371/JHA.
2. This Regulation shall not affect the legal force of agreements concluded by Europol as established by Decision 2009/371/JHA before 13 June 2016, or of agreements concluded by Europol as established by the Europol Convention before 1 January 2010.

*Article 72***Transitional arrangements concerning the Management Board**

1. The term of office of the members of the Management Board as established on the basis of Article 37 of Decision 2009/371/JHA shall terminate on 1 May 2017.
2. During the period from 13 June 2016 to 1 May 2017, the Management Board as established on the basis of Article 37 of Decision 2009/371/JHA shall:
  - (a) exercise the functions of the Management Board in accordance with Article 11 of this Regulation;
  - (b) prepare the adoption of the rules relating to the application of Regulation (EC) No 1049/2001 with regard to Europol documents as referred to in Article 65(2) of this Regulation, and of the rules referred to in Article 67 of this Regulation;
  - (c) prepare any instrument necessary for the application of this Regulation, in particular any measures relating to Chapter IV; and
  - (d) review the internal rules and measures which it has adopted on the basis of Decision 2009/371/JHA so as to allow the Management Board as established pursuant to Article 10 of this Regulation to take a decision pursuant to Article 76 of this Regulation.

3. The Commission shall without delay after 13 June 2016 take the measures necessary to ensure that the Management Board established pursuant to Article 10 starts its work on 1 May 2017.
4. By 14 December 2016, the Member States shall notify the Commission of the names of the persons whom they have appointed as member and alternate member of the Management Board, in accordance with Article 10.
5. The Management Board established pursuant to Article 10 shall hold its first meeting on 1 May 2017. On that occasion it shall, if necessary, take decisions as referred to in Article 76.

#### *Article 73*

#### **Transitional arrangements concerning the Executive Director, the Deputy Directors and staff**

1. The Director of Europol appointed on the basis of Article 38 of Decision 2009/371/JHA shall, for the remaining period of his or her term of office, be assigned the responsibilities of Executive Director, as provided for in Article 16 of this Regulation. The other conditions of his or her contract shall remain unchanged. If the term of office ends between 13 June 2016 and 1 May 2017, it shall be extended automatically until 1 May 2018.
2. Should the Director appointed on the basis of Article 38 of Decision 2009/371/JHA be unwilling or unable to act in accordance with paragraph 1 of this Article, the Management Board shall designate an interim Executive Director to exercise the duties assigned to the Executive Director for a period not exceeding 18 months, pending the appointment provided for in Article 54(2) of this Regulation.
3. Paragraphs 1 and 2 of this Article shall apply to the Deputy Directors appointed on the basis of Article 38 of Decision 2009/371/JHA.
4. In accordance with the Conditions of Employment of Other Servants, the authority referred to in the first paragraph of Article 6 thereof shall offer employment of indefinite duration as a member of the temporary or contract staff to any person who, on 1 May 2017, is employed under a contract of indefinite duration as a local staff member concluded by Europol as established by the Europol Convention. The offer of employment shall be based on the tasks to be performed by the servant as a member of the temporary or contract staff. The contract concerned shall take effect at the latest on 1 May 2018. A staff member who does not accept the offer referred to in this paragraph may retain his or her contractual relationship with Europol in accordance with Article 53(1).

#### *Article 74*

#### **Transitional budgetary provisions**

The discharge procedure in respect of the budgets approved on the basis of Article 42 of Decision 2009/371/JHA shall be carried out in accordance with the rules established by Article 43 thereof.

#### CHAPTER XIII

#### **FINAL PROVISIONS**

#### *Article 75*

#### **Replacement and repeal**

1. Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA are hereby replaced for the Member States bound by this Regulation with effect from 1 May 2017.

Therefore, Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA are repealed with effect from 1 May 2017.

2. With regard to the Member States bound by this Regulation, references to the Decisions referred to in paragraph 1 shall be construed as references to this Regulation.

*Article 76*

**Maintenance in force of the internal rules adopted by the Management Board**

Internal rules and measures adopted by the Management Board on the basis of Decision 2009/371/JHA shall remain in force after 1 May 2017, unless otherwise decided by the Management Board in the application of this Regulation.

*Article 77*

**Entry into force and application**

1. This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

2. It shall apply from 1 May 2017.

However, Articles 71, 72 and 73 shall apply from 13 June 2016.

This Regulation shall be binding in its entirety and directly applicable in the Member States in accordance with the Treaties.

Done at Strasbourg, 11 May 2016.

*For the European Parliament*

*The President*

M. SCHULZ

*For the Council*

*The President*

J.A. HENNIS-PLASSCHAERT

---

## ANNEX I

## LIST OF FORMS OF CRIME REFERRED TO IN ARTICLE 3(1)

- terrorism,
  - organised crime,
  - drug trafficking,
  - money-laundering activities,
  - crime connected with nuclear and radioactive substances,
  - immigrant smuggling,
  - trafficking in human beings,
  - motor vehicle crime,
  - murder and grievous bodily injury,
  - illicit trade in human organs and tissue,
  - kidnapping, illegal restraint and hostage-taking,
  - racism and xenophobia,
  - robbery and aggravated theft,
  - illicit trafficking in cultural goods, including antiquities and works of art,
  - swindling and fraud,
  - crime against the financial interests of the Union,
  - insider dealing and financial market manipulation,
  - racketeering and extortion,
  - counterfeiting and product piracy,
  - forgery of administrative documents and trafficking therein,
  - forgery of money and means of payment,
  - computer crime,
  - corruption,
  - illicit trafficking in arms, ammunition and explosives,
  - illicit trafficking in endangered animal species,
  - illicit trafficking in endangered plant species and varieties,
  - environmental crime, including ship-source pollution,
  - illicit trafficking in hormonal substances and other growth promoters,
  - sexual abuse and sexual exploitation, including child abuse material and solicitation of children for sexual purposes,
  - genocide, crimes against humanity and war crimes.
-

## ANNEX II

- A. Categories of personal data and categories of data subjects whose data may be collected and processed for the purpose of cross-checking as referred to in point (a) of Article 18(2)
1. Personal data collected and processed for the purpose of cross-checking shall relate to:
    - (a) persons who, in accordance with the national law of the Member State concerned, are suspected of having committed or having taken part in a criminal offence in respect of which Europol is competent, or who have been convicted of such an offence;
    - (b) persons regarding whom there are factual indications or reasonable grounds under the national law of the Member State concerned to believe that they will commit criminal offences in respect of which Europol is competent.
  2. Data relating to the persons referred to in paragraph 1 may include only the following categories of personal data:
    - (a) surname, maiden name, given names and any alias or assumed name;
    - (b) date and place of birth;
    - (c) nationality;
    - (d) sex;
    - (e) place of residence, profession and whereabouts of the person concerned;
    - (f) social security numbers, driving licences, identification documents and passport data; and
    - (g) where necessary, other characteristics likely to assist in identification, including any specific objective physical characteristics not subject to change such as dactyloscopic data and DNA profile (established from the non-coding part of DNA).
  3. In addition to the data referred to in paragraph 2, the following categories of personal data concerning the persons referred to in paragraph 1 may be collected and processed:
    - (a) criminal offences, alleged criminal offences and when, where and how they were (allegedly) committed;
    - (b) means which were or which may have been used to commit those criminal offences, including information concerning legal persons;
    - (c) departments handling the case and their filing references;
    - (d) suspected membership of a criminal organisation;
    - (e) convictions, where they relate to criminal offences in respect of which Europol is competent;
    - (f) inputting party.

These data may be provided to Europol even when they do not yet contain any references to persons.

4. Additional information held by Europol or national units concerning the persons referred to in paragraph 1 may be communicated to any national unit or to Europol, should either so request. National units shall do so in compliance with their national law.
5. If proceedings against the person concerned are definitively dropped or if that person is definitively acquitted, the data relating to the case in respect of which either decision has been taken shall be deleted.



- B. Categories of personal data and categories of data subjects whose data may be collected and processed for the purpose of analyses of a strategic or thematic nature, for the purpose of operational analyses or for the purpose of facilitating the exchange of information as referred to in points (b), (c) and (d) of Article 18(2)
1. Personal data collected and processed for the purpose of analyses of a strategic or thematic nature, for the purpose of operational analyses or for the purpose of facilitating the exchange of information between Member States, Europol, other Union bodies, third countries and international organisations shall relate to:
- (a) persons who, pursuant to the national law of the Member State concerned, are suspected of having committed or having taken part in a criminal offence in respect of which Europol is competent, or who have been convicted of such an offence;
  - (b) persons regarding whom there are factual indications or reasonable grounds under the national law of the Member State concerned to believe that they will commit criminal offences in respect of which Europol is competent;
  - (c) persons who might be called on to testify in investigations in connection with the offences under consideration or in subsequent criminal proceedings;
  - (d) persons who have been the victims of one of the offences under consideration or with regard to whom certain facts give reason to believe that they could be the victims of such an offence;
  - (e) contacts and associates; and
  - (f) persons who can provide information on the criminal offences under consideration.
2. The following categories of personal data, including associated administrative data, may be processed on the categories of persons referred to in points (a) and (b) of paragraph 1:
- (a) personal details:
    - (i) present and former surnames;
    - (ii) present and former forenames;
    - (iii) maiden name;
    - (iv) father's name (where necessary for the purpose of identification);
    - (v) mother's name (where necessary for the purpose of identification);
    - (vi) sex;
    - (vii) date of birth;
    - (viii) place of birth;
    - (ix) nationality;
    - (x) marital status;
    - (xi) alias;
    - (xii) nickname;
    - (xiii) assumed or false name;
    - (xiv) present and former residence and/or domicile;
  - (b) physical description:
    - (i) physical description;
    - (ii) distinguishing features (marks/scars/tattoos etc.);

- (c) means of identification:
  - (i) identity documents/driving licence;
  - (ii) national identity card/passport numbers;
  - (iii) national identification number/social security number, if applicable;
  - (iv) visual images and other information on appearance;
  - (v) forensic identification information such as fingerprints, DNA profile (established from the non-coding part of DNA), voice profile, blood group, dental information;
- (d) occupation and skills:
  - (i) present employment and occupation;
  - (ii) former employment and occupation;
  - (iii) education (school/university/professional);
  - (iv) qualifications;
  - (v) skills and other fields of knowledge (language/other);
- (e) economic and financial information:
  - (i) financial data (bank accounts and codes, credit cards, etc.);
  - (ii) cash assets;
  - (iii) shareholdings/other assets;
  - (iv) property data;
  - (v) links with companies;
  - (vi) bank and credit contacts;
  - (vii) tax position;
  - (viii) other information revealing a person's management of his or her financial affairs;
- (f) behavioural data:
  - (i) lifestyle (such as living above means) and routine;
  - (ii) movements;
  - (iii) places frequented;
  - (iv) weapons and other dangerous instruments;
  - (v) danger rating;
  - (vi) specific risks such as escape probability, use of double agents, connections with law enforcement personnel;
  - (vii) criminal-related traits and profiles;
  - (viii) drug abuse;
- (g) contacts and associates, including type and nature of the contact or association;

- (h) means of communication used, such as telephone (static/mobile), fax, pager, electronic mail, postal addresses, internet connection(s);
  - (i) means of transport used, such as vehicles, boats, aircraft, including information identifying those means of transport (registration numbers);
  - (j) information relating to criminal conduct:
    - (i) previous convictions;
    - (ii) suspected involvement in criminal activities;
    - (iii) modi operandi;
    - (iv) means which were or may be used to prepare and/or commit crimes;
    - (v) membership of criminal groups/organisations and position in the group/organisation;
    - (vi) role in the criminal organisation;
    - (vii) geographical range of criminal activities;
    - (viii) material gathered in the course of an investigation, such as video and photographic images;
  - (k) references to other information systems in which information on the person is stored:
    - (i) Europol;
    - (ii) police/customs agencies;
    - (iii) other enforcement agencies;
    - (iv) international organisations;
    - (v) public entities;
    - (vi) private entities;
  - (l) information on legal persons associated with the data referred to in points (e) and (j):
    - (i) designation of the legal person;
    - (ii) location;
    - (iii) date and place of establishment;
    - (iv) administrative registration number;
    - (v) legal form;
    - (vi) capital;
    - (vii) area of activity;
    - (viii) national and international subsidiaries;
    - (ix) directors;
    - (x) links with banks.
3. 'Contacts and associates', as referred to in point (e) of paragraph 1, are persons through whom there is sufficient reason to believe that information which relates to the persons referred to in points (a) and (b) of paragraph 1 and which is relevant for the analysis can be gained, provided they are not included in one of the categories of persons referred to in points (a), (b), (c), (d) and (f) of paragraph 1. 'Contacts' are those persons who have a sporadic contact with the persons referred to in points (a) and (b) of paragraph 1. 'Associates' are those persons who have a regular contact with the persons referred to in points (a) and (b) of paragraph 1.

In relation to contacts and associates, the data referred to in paragraph 2 may be stored as necessary, provided there is reason to assume that such data are required for the analysis of the relationship of such persons with persons referred to in points (a) and (b) of paragraph 1. In this context, the following shall be observed:

- (a) such relationship shall be clarified as soon as possible;
  - (b) the data referred to in paragraph 2 shall be deleted without delay if the assumption that such relationship exists turns out to be unfounded;
  - (c) all data referred to in paragraph 2 may be stored if contacts or associates are suspected of having committed an offence falling within the scope of Europol's objectives, or have been convicted for the commission of such an offence, or if there are factual indications or reasonable grounds under the national law of the Member State concerned to believe that they will commit such an offence;
  - (d) data referred to in paragraph 2 on contacts, and associates, of contacts as well as on contacts, and associates, of associates shall not be stored, with the exception of data on the type and nature of their contact or association with the persons referred to in points (a) and (b) of paragraph 1;
  - (e) if a clarification pursuant to the previous points is not possible, this shall be taken into account when a decision is taken on the need for, and the extent of, data storage for further analysis.
4. With regard to a person who, as referred to in point (d) of paragraph 1, has been the victim of one of the offences under consideration or who, on the basis of certain facts there is reason to believe could be the victim of such an offence, the data referred to in point (a) to point (c)(iii) of paragraph 2 as well as the following categories of data may be stored:
- (a) victim identification data;
  - (b) reason for victimisation;
  - (c) damage (physical/financial/psychological/other);
  - (d) whether anonymity is to be guaranteed;
  - (e) whether participation in a court hearing is possible;
  - (f) crime-related information provided by or through persons referred to in point (d) of paragraph 1, including where necessary information on their relationship with other persons, for the purpose of identifying the persons referred to in points (a) and (b) of paragraph 1.

Other data referred to in paragraph 2 may be stored as necessary, provided there is reason to assume that they are required for the analysis of a person's role as victim or potential victim.

Data not required for any further analysis shall be deleted.

5. With regard to persons who, as referred to in point (c) of paragraph 1, might be called on to testify in investigations in connection with the offences under consideration or in subsequent criminal proceedings, data referred to in point (a) to point (c)(iii) of paragraph 2 as well as categories of data complying with the following criteria may be stored:
- (a) crime-related information provided by such persons, including information on their relationship with other persons included in the analysis work file;
  - (b) whether anonymity is to be guaranteed;
  - (c) whether protection is to be guaranteed and by whom;
  - (d) new identity;
  - (e) whether participation in a court hearing is possible.

Other data referred to in paragraph 2 may be stored as necessary, provided there is reason to assume that they are required for the analysis of such persons' role as witness.

Data not required for any further analysis shall be deleted.

6. With regard to persons who, as referred to in point (f) of paragraph 1, can provide information on the criminal offences under consideration, data referred to in point (a) to point (c)(iii) of paragraph 2 as well as categories of data complying with the following criteria may be stored:
- (a) coded personal details;
  - (b) type of information supplied;
  - (c) whether anonymity is to be guaranteed;
  - (d) whether protection is to be guaranteed and by whom;
  - (e) new identity;
  - (f) whether participation in a court hearing is possible;
  - (g) negative experiences;
  - (h) rewards (financial/favours).

Other data referred to in paragraph 2 may be stored as necessary, provided there is reason to assume that they are required for the analysis of such persons' role as informant.

Data not required for any further analysis shall be deleted.

7. If, at any time during the course of an analysis, it becomes clear on the basis of serious and corroborating indications that a person should be included in a category of persons, as defined in this Annex, other than the category in which that person was initially placed, Europol may process only the data on that person which is permitted under that new category, and all other data shall be deleted.

If, on the basis of such indications, it becomes clear that a person should be included in two or more different categories as defined in this Annex, all data allowed under such categories may be processed by Europol.

---



Европейски парламент Parlamento Europeo Evropský parlament Europa-Parlamentet Europäisches Parlament  
Euroopa Parlament Ευρωπαϊκό Κοινοβούλιο European Parliament Parlement européen Parlaimint na hEorpa  
Europski parlament Parlamento europeo Eiropas Parlaments Europos Parlamentas Európai Parlament  
Parlament Ewropew Europees Parlement Parlament Europejski Parlamento Europeu Parlamentul European  
Európsky parlament Evropski parlament Euroopan parlamentti Europaparlamentet



parleu2018bg.bg

Parliamentary Dimension  
Bulgarian Presidency of the Council  
of the European Union

# **RULES OF PROCEDURE OF THE JOINT PARLIAMENTARY SCRUTINY GROUP ON EUROPOL**

## **PREAMBLE**

The Joint Parliamentary Scrutiny Group on Europol, having regard to:

- Article 88 of the Treaty on the Functioning of the European Union,
- Protocol No 1 to the Treaties on the Role of National Parliaments in the European Union,
- Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol), hereinafter referred to as the “Europol Regulation”, applicable as of 1 May 2017,

and in accordance with the Conclusions of the Conference of Speakers of the European Union Parliaments at its meetings of 22-24 May 2016 in Luxembourg and of 23-24 April 2017 in Bratislava,

Adopted these Rules of Procedure on 19 March 2018 in Sofia, Bulgaria.

## **ARTICLE 1: TASKS AND COMPETENCE**

The tasks and competence of the Joint Parliamentary Scrutiny Group are enshrined in the Europol Regulation, in particular in Article 51.

## **ARTICLE 2: COMPOSITION**

### *2.1 Members*

- (a) Each national Parliament of a Member State applying the Europol Regulation shall be represented by a maximum of four members in the JPSG. In the case of bicameral parliaments

each Chamber shall have the right to nominate up to two members to the JPSG. The European Parliament shall be represented by a maximum of 16 members in the JPSG.<sup>1</sup>

The number of members nominated by each Parliament/Chamber shall not affect the equality of Parliaments/Chambers. Each Parliament/Chamber may nominate substitute members to replace full members in case of absence.

(b) Members of the JPSG shall be selected individually by each Parliament/Chamber, bearing in mind the necessity to ensure substance matter expertise as well as long-term continuity. Where possible, members of the JPSG shall be nominated for the duration of their parliamentary mandate.

## *2.2 Observers*

The JPSG shall invite, to all its meetings, observers from the list of EU Member States that have concluded an Agreement on Operational and Strategic Cooperation with Europol.

The JPSG may also decide to invite, on an ad hoc basis and for specific points on the agenda, observers from the list of international organisations or third countries with which Europol has concluded agreements.

Observers shall not have the right to take part in the decision-making.

## *2.3 Representatives of Europol, guests and experts*

Pursuant to the Europol Regulation, and in particular Article 51, the Chairperson of the Management Board, the Executive Director or their Deputies, and the European Data Protection Supervisor (EDPS) shall appear before the JPSG at its request. The JPSG may decide, where appropriate, to invite to its meetings guests and experts with experience relevant to its competence and tasks.

# **ARTICLE 3: PRESIDENCY AND MEETINGS**

## *3.1 Presidency*

The JPSG shall be presided jointly by the Parliament of the Member State holding the rotating presidency of the Council of the European Union and the European Parliament, the latter represented by the Chair of the competent committee (Co-Chairs).

When the Parliament of the Member State holding the rotating presidency of the Council of the European Union is not taking part in the Europol Regulation, the JPSG shall be presided jointly by the Parliament of the Member State previously holding the rotating presidency of the Council of the European Union and the European Parliament.

---

<sup>1</sup> This shall be without prejudice to the transferability of seats between chambers of a parliament, when agreed.

### *3.2 Presidential Troika*

The Presidential Troika of the JPSG shall consist of the heads of delegations of the current, preceding and following Presidency Parliaments and of the European Parliament.

### *3.3 Secretariat*

The JPSG Secretariat shall be provided by the Presidential Troika. The Secretariat shall assist the Co-Chairs and Presidential Troika in their respective tasks and competences. It shall also fulfil administrative tasks i.a. prepare and communicate the documents for each meeting to JPSG members.

### *3.4 Frequency and place of meetings*

The JPSG shall meet twice a year. In the first half of the year, the JPSG shall meet in the Parliament of the Member State holding the rotating presidency of the Council of the European Union. In the second half of the year, the JPSG shall meet in the European Parliament in Brussels.

### *3.5 Extraordinary meetings*

If necessary, extraordinary meetings can be convened upon agreement of the Parliament of the Member State holding the rotating presidency of the Council of the European Union and the European Parliament, or upon agreement by at least one third of the Parliaments/Chambers, to address matters of urgency or matters that cannot be reasonably included in the agenda of the ordinary meetings. The date and venue of extraordinary meetings shall be decided jointly by the JPSG Co-Chairs.

### *3.6 Subgroups*

The JPSG may establish subgroups where necessary to fulfil its tasks. The mandate, role, scope, objectives and working methods of the subgroup shall be set on an ad hoc basis. All JPSG members shall have the right to join such subgroups.

## **ARTICLE 4: PROCEEDINGS AND LANGUAGES**

### *4.1 Conduct of meetings*

(a) At the beginning of each meeting, the Co-Chairs shall present the draft agenda and submit it for adoption by the JPSG. They shall also determine the order and the length of interventions.

(b) As a general rule, the meetings of the JPSG are public and shall be conducted in full transparency.

(c) Notwithstanding point b), the JPSG may hold in camera meetings when the nature of the information to be discussed so requires.

(d) A presence register of the Members and participants shall be established during each meeting.



(e) The JPSG shall adopt its decisions, in principle, by consensus.

#### *4.2. Right to ask questions*

Members of the JPSG may address both oral and written questions to Europol. Written questions may also be asked outside the meeting framework and independently of items listed on the agenda and shall be answered within an appropriate timeframe. The questions shall reflect the mandate of the JPSG as defined in Regulation (EU) 2016/794 (Europol Regulation). These questions shall be relayed to Europol after their admissibility has been checked by the Co-Chairs and the question is deemed to be in line with the Europol regulation. A further written reply can be requested in case the answer to an oral question is deemed insufficient.

#### *4.3 Working languages*

The working languages of the JPSG shall be English and French. Documents published by the JSPG shall be communicated to the national Parliaments and the European Parliament in English and French.

#### *4.4 Interpretation*

(a) Meetings held at the Parliament of the Member State holding the presidency of the Council of the European Union (1st semester): Simultaneous interpretation from and into English and French, as well as from and into the language(s) of the Member State of the EU Council Presidency shall be provided by the Presidency Parliament. Simultaneous interpretation into additional languages may be provided if requested. Parliaments are entitled to bring their own interpreters or request them from the Presidency Parliament at their own expense. The Presidency Parliament shall make available the appropriate technical facilities.

(b) Meetings held at the European Parliament (2nd semester): Simultaneous interpretation from and into all EU languages shall be provided.

#### *4.5 Documents*

Documents originating from Europol that are relevant to or requested by the JPSG pursuant to Article 51 (4) of the Europol Regulation, are to be addressed to each national parliament and the European Parliament. The respective parliaments will bear the responsibility to forward the received documents to the appointed JPSG Members.

#### *4.6 Documentation of the meetings*

##### *4.6.1. Agenda of the meeting*

A draft agenda shall be drawn up by the Presidential Troika and shall be communicated, by the Co-Chairs, to all participating parliaments no later than eight (8) weeks prior to each meeting. The agenda shall only include matters relating to the scrutiny of Europol, in line with the tasks and competence of the JPSG as set out in the Europol Regulation.

#### 4.6.2. Other documents

Prior to each meeting, delegations may send any documents relating to items of the agenda to the Co-Chairs. Each delegation shall be responsible for translating any document, which it submits to the JPSG into English and/or French.

The Presidential Troika may also draw up discussion documents.

#### 4.6.3. Requests to Europol for providing documents

In accordance with Article 51 (4) of the Europol Regulation the JPSG may request other relevant documents necessary for the fulfilment of its tasks relating to the political monitoring of Europol's activities. Any JPSG parliamentary delegation may submit such a written request to the Co-Chairs. Documents shall be provided in accordance with Article 64 of the Europol Regulation.

#### 4.7. *Conclusions*

In accordance with Article 51 (5) of the Europol Regulation, the JPSG may draw up summary conclusions on the outcome of the JPSG meetings relating to the political monitoring of Europol's activities. The Presidential Troika shall draft an initial proposal. The Co-Chairs shall submit these draft conclusions to the JPSG for approval. Parliaments/Chambers shall have the right to propose amendments. Parliaments/Chambers wishing to put forward a specific point of view, may present observations which shall be annexed to the conclusions. The European Parliament shall forward the adopted conclusions, for information purposes, to the Council, the Commission and Europol.

### **ARTICLE 5: REPRESENTATIVE TO THE MANAGEMENT BOARD OF EUROPOL**

The JPSG shall appoint, from its full Members, a representative who will be entitled to attend, in accordance with Article 14 of the Europol Regulation and for a duration determined by the JPSG, meetings of the Management Board of Europol as a non-voting observer. The representative shall report back to the JPSG after each meeting of the Management Board on his/her main findings in writing.

### **ARTICLE 6: FINAL PROVISIONS**

#### *6.1 Entry into force of the Rules of Procedure*

These Rules of Procedure are drawn up in a single original in English and French, each of these texts being equally authentic. Translations into the other official languages of the European Union shall be the responsibility of the relevant Parliaments. The Rules of Procedure shall enter into force on the date of their adoption.

## *6.2. Revision*

In line with the recommendations of the EU Speakers Conference of 23-24 April 2017 in Bratislava, the JPSG shall make a review of its Rules of Procedure, two years after its constituent meeting, and submit the conclusions from such a review to the Presidency of the Conference of Speakers of the European Union Parliaments.

Sofia, 10 May 2018

## **Summary conclusions by the Co-Chairs**

On 18 and 19 March 2018, the Bulgarian Parliament and the European Parliament (EP) jointly organised the 2nd meeting of the Joint Parliamentary Scrutiny Group (JPSG) in Sofia, Bulgaria. The meeting was co-chaired by Tsvetan TSVETANOV, Chair of the Committee on Internal Security and Public Order of the National Assembly of the Republic of Bulgaria and Head of the Bulgarian Delegation to the Joint Parliamentary Scrutiny Group and Claude MORAES, Chair of the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament and Head of the EP delegation to the JPSG.

The JPSG meeting was attended by over 130 members of 27 national parliaments and 9 members of the European Parliament.

In line with the JPSG's tasks and responsibilities as set out in the Europol Regulation ((EU) 2016/794), the agenda included an exchange of views on the 2019-2021 Europol Multiannual Work Programme, an exchange of views with the Chairperson of the Europol Management Board and the European Data Protection Supervisor, as well as thematic discussions on cooperation with the Western Balkans, illegal content online and cybersecurity, and the fight against terrorism and organised crime.

## **Exchange of views and adoption of the Rules of Procedure**

The JPSG debated the compromise proposal for the Rules of Procedure, as drafted by the Co-Chairs prior to the JPSG Meeting. The compromise text was based on feedback received after the Co-Chairs held an extensive set of bilateral meetings with those delegations that had tabled amendments before the JPSG constituent meeting or had expressed doubts regarding certain points. The compromise proposal reflects a strong role for national parliaments, through the Presidential Troika, notably in the agenda



setting, the preparation of discussion documents, the secretariat and the drafting of meeting conclusions of the Joint Parliamentary Scrutiny Group. The text also gives delegations the possibility to effectively contribute to the agenda and the scrutiny findings. It warrants the right to ask questions while guaranteeing their quality control and ensuring a workable scenario for Europol and its services. A review clause was inserted and the text foresees the possibility to set up subgroups where the participation of all chambers and parliaments in the scrutiny activity is ensured. This compromise proposal was adopted on 19 March, by consensus, in line with the Speakers' Conference Conclusions of 24 April 2017.

Further to the adoption of the JPSG Rules of Procedure and to the meeting held on 18 March between the JPSG Co-Chairs, the Europol Rapporteur and the Danish Parliament delegation, the Co-Chairs announced the agreement reached on setting up a JPSG working group on the representation of Denmark in JPSG meetings. The working group will be composed of the Presidential Troika and the Danish Parliament and deliver recommendations ahead of the revision of the JPSG Rules of Procedure scheduled for October 2019 (as provided for under Article 6 paragraph 2 thereof).

Further to the adoption of the JPSG Rules of Procedure, the Polish delegation reiterated the need for the new European Union's Multiannual Financial Framework to take due consideration of the necessity of adequate financing for Europol to be able to translate its documents in all EU languages.

### **Past and future EUROPOL cooperation with the Western Balkan countries**

Presentations were made by Oldrich MARTINU (Deputy Executive Director Governance of EUROPOL) and Vladimir REBIC (General Police Director of Republic of Serbia), followed by a debate with the JPSG members.



Focus was put by Mr MARTINU on the fact that the Western Balkan region is a transit and destination area of several types of illicit goods, as well as an area of origin of some property and violent crimes, production of illicit drugs and smuggling of goods. Migrant smuggling was named as one of the major problems; despite the decrease of transits detected, the region remains one of the key secondary transit routes to the EU. Organised property crime remains an issue in this region; the crime rate remains high and so is the number of Balkan groups that are involved in property crime on European territory. Europol also identifies a growing trend in cybercrime. Radicalisation and recruitment remain a problem, however to a lesser extent than in previous years. By now, around 800 persons have travelled from the Balkan countries to the conflict zones of Syria and Iraq to join ISIS.

Mr MARTINU also highlighted that Europol has set up supporting operations to tackle main criminal activities, for example drugs, smuggling, weapons as well as counterterrorism. All Western Balkan countries have concluded and ratified operation agreements with Europol and posted or are about to post liaison officers in The Hague. Nevertheless, there is a need for further strengthening the cooperation. The pilot project on deployment of Europol liaison officers to the Western Balkan should be a priority.

Mr REBIC presented Serbia's experience on cooperation with Europol and other Western Balkan countries. He highlighted Serbia has had an operational agreement with Europol since June 2014. Serbia has actively participated together with countries of the region and EU member countries in more than 17 police operations against all types of crime, especially to combat of migrant smuggling, arms smuggling and cybercrime. Serbia shall continue to follow the priorities of Policy Cycle 2018-2021. Europol offers significant support to regional activities, strengthening cooperation, especially in the field of counterterrorism. Serbia has provided a national FTF list and also agrees that this list should be provided to the Schengen system in order to strengthen the security of the EU in the fight against terrorism. The migration routes along the Western Balkans could have been taken advantage of by terrorists in order to reach countries they consider interesting for potential attacks. However, thanks to the important cooperation between Western Balkan countries, this significant flow of illegal immigrants has been stopped. However, one should remain cautious and therefore cooperation to exchange information



with Europol is required. Serbia is willing to fully contribute to ensure stability and security through extensive cooperation with all partners.

The presentations were followed by an exchange of views with the JPSG Members. In particular, representatives of the Spanish, Cypriot, French, and Slovenian national parliaments took the floor.

### **Multiannual programming document 2019-2021 Europol**

A presentation was made by Mr Rob WAINWRIGHT, Executive Director of Europol. The multiannual programming document is comprised of three main elements, namely the strategic objectives based on a three-year program, a resource program and an external strategy. Two major objectives can be identified: on the one hand how to deal with the increase of information exchange and secondly to provide the most effective operational support, especially in the areas of organised crime, cybercrime and terrorism. To achieve this, Europol improves its core IT systems in order to be a principal provider of information exchange; over 1000 law enforcement agencies are now cooperating on the Europol channel. Looking at 2019 and beyond, Europol will further invest in technology and business innovation to try and increase the means by which it can deal with the significant expansion in information sharing. The last nine years, the amount of information sharing that Europol is now dealing with has experienced a nine-fold increase. To cope with this growth, Europol has to continuously invest in innovation and technology.

The second strategic goal is the provision of operational support and expertise to Member States' investigations. Last year, Europol supported around 1500 high-level operations.

Europol also aims to remain an efficient organisation with effective governance arrangements and with a positive reputation. Mr WAINWRIGHT welcomed the parliamentary scrutiny by JPSG as a means for Europol to project its image in a better and more transparent way.



Mr WAINWRIGHT expressed concern about Europol's IT information technology capability. Although there have been important increases to budget and resources, these increases have gone directly to operational areas. Europol was not able to adjust the capabilities of, for example, the IT department. IT support is the frontline area of Europol's work and is needed to maintain Europol's core business of sharing information.

The presentation was followed by an exchange of views with the JPSG members, including representatives of the Belgian and Greek national parliaments as well as Members of the European Parliament.

JPSG members expressed concern over information-sharing between Member States as 85% of Europol's data originates from 5 Member States. The importance of funding was also highlighted as Europol receives half the size of Frontex's budget, for example. Members also addressed the strategy for relations with international organisations and third countries - including Europol's cooperation with Libya - and stressed that checks on the quality of information, data protection of personal data of EU citizens, etc. should be ensured. Other topics raised included Brexit, hotspot locations, interoperability of IT systems, the possible need for a European TFTP (Terrorist Finance Tracking) Programme and the future and current role of Europol in developing participation in EU operations and missions and further exploring the potential for deploying staff to delegation missions outside the EU.

Mr WAINWRIGHT confirmed Member States are aware of the funding needs, through the Europol Management Board representatives, but this understanding does unfortunately not materialize at the political level of the Council. The realities of fixing the EU budget as a whole tend to have the effect of pushing down the demands of Europol. This is more a question of the Ministries of Finance in Member States than the Ministries of Security and Justice. More funding is needed to be able to pay more attention to other topics such as child sex exploitation. But it is also needed to attract the best people from the technology sector.





On the issue of relations with third countries, Mr WAINWRIGHT highlighted the global dimension of national security threats. This leads to Europol establishing a global information exchange network and the legal basis has to adjust to that. However, there are important differences in sharing data within the EU and outside. There are obvious challenges about how to strike agreements with third countries that would serve the operational requirements of Europol but at the same time still meet the EU data protection demands. Mr WAINWRIGHT confirmed that Europol liaison officers could be stationed in EU delegations.

A European TFTP equivalent is needed according to Mr WAINWRIGHT. Currently, the TFTP programme excludes the possibility to monitor terrorist financial tracking within the EU and this needs to be changed in the future. Furthermore, Europol and EU law enforcement should not be fragmented. Europol has an interest in ensuring that the instruments built will be maintained in the future, even after Brexit.

### **Europol Management Board - Update on the work of the Europol Management Board, with special focus on the Europol External Strategy 2017-2020**

Mr Priit PÄRKNA, Chairperson of the Europol Management Board, presented the activities of the Europol Management Board. His presentation focussed on the following subjects: interoperability of EU information systems, the 2019-2021 Multiannual Programming Document and the Europol external strategy. Europol's external relations are governed by the new Europol Regulation (article 23 - 25). In addition to setting up international agreements to exchange personal data with third countries, the Europol Management Board encourages the expansion of liaison offices attached to Europol. The number of liaison offices already increased from 55 in 2017 to 68 currently. On the 13<sup>th</sup> of December 2017, the Europol Management Board adopted the list of priority partners, which reflects the growing need to establish partnerships with the MENA region.

A representative of the European Parliament delegation enquired about the envisaged international agreement with Israel.



## **Exchange of views with European Data Protection Supervisor - 'EDPS supervision of Europol: 2017 activities and ongoing work '**

Mr Giovanni BUTARELLI, European Data Protection Supervisor, presented in a video message the outcome of the first year of the supervision of Europol. An in-depth exchange of views with Wojciech WIEWIOROWSKI, European Data Protection Assistant Supervisor, followed.

The JPSG's essential role in politically monitoring Europol's activities and the support the EDPS will provide the JPSG in its tasks were mentioned. Focussing on accountability, cooperation with national supervisory authorities, and an innovative approach, in 2017 the EDPS established effective working relationships with the Europol staff, organised operational visits to its premises, and had regular contacts with Europol's Data Protection Function team. The EDPS held exchanges on Europol's portfolio existing operational analysis projects for each of which Europol must define the specific purpose, the categories of data and the individuals involved, the participants, how long the data will be stored and the conditions for access, transfer or use of the data concerned

The first Europol Opinion on Europol's Integrated Data Management Concept (IDMC) Guidelines was published in 2017. It clarifies the procedures according to which Europol must carry out all future processing of personal data and addressed the different purposes for which Europol can carry out simultaneous data processing for operational and for strategic analysis. Europol was commended for its prompt implementation of the recommendations contained in the opinion, and its general positive approach on scrutiny.

The EDPS carried out its first inspection of Europol in 2017, aimed to check on the implementation of the Joint Supervisory Body's pending recommendations and assess Europol's level of compliance with the new legal framework. The legal part the inspection focused on Europol's data lifecycle, while the technical one focused on the audit of the Information Security Management Programme applied by Europol.



In 2017 the EDPS received 3 prior consultations, required whenever a new data processing activity involves the processing of sensitive data or might present a specific risk to individuals. It received 2 complaints, one of which was deemed admissible. In 2017 several meetings of the Cooperation Board composed of representatives from the relevant national DPAs and the EDPS were held. In its exchanges with the Europol Management Board the EDPS called for a data protection approach based on accountability and for the use of risk assessments.

Other points raised in the presentation concerned: the effective cooperation with national DPAs and the importance of joint inspections, the EDPS recent opinion on 8 negotiating mandates to conclude international agreements allowing the exchange of data between Europol and third countries, the impact of the application of the GDPR, the need for the EU to develop appropriate legislation on ePrivacy to complement the GDPR, as well as to finalise the regulation on data protection in the EU institutions encompassing both the administrative and operational data, and the upcoming launch of the European Data Protection Board. The upcoming challenges of making Europol a hub for the exchange of information in the EU and of the interoperability of large scale info systems were also discussed.

Representatives of the European Parliament and French and Cypriot national intervened in the ensuing debate.

The discussion revolved around the negotiation and conclusion of cooperation agreements with third countries, the need for a differentiated approach and for guarantees that such agreements are not instrumentalised. The purpose limitation and purpose specification of data transfers by Europol and the specific restrictions on the processing of information transferred by Europol were also mentioned. The need to ensure the right balance between security and privacy when dealing with data processing for the purpose of law enforcement was underlined.



## **Countering illegal content online and optimizing cybersecurity: Europol's Cybercrime Centre and the EU Internet Referral Unit**

Mariya GABRIEL (Commissioner for Digital Economy and Society) outlined the Commission's response to illegal content online as set out in its Communication of September 2017 and Recommendation of March 2018.

She explained that the latest set of operational measures to be taken by companies and Member States apply to all forms of illegal content online and aim to ensure faster detection and removal of illegal content online, and to reinforce the cooperation between companies, trusted flaggers and law enforcement authorities. The recommendations build on the on-going voluntary initiatives, such as the EU Internet Forum on terrorist content online, and the Code of Conduct on Countering Illegal Hate Speech Online. There are specific provisions to further curb terrorist content online, such as the 'one-hour rule': enabling the removal by companies of terrorist content in the first hours of its appearance online within one hour from its referral. In addition to referrals, internet companies should use automated detection, to swiftly remove terrorist content and stop it from reappearing once it has been removed. To assist smaller platforms with more limited resources and expertise, companies should share and optimise appropriate technological tools.

Fast-track procedures should be put in place to process referrals, and Member States were urged to ensure the necessary capabilities and resources to detect and refer terrorist content, as well as to report on a regular basis to the Commission on referrals.

The need for a clear definition of "illegal online content" and for deepening cooperation with national authorities, the EU institutions and agencies, and private companies was underlined. The successful cooperation between Europol and ENISA, or between the Computer Emergency Response Team for the EU Institutions, bodies and agencies (CERT-EU) with other CERTs in the Members States and with specialised IT security companies were mentioned. A Memorandum of understanding ENISA, EDA, EC3, and CERT-EU is under negotiation. Setting up a Network of Cybersecurity



Competence Centres and a European Cybersecurity Research and Competence Centre in 2018, which would collaborate with all EU agencies with tasks in the area of cybersecurity, remains a priority.

Sir Julian KING (Commissioner for the Security Union) gave a brief overview of the evolving on-line security threats to Europe's citizens, businesses and public and democratic institutions and the need for the EU to create an effective EU cyber deterrence and criminal law response.

He presented the Cybersecurity Package which is building EU resilience, via a strong EU Cybersecurity Agency which will ensure sharing of threat intelligence, help implement the Directive on the Security of Network and Information Systems, and the EU-wide certification framework for cyber secure products and services. Stepping up the EU's cybersecurity capacity by setting up the European Cybersecurity Research and Competence Centre and help develop the technology needed to keep up with an ever-changing threat, was also mentioned. Creating an effective criminal law response focusing on detection, traceability and the prosecution of cyber criminals remains a priority; it includes a Directive on combating fraud and counterfeiting of non-cash means of payment, proposals to facilitate cross-border access to electronic evidence, reflections on the role of encryption in criminal investigations.

While stressing that there should be no trade-off between online safety and fundamental rights, the Commissioner called for a joint approach at policy and operational level and commended Europol and the European Cybercrime Centre (EC3), for its activity and its role of facilitator of private-public cooperation in this field.

Rob WAINWRIGHT (Executive Director, Europol) gave an overview of Europol's activities on cybercrime and the work of the European Cybercrime Centre, a leading international law-enforcement centre which engages with the large private tech firms and with the banking sector. He pointed to the trends of cybercrime, namely the growing number of ransomware attacks, enabled by the exploitation of crypto currencies, as well as data breaches and their impact on critical infrastructure. The infrastructure of cyber criminality on the dark web, the blend of cybercriminal capability



with that of state actors were also mentioned. A trend towards more aggressive and direct targeting against states, critical infrastructure, banking, highest profile organisations or high, net worth individuals.

In 2018 the impact of the GDPR and the Directive on security of network and information systems will impose on companies and critical services minimum standards of cyber security. The response trend was improved due to legislative and policy action at national and mostly at the EU level on e-evidence, encryption, and the emergency protocol for coordinating law-enforcement response. Europol wants to act as an international centre of expertise in this field; it is also active in countering the evolving threat of terrorism contents online, via its European Union Internet Referral Unit. Europol is also taking an intelligence-based approach to identify how the of eco system of online terrorism functions, in cooperation with platforms and national counterparts. Pilot projects on improving automatic detection capability are currently ongoing.

Members of the Polish, Greek, French, Dutch, Austrian, UK national parliaments and European Parliament took the floor in the subsequent debate.

The following issues were discussed: Europol's cooperation with third countries and international organisations; the calendar and necessary resources for ensuring the interoperability of large-scale databases set up at EU level to deal with migration, asylum and internal security; the need to ensure that security is at the service of freedom and avoid the risk or arbitrary law-enforcement in the referrals process, via a possible role of judicial authority on determining if content is illegal; possible new prevention measures or legal instruments to remove illegal content in real time and address swiftly the ever-evolving cyber threats; the need for a strategy to prevent cyber-attacks, and for a less fragmented approach in addressing cyber threats stemming from the dark net, the Internet of things, the need to ensure more flexible working structures, endowed with substantial resources; cooperation with trust flaggers and smaller platforms; a possible EU strategy for countering cyber threats to democratic institutions; the gaps in the current anti-money laundering regime and the lack of regulation of crypto currencies; the role of national parliaments in pushing governments to step up cooperation on cyber security;





possible measures to mitigate the impact of artificial intelligence on labour markets.

### **Europol's contribution to the fight against terrorism and the prevention of organised crime:**

Sir Julian KING (Commissioner for the Security Union) explained in his address how the EU could support national action in the field of prevention, protection and response to transnational security threats. He underlined Europol's essential role in providing operational support in this field, as outlined in the Commission's comprehensive assessment.

Closing down the space in which terrorists operate, by making harder for them to access money, fire arms, explosives, strengthen control of terrorists' travel, disrupt networks, get the best of existing information systems, to develop new ones like the planned European Travel Information and Authorisation System or ensuring the interoperability of systems. Work was undertaken to better protect public spaces, in cooperation with all relevant stakeholders and Europol. Via its IRU Europol helped tackling radicalization on the online platforms and shared its expertise.

The Commissioner mentioned the upcoming package of new measures for combating terrorism, on explosive precursors, firearms, terrorism financing, the security of ID cards, and better and faster access to electronic evidence. The work of the European Counter-Terrorism Centre was commended and the increasing engagement of member States was welcomed.

Given the link between terrorism and organised crime, the Commission will continue to support Member States help to fight organised crime, with the help of Europol, in the current policy cycle (2018-2021) with 10 priority areas among which the fight against illicit fire arm trafficking or the fight against against drug trafficking. Crime prevention is included as a horizontal priority in the current policy cycle.



Rob WAINWRIGHT (Executive Director of Europol) underlined the complexity of the terrorist threats, the issue of foreign fighters and the emergence of stronger crime and terrorist networks. In his view, beyond the traditional response based on the institutional and intelligence community, it is necessary to turn to the broader capabilities of the police community and increased information sharing. On organised crime, he referred to: drug trafficking and the need for better partnerships among Member States; trafficking of human beings, migrants' smuggling, exploitation of unaccompanied minors by crime syndicates which required closing the gaps on intelligence sharing; the need to fight fake and counterfeit market in the technology space; environmental crime; money laundering where the remaining problem is minor confiscation of freezing of proceeds of crime. He praised the work of national liaison officers, a successful integrated team effort for operational success.

Members of the French, Irish, Spanish, Portuguese, Belgian, Bulgarian national parliaments and European Parliament took the floor in the subsequent debate. The issues raised included: the action of national Parliaments to encourage governments to support the work of Europol and share more information; a joint strategy for combatting terrorism and organised crime and a mandate for the EPPO; the fight against the illegal tobacco trade; possible ways to increase freezing of assets; the risk of overlapping between the actions of Frontex and Europol, the need to engage with diplomatic actors for access to information; the exchange on best practices on radicalization and return of foreign fighters; the possible improvements to the money laundering regime; the impact on the EU of attacks in third countries which are EU neighbours.

### **Conclusions and closing of the meeting by the Co-Chairs**

In their concluding remarks, the Co-Chairs welcomed the adoption of the Rules of Procedure of the JPSG. The Presidential Troika will set up a working group with the Danish Parliament in order to come up with recommendations on Denmark's status, before the 2019 general review of the RoP. The summary conclusions of the 2nd JPSG meeting will mention the importance of linguistic diversity and of the necessary resources enabling Europol to provide documents in additional languages. The Presidential Troika will draw up guidelines for the procedure for questions to Europol and launch a debate on





parleu2018bg.bg  
Parliamentary Dimension  
Bulgarian Presidency of the Council  
of the European Union



the topics for which subgroups could be established. Delegates were invited to send written contributions on the Europol multi-annual programme, ahead of the September meeting of the JPSG.

Next meeting will take place on 24 and 25 September 2018 at the European Parliament in Brussels.

Claude MORAES

Chair of the Committee on Civil Liberties,  
Justice and Home Affairs

Tsvetan TSVETANOV

Head of the Bulgarian  
Delegation to the Joint  
Parliamentary Scrutiny Group