BRIEFING

European Parliament

Europol: The EU law enforcement cooperation agency

SUMMARY

Evolving from informal police cooperation in the 1970s to a fully fledged European Union (EU) agency with a strengthened mandate under its new legal basis (Regulation (EU) 2016/794), Europol's mandate is to strengthen EU Member States' competent authorities and ensure their cooperation for the purpose of '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'. The agency is therefore empowered to tackle more than 30 forms of serious crime and related criminal offences, including terrorism, drug trafficking, money laundering, human trafficking, sexual abuse and exploitation, trafficking in arms and ammunition. To fulfil its objectives, Europol carries out a series of tasks, including the core activities of performing as the EU criminal information exchange hub and providing operational support and expertise to Member States' criminal investigations.

To frame Europol's activities, the Europol Regulation strengthens its data management and data protection rules and provides for enhanced scrutiny: political scrutiny – by a new parliamentary oversight body made up of representatives of the European Parliament and Member States' national parliaments; and scrutiny of its data processing operations – by the European Data Protection Supervisor. Furthermore, the Regulation reforms the framework for Europol's cooperation with partners such as third countries and international organisations, which also allows for an increased role for the Commission and the European Parliament.

On the occasion of Europol's 20th anniversary, this briefing provides a timeline of the agency's establishment and consolidation; an overview of its competences, structure and functioning under the current legal framework; as well as some elements related to further developments.

In this Briefing

EPRS | European Parliamentary Research Service

Author: Carmen-Cristina Cîrlig
Members' Research Service

PE 640.162 – September 2019

EN

Introduction

Headquartered in The Hague, in the Netherlands, the European Union Agency for Law Enforcement Cooperation (Europol) is an EU body tasked with supporting and strengthening cooperation between EU Member States (MS) in the area of cross-border law enforcement. On 1 July 2019, Europol celebrated the 20th anniversary of its operations, following the October 1998 entry into force of the Europol Convention. However, Europol's roots go back to informal police cooperation in the 1970s, from which it evolved into a fully fledged EU agency with a strengthened mandate under its new legal basis (Regulation (EU) 2016/794).

From informal cooperation to EU agency

The origins of EU cooperation in the area of police and criminal law dates back to the 1976 'Trevi' Group. Established to address the challenge of terrorism in Europe, the group later expanded cooperation to tackle other forms of crime, such as drug trafficking and illegal immigration. Composed of representatives of the interior and justice ministries from the 12 European Economic Community Member States, the 'Trevi' group was an informal, intergovernmental structure formed outside the Community framework.

Eventually, a German proposal to set up a European police entity was agreed at the December 1991 European Council meeting. Subsequently, the 1992 Treaty of Maastricht established police cooperation on combatting terrorism, drug trafficking and other serious forms of international crime as a matter of common interest to the EU. This cooperation would be supported by an EU-wide system for information exchange within a European Police Office, under the EU's intergovernmental 'third pillar' (Justice and Home Affairs). While waiting for the adoption of an intergovernmental convention on Europol and its ratification, a ministerial agreement established the Europol Drug Unit (EDU), Europol's predecessor, in June 1993. Its mandate was limited to combating drug trafficking, and associated criminal organisations and money laundering, through data exchange between Member States' national authorities, data analysis and coordination of the investigative activities of national law enforcement authorities. The EDU lacked a central database and could not store personal data, therefore information was exchanged bilaterally between Member States' liaison officers on the basis of national legislation. Two Council Joint Actions, in 1995 and 1996, expanded EDU's mandate to cover trafficking in nuclear and radioactive substances, clandestine immigration networks, illicit vehicle trafficking, human trafficking, and sexual abuse of children. In 1995, the EU Member States signed the Europol Convention replacing the EDU with the European Police Office. Moreover, the 1997 Treaty of Amsterdam emphasised Europol's role in the 'collection, storage, processing, analysis and exchange of relevant information, including information held by law enforcement services on reports on suspicious financial transactions', and provided for further increases in cooperation through Europol within five years of the Treaty's entry into force.

Following the October 1998 entry into force of the Europol Convention and the adoption of other necessary measures, Europol began operations on 1 July 1999. The new body was given a mandate 'in preventing and combating terrorism, unlawful drug trafficking and other serious forms of international crime where there are factual indications that an organized criminal structure is involved and two or more MS are affected by the forms of crime in question', a mandate which was to be accomplished progressively in the following years. Illegal money laundering in connection to the crimes covered and associated offences were also included in Europol's activities. The Annex to the Convention included the list of crimes Europol could deal with, which the Council of the EU could expand, acting unanimously. The Convention was complemented by a Protocol on its interpretation by the Court of Justice by way of preliminary rulings (1996), and another on privileges and immunities for Europol staff (1997). Another three Protocols were adopted (entering into force in 2007) that: extended Europol's mandate to include tackling certain money laundering offences (2000); allowed Europol to take part in Joint Investigation Teams (JITs) and to ask Member States to

initiate investigations (2002); further clarified Europol's mandate and set the rules for concluding operational agreements with third countries, including the exchange of personal data (2003).

The Convention tasked Europol with: facilitating the exchange of information between Member States; obtaining and analysing information and intelligence; notifying the competent national authorities through the national units (i.e. contact points) of any information concerning them and forwarding any information relevant to national investigations; and maintaining a computerised system of collected information. The latter would comprise an information system, containing data provided by Member States in accordance with their national law and by third parties, as well as thematic work files for the purposes of analysis. In 2005, the Europol Information System (EIS) was created to include data on persons suspected of crimes or likely to commit crimes falling under Europol competence, on crimes committed and the means used, and on convicted persons. The analysis work files (AWFs), set up to support criminal investigations, included a wider array of data than the EIS (e.g. data on victims or witnesses). Europol was also tasked with developing specialist knowledge of national investigative procedures, providing strategic intelligence and preparing general situation reports.

The long process of national ratification determined the EU Member States to replace the Convention and its protocols with a Council decision that would be easier to amend. Therefore, in April 2009, following a Commission proposal and a Parliament opinion, the Council adopted Decision 2009/371/JHA establishing the European Police Office (Europol), under the EU's third pillar on police and judicial cooperation in criminal matters. It entered into force on 1 January 2010. Europol consequently became an EU body, funded by the EU general budget, thereby increasing the role of the EP through its budgetary powers. Moreover, the scope of the crimes within Europol's mandate was broadened, by removing the necessity for a link with organised crime. The Council decision also institutes the obligation for Europol to issue threat assessments and strategic analysis; and expands the data categories permitted in EIS. The structure of cooperation, based on liaison officers at Europol and national units, was maintained.

Following the Lisbon Treaty's entry into force, Europol is now governed by Article 88 of the Treaty on the Functioning of the EU (TFEU). The article defines Europol's mission and provides that regulations adopted jointly by the Parliament and the Council under the ordinary legislative procedure are to determine the agency's structure, operation and tasks. Moreover, it highlights two types of tasks for Europol: a) collection, storage, processing, analysis and exchange of information; and b) the coordination, organisation and implementation of operative action carried out jointly with the Member States, including on the basis of JITs. The European Parliament will, together with national parliaments, scrutinise Europol's activities. While not an immediate obligation, the Europol Decision was replaced by the Europol Regulation, adopted on 11 May 2016 jointly by the EP and the Council.[1] The Regulation applied from 1 May 2017 for all EU countries, except Denmark, which has an opt-out from the Treaty's justice and home affairs provisions.[2] The Regulation enhances Europol's role as a central hub for information exchange; sets more flexible rules for setting up specialised units or centres dealing with certain types of crime; strengthens Europol's data management and protection regime; and creates a new parliamentary oversight body, the Joint Parliamentary Scrutiny Group. The Regulation also reforms the way Europol exchanges information with its partners. Finally, it provides for individuals' right of access to their personal data, a complaints procedure, and a right to obtain compensation for unlawful data processing.

Organisational structure and oversight

Governance

Europol's administrative and management structure consists of a Management Board, an Executive Director and other advisory bodies that may be set up by the Management Board.

Management Board

Europol's Management Board is a policy and decision-making body. The Board comprises one representative from each Member State, plus one representative from the European Commission, with a four-year (renewable) mandate. A chair and deputy chair are elected from the three Member States making up the 18-month Council Presidency trio, and they hold these positions for that period, unless their membership of the Management Board ends beforehand. The Europol Regulation also envisages that the principle of balanced gender representation is taken into account; as of July 2019, women represented 20.7 % of Board members (including alternates).

The Board defines the strategic direction of Europol and oversees the implementation of its tasks; it decides on the internal rules of the agency, in terms of financial and human resources or additional data protection guidelines, and it has the power to set up other internal structures (e.g. centres of specialised expertise). It also adopts an annual consolidated report on Europol's activities, which is sent to the European Parliament, Council, Commission, the Court of Auditors and national parliaments by 1 July of the following year. The Board takes decisions by a majority of its members, with some exceptions, when a two-thirds majority is required, e.g. the yearly adoption of Europol's multiannual programming and its annual work programme for the following year; the adoption of Europol's annual budget and other budget-related functions; the election of the chair and deputy chair of the Management Board; and the proposals (to the Council) on the appointment, extension of the term of office, or removal of the Executive Director of Europol.

Executive Director

The Executive Director of Europol is the agency's legal representative and responsible for its operations. The Executive Director should act independently in the performance of his/her duties, although accountable to the Management Board. The Executive Director is appointed for a four-year term, renewable once, by the Council (JHA), after receiving the Board's opinion. Three Deputy Executive Directors are appointed in accordance with the same procedure (after consulting the Executive Director). Before the appointment (or renewal of the term of office), the candidate may be invited to appear before the EP committee responsible, which gives a non-binding opinion. Since May 2018, Europol's Executive Director is Catherine De Bolle (Belgium).[3] Three Deputy Directors manage the Operations, Governance and Capabilities Directorates respectively.

Europol staff and budget

In December 2018, Europol counted 1 294 staff members, including liaison officers from Member States and other partners (243 liaison officers), seconded national experts, trainees and contractors. Europol's allocated budget in 2019 is €138.3 million, an increase of €8 million compared to 2018. Europol expects its budget to increase in time, as it predicts a need for more resources.

Specialised centres or units

A number of centres focused on specific crime challenges have been set up at Europol.

The European Cybercrime Centre (EC3) was created in 2013, to become a focal point in the fight against cybercrime in the EU. It currently focuses on cyber-dependent crime, online child sexual exploitation and payment fraud. The EC3 publishes the annual Internet Organised Crime Threat Assessment report on developments in cybercrime. The EC3 also relies on the work of the Joint Cybercrime Action Taskforce and the Cyber Intelligence Team set up at EC3. Since May 2018, a Europol Dark Web Team within the EC3 coordinates efforts in fighting criminality on the dark web.

The European Counter-Terrorism Centre (ECTC), set up in 2016, is designed as a central EU hub in the fight against terrorism. It acts as an information centre for intelligence and expertise sharing; provides operational support to Member States in investigations following terrorist attacks; and tackles the challenges of foreign fighters and illegal arms trafficking. Through the EU Internal Referral Unit (EU IRU, 2015), currently based at the ECTC, Europol has a role in detecting,

investigating and requesting the removal of terrorist/violent extremist content online (and content used by smuggling networks). The EU IRU also provides strategic and operational analysis.

Also set up in 2016, the European Migrant Smuggling Centre (EMSC), helps police and border authorities to coordinate complex cross-border anti-smuggling operations. It is incorporated in the European Serious Organised Crime Centre (ESOCC), which supports Member States in fighting drug trafficking, facilitation of illegal immigration, organised theft and burglary, trafficking in human beings, excise fraud, firearms trafficking, document fraud, financial and environmental crime.

The Intellectual Property Crime Coordinated Coalition (IPC3), was launched in 2016 in cooperation with the EU Intellectual Property Office and supports law enforcement and partners in fighting counterfeiting and piracy offline and online.

Cooperation between Member States and Europol

Each Member State establishes or designates a Europol National Unit (ENU), which acts as the liaison body between Europol and the competent national authorities; Member States may also allow direct contact between Europol and the national authorities, on condition that Europol shares the information exchanged in this way with the ENU. Each ENU designates at least one liaison officer to be attached to Europol and represent the ENU within the agency. The ENU is responsible for transmitting the relevant information to Europol; responding to Europol's requests for information; ensuring effective communication and cooperation between Europol and national authorities; and raising awareness about Europol activities. The relationship between ENUs and Europol is governed by national law. There are three exceptions to the ENUs' sharing of information with Europol if it would: run contrary to the Member State's security interests; jeopardise an ongoing investigation or endanger an individual; or if the information relates to intelligence activities in the field of national security. Liaison officers are also subject to national law, except when the Regulation provides otherwise. Their main task is to ensure the exchange of information between their Member State and liaison officers from other EU countries, third countries and international organisations. Bilateral exchanges may involve crimes beyond the scope of Europol's mandate.

Scrutiny of Europol

European Data Protection Supervisor (EDPS)

The EDPS (the EU's independent data protection authority) monitors Europol's data processing activities and ensures they comply with the Regulation's provisions on the protection of the fundamental rights and freedoms of individuals regarding the processing of their personal data. The EDPS oversight of Europol's data processing includes: conducting enquiries; investigating complaints; monitoring and ensuring the application of the Regulation's data provisions; and advising Europol on all data protection matters. In addition, the EDPS may order the agency to rectify, erase or destroy unlawfully processed personal data or order a ban on unlawful processing operations. It may also refer a matter to the Commission, Council, Parliament and Court of Justice of the EU (CJEU). The Europol Regulation also institutes a Cooperation Board, made up of the EDPS and a representative from the supervisory authority of each Member State. The national supervisory authority is responsible for the supervision, in accordance with national law, of data input, retrieval and communication by the Member State to Europol, as well as of the activities of the ENU and the liaison officers. The Cooperation Board has an advisory role and, among other tasks, may issue guidelines, recommendations and best practices.

Data protection

The Europol Regulation institutes a number of safeguards to protect the rights of individuals over their personal data. Firstly, processing of data by Europol must comply with general data protection principles (fair and lawful processing of data; accuracy and security of data; purpose limitation, etc.). The processing (and transfer) of certain categories of personal data (e.g. relating to witnesses or victims of criminal offences or to minors under 18; as well as data revealing racial or ethnic origin, genetic data, etc.) is allowed only if strictly necessary and proportionate for preventing and combating crime covered by Europol's mandate. Europol must also store data for a limited period of time; data are to be erased automatically after three years, unless a justified decision is taken regarding continued storage. Europol is obliged to keep records of all personal data operations and also to notify any breach of personal data to the EDPS and the national competent authorities, as well as to individual persons under certain conditions. Importantly, the Regulation provides for specific individual rights: the right of access to personal data held by Europol and the right to rectification, erasure and restriction; the right to lodge a complaint with the EDPS and to a judicial remedy against the EDPS before the CJEU; and the right to receive compensation for damage resulting from an unlawful data processing operation. A data protection officer, appointed from Europol staff (four-year term) and acting independently, must ensure Europol's compliance with the Regulation's provisions on personal data.

Joint Parliamentary Scrutiny Group

The Europol Regulation establishes a Joint Parliamentary Scrutiny Group (JPSG), made up of representatives of the European Parliament and of the national parliaments, to monitor the activities of Europol politically, both with regard to the accomplishment of its tasks and to the impact of its activities on individuals' fundamental rights and freedoms. Article 51 of the Regulation sets out the tasks and powers of the JPSG. It may request the chair of the Management Board, the Executive Director or their deputies to appear before the JPSG, while the EDPS must appear before the JPSG at its request and at least once a year. The JPSG also has the right to be consulted regarding the multiannual programming of Europol and the right to request any documents from Europol for the fulfilment of its tasks. It may also draw up conclusions on the political scrutiny of Europol. Finally, the Management Board may invite a JPSG representative to its meetings as observer. In October 2018, the Board decided to invite the JPSG representative to attend two Board meetings per year concerning items for which the JPSG's opinion was deemed relevant.

The JPSG has a maximum of 4 members from each EU national parliament and a maximum of 16 Members of the European Parliament. It meets twice a year, in the country holding the Council Presidency and in the European Parliament. It adopted its rules of procedure in March 2018. The EP hosts it on 23-24 September 2019.

Europol competences and tasks

Article 3 of the Europol Regulation sets the agency's objectives, namely to strengthen action by the Member States' competent authorities and ensure their cooperation for the purpose of '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'. In this respect, the Europol Regulation broadened the agency's mandate to 30 forms of crime which are listed in its Annex I.[4] In addition, Europol is competent for the related criminal offences (crimes committed to obtain the means of perpetrating the acts under Europol's mandate; crimes aimed at facilitating or perpetrating those acts for which Europol is competent; and crimes committed to ensure impunity for perpetrators of the crimes in Annex I). In order to fulfil its objectives, Europol can perform a series of tasks, including:

- Collecting, storing, processing, analysing and exchanging data, including criminal intelligence, as well as notifying the Member States via the ENUs of any information about criminal activities concerning them.
- Supporting national investigations, through joint action with the national competent authorities or within a JIT, also in cooperation with Eurojust where appropriate. Europol

participates in JITs and may propose the establishment of a JIT, and may also request national authorities initiate investigations into crimes under its mandate.

- Preparing threat assessments, strategic and operational analyses and general situation reports. Europol publishes annual reports providing strategic assessments of emerging threats and trends and key developments in the area of terrorism (TE-SAT), serious and organised crime and cybercrime (IOCTA). Based on the Serious and Organised Crime Threat Assessment (SOCTA), the Council decides EU priorities for the fight against organised and serious international crime. Moreover, the annual Europol review summarises the developments of the previous year in the crime areas Europol covers. Europol also issues early warning and intelligence notifications.
- Developing specialist knowledge of crime prevention methods, investigative procedures, forensic methods, etc.; organising and supporting training activities.
- Cooperating with other EU bodies (e.g. European Anti-Fraud Office (OLAF), EU Agency for Law Enforcement Training (CEPOL), Eurojust) through exchange of information and providing them with analytical support; cooperating with EU crisis management structures and missions, within the scope of Europol's objectives.
- Supporting Member States' action to combat crimes facilitated or perpetrated using the internet; cooperating with MS to refer content to internet service providers.
- Acting as the central office for combating euro counterfeiting.

Nevertheless, Europol does not have coercive powers (e.g. to make arrests), which remain the exclusive competence of national authorities. Any operational action by Europol on the territory of a Member State must be carried out in liaison and with the agreement of that country.

The Europol Strategy 2016-2020 sets three strategic goals for the agency: to be the EU criminal information hub; to provide the most effective operational support and expertise for Member States; and to run an efficient organisation with effective governance and positive reputation. The Europol Programming documents 2018-2020 and 2019-2021 incorporate the three strategic goals and break them down into multi-annual objectives. The new Europol Strategy 2020+ sets five strategic goals: to be the EU criminal information hub; to deliver agile operational support; to provide a platform for European policing solutions; to be at the forefront of law enforcement innovation and research; and to act as the model EU law enforcement organisation. The multiannual strategic objectives corresponding to the 2020+ Strategy are being developed in 2019.

The next sections focus on Europol's core activities and efforts to consolidate the agency's role as an indispensable actor of EU and international law enforcement cooperation.

Information exchange and analysis

Europol's priority is to consolidate its position as the EU criminal information exchange hub; it currently focuses on three strands of efforts regarding its information management capabilities: building Europol's new information architecture based on the concept of integrated data management and on the EU interoperability solutions recently agreed; providing fast and reliable first-line response; and enhancing partnerships to develop a comprehensive intelligence picture.

Processing information

The Europol Regulation moves away from the previous 'silo' based approach, whereby data are stored in separate databases governed by specific rules (which led to such problems as missing links between crimes, or data duplication), to the purpose limitation approach, whereby personal data may be processed for specific purposes and are limited to the minimum necessary.

Prior to the Regulation, Europol relied on databases – the Europol Information System (EIS) and the Analysis Work Files (AWFs) – each with a different purpose and regulated by specific data provisions. Analysts therefore could not link the data stored in the AWFs to EIS data. The 23 initial AWFs were eventually merged into 2 files, on organised crime and on terrorism, but the inability to link the data in the two files (except

through 'hit/no hit') persisted. Focal Points were created within the AWFs to focus on a specific phenomenon, from a commodity, regional or thematic angle. The Regulation aimed to remove these obstacles, to foster information sharing and set data processing rules that facilitate analysts' tasks.

The Regulation provides that Europol will only process information shared with the agency by Member States in accordance with their national law; by other EU bodies, third countries and international organisations; and by private parties and private persons. Europol can also process information from publicly available sources. According to the purpose limitation principle, data sent by Member States to Europol are still subject to national decision-making, as countries decide on the type and scope of information shared, as well as on its onward transfer to other parties. The same is valid for data provided to Europol by international organisations, EU bodies and third countries.

Moreover, the Regulation establishes **the only purposes** for which Europol may process information, including personal data, are: cross-checking aimed at identifying connections or other links between information related to suspected or convicted persons for a crime falling under the competence of Europol (or persons it is believed, on factual and reasonable grounds, will commit such a crime); carrying out strategic, thematic or operational analyses; and facilitating information exchange between Member States, Europol, other EU bodies, third countries and international organisations. The Europol Regulation further specifies that data processing for the purpose of operational analysis (i.e. linked to an investigation) must be performed by means of analysis projects (formerly Focal Points), governed by a number of safeguards: for each Analysis Project (AP) the Europol Executive Director defines the specific purpose, the categories of personal data and of data subjects; the participants, the storage and conditions of access; the transfer and use of the data. If the personal data appear relevant to another operational AP, further processing may be allowed under conditions of necessity and proportionality. However, these safeguards do not apply to data processing for strategic or thematic analyses, as it is more difficult to define the data that will be required beforehand; the general requirement to document any data processing operation applies.

The Europol Regulation also defines the **access to information** stored by Europol. Without prejudice to any restrictions on the data and only in relation to the crimes covered by the Europol Regulation and the European Arrest Warrant Framework Decision, Member States have access and may search all information for the purpose of cross-checking to identify connections between information related to convicted or suspected persons (or where it is believed an individual will commit a crime) and for the purpose of strategic and thematic analysis; they have only indirect access ('hit/no hit') to the information provided for operational analysis. If there is a hit, Europol starts the procedure to share the information after agreement from the provider of the data. Secondly, authorised Europol staff have access to Europol information to the extent required for the performance of their duties. Eurojust and OLAF may also have indirect access to Europol information to cross check to identify links; strategic and thematic analyses and operational analyses. This is only allowed to check if information stored at Eurojust and OLAF matches information processed at Europol. As mentioned, Europol is also under a duty to notify Member States without delay of any information concerning them. If such information is restricted, Europol must ask the data provider for authorisation to share; however, Europol may disregard the restrictions if sharing the data is absolutely necessary to prevent an imminent threat to life.

The Europol Programming Document 2019-2021 emphasises the concept of integrated data management (IDMC) as the expression of the purpose limitation principle. Europol will continue to implement the IDMC by modernising its systems architecture, through adapting the EIS and developing innovative ICT solutions. The integration of data will ensure that links across crime areas will be identified faster and thus increase the value of analytical products. The EU-wide efforts to ensure the interoperability of EU border and security information systems will be an important factor behind the design of Europol's information architecture.

Under the new rules on interoperability (in this context Europol's cooperation with eu-LISA is essential), Europol data will be searchable through a European Search Portal and a shared biometric matching service. At the same time, under specific EU laws, Europol obtains access to various databases such as the Entry/Exit

System, the Visa Information System, the European Travel Information and Authorisation System (ETIAS) and Eurodac (fingerprints database), for the sole purpose of checking whether data on a specific person are present, following which a request for full access may be made. Europol also gets access to ECRIS-TCN for the purpose of identifying the Member State holding criminal record information on a third-country national, as well as to Passenger Name Records (PNR) or the result of PNR data processing on a case-by-case basis and within the limits of its competences. Under the new rules on the Schengen Information System, Europol (authorised staff) will be able to access all categories of data in the SIS and to exchange supplementary information with Member States; moreover, Member States must inform Europol of any hits when a person is sought in relation to a terrorist offence. Regarding Prüm information (DNA, fingerprint and vehicle registration data) Europol has sought the possibility to cross-match data with third countries with which there is an operational agreement.

On the practical exchange of information, Europol maintains a non-stop operational centre to ensure uninterrupted receipt, processing and availability of information. Since 2017, a non-stop counter-terrorism service is also available. SIENA, the agency's secure communication network, can be used to exchange information between EU law enforcement agencies, as well as some Europol partners. The exchanges may concern information falling exclusively under Europol's mandate, as well as bilateral or multilateral communication between Member States outside the scope of Europol's mandate. Since January 2016, FIU.net (a computer network supporting the Financial Intelligence Units in the EU mandated to fight money laundering and financing of terrorism) was incorporated into Europol. In October 2017, Europol also launched SIRIUS, a web platform supporting Member States' investigations in the field of internet-facilitated crime, in particular through sharing knowledge, best practices and expertise, with special focus on counter-terrorism.

Europol will further cooperate with Member States to increase the quality and speed of their information exchange; it also plans to invest more in standardisation, automation of cross-matching and optimisation of information flows. Finally, in relation to the challenges posed by new technologies, Europol is analysing and implementing measures relating, for example, to the development of its own decryption capabilities to support Member States' investigations, as well as the establishment of an encryption observatory function to assess the technical and legal developments in this area.

Relations with partners

In the performance of its mandate, Europol has been exchanging security and intelligence information with a series of external partners. The Europol Regulation confirms Europol's competence to 'establish and maintain cooperative relations with Union bodies ..., the authorities of third countries, international organisations and private parties', but reforms the way Europol cooperates with partners, in particular as regards the transfer of personal data, and by enhancing the role of the Commission and the European Parliament.

The previous Europol Convention and Europol Council decision also provided for cooperation with EU entities, third countries and international organisations. EU bodies (Eurojust; OLAF; the European Agency for the Management of Operational Cooperation at the External Borders (Frontex); CEPOL, etc.) could conclude an agreement or working arrangement with Europol that could include the exchange of operational, strategic or technical information, including personal data and classified information. Prior to the Europol Regulation's entry into force, the following agreements were concluded **with EU entities** (N.B. unlike operational agreements, strategic agreements did not allow for the transfer of personal data): strategic agreements with the European Commission (administrative agreement, 2003), OLAF (administrative agreement, 2004), CEPOL (2007), European Centre for Disease Prevention and Control (2011), EU Intellectual Property Office (2013), EU Agency for Network and Information Security (ENISA, 2014), European Central Bank (2014), European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA, 2016); and operational agreements with Eurojust (2010) and Frontex (2015).

Prior to the Regulation, Europol could only conclude strategic and operational agreements with **third countries** and **international organisations** with Council approval (a list was adopted by the Council by qualified majority vote, after consulting the EP). Strategic agreements were concluded with Russia (2003), Turkey (2004), United Arab Emirates (2016), China (2017), Brazil (2017), United Nations Office on Drugs and Crime (UNODC, 2004), and the World Customs Organization (2002). Operational agreements were concluded with Iceland (2001), Norway (2001), the United States of America (2001), Serbia (2004), Switzerland (2004), Australia (2007), Colombia (2010), Monaco (2011), Albania (2013), Canada, North Macedonia, Liechtenstein (2013), Moldova (2014), Montenegro (2014), Ukraine (2016), Bosnia and Herzegovina (2016), Georgia (2017), and Interpol (2001).

Denmark and Europol

Due to its opt-out from EU justice and home affairs legislation, Denmark, lacking any possibility to opt in, could not cooperate with Europol under the new Regulation. The EU therefore designated Denmark a third country only for the purpose of concluding a cooperation agreement. On 29 April 2017, the Agreement on operational and strategic cooperation between Denmark and Europol was officially signed, and entered into force on 30 April 2017. Under its terms, Denmark benefits from closer cooperation with Europol as regards access to the databases than true third countries, albeit this access is conditional on Denmark's continued EU membership and participation in the Schengen area. Moreover, Denmark must implement Directive (EU) 2016/680 (the Police Data Protection Directive) in its national law, and agree to CJEU jurisdiction and the competence of the EDPS. Denmark obtained observer status (no voting rights) on Europol's Management Board, but lost direct access to the Europol databases, although Europol is obliged to notify Denmark 'without delay of any information concerning it'. Denmark takes no part in the Cooperation Board on data protection, but is an observer to the JPSG. The Commission must evaluate this agreement by 31 October 2020, after which, it may recommend to the Council (by 30 April 2021), to replace it with an international agreement under Article 218 TFEU.

The Europol Regulation brought several changes to this area. Firstly, Europol may directly (without an agreement) exchange information, except personal data, with EU bodies, third countries and international organisations and private parties, if relevant to its tasks. This could also happen on the basis of working arrangements (excluding personal data). Such working arrangements have been concluded with Israel (2018); Japan (2018); New Zealand (2019); the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA, 2018); and EUNAVFOR MED Operation Sophia (2018). As regards cooperation with private parties, by July 2019, more than 60 Memoranda of Understanding had been concluded, with others under consideration. The Regulation also includes a general ban on processing information obtained in clear violation of human rights.

Secondly, as regards personal data transfers, Europol is allowed to transfer personal data to an EU body when necessary for the performance of their respective tasks. Importantly, personal data exchange with **third countries** and **international organisations** will no longer be based on operational agreements concluded by Europol, but on the basis of either:

- an **adequacy decision** by the Commission adopted in accordance with Article 36 of the 2016 Police Data Protection Directive finding that the third country or the international organisation ensures an adequate level of data protection;
- an **EU international agreement** concluded on the basis of Article 218 TFEU (i.e. the Commission recommends the opening of negotiations with the third party, and if the Council approves the mandate, the Commission negotiates the agreement; Parliament must give consent to the conclusion of such agreements).

Europol may also conclude administrative arrangements to implement the adequacy decisions or the international agreements concluded.

Europol **operational agreements concluded prior to 1 May 2017** remain in force as the basis for exchanging personal data with the countries and organisations concerned; however the Commission must evaluate these agreements by 14 June 2021, after which it may recommend the opening of negotiations for an EU international agreement to replace the existing provisions.

Exceptionally (absent one of the above legal bases), the Executive Director of Europol may authorise a personal data transfer to third countries and international organisations, solely on a case-by case basis and under certain conditions, e.g. the data transfer is necessary to protect the vital interests of a person; or to prevent an immediate and serious threat to the public security of a Member State or third country; or to prevent, detect, or prosecute a criminal offence in individual cases. The Management Board, with the EDPS's agreement, may authorise personal data transfers, under specific conditions, for a maximum of one year (renewable).

So far, no EU international agreement has been concluded with a third country on the basis of the Europol Regulation. In December 2017, the Commission recommended to the Council the opening of negotiations with eight Middle Eastern and North African countries: Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia and Turkey. The Council authorised the negotiating mandates on 4 June 2018, and negotiations have started with some of these countries.

Third countries and international organisations may send liaison officers to Europol. Currently, Europol hosts liaison officers from 41 countries, as well as Eurojust and Interpol.

Finally, the Regulation's provisions on **the exchange of personal data with private parties** offer new possibilities for cooperation. These include the ability to receive (bulk) personal data from private parties, as long as Europol only processes it to identify the Member State concerned. The data transfers between Europol and private parties are therefore indirect, via a Member State national unit or via third countries' or international organisations' contact points. Europol may however send personal data to private parties in individual cases, where it is necessary and in the interest of the data subject, for the prevention of imminent crime or, if it is publically available, for any reason to combat cybercrime. The practice of direct exchanges of personal data with private parties should be the subject of an evaluation by the Commission, which has launched the procedures for a study on the issue. In the meantime, the Council continues to reflect on Europol's cooperation with private parties, in the context of the changing operational environment for EU law enforcement. Europol's increased needs for cooperation with service and internet providers are highlighted, as is a greater focus on preventing and tackling organised crime activities online. Against this background, the lack of possibilities for Europol to exchange data directly is beginning to be seen as a shortcoming of the current legislative framework, particularly as regards cybercrime investigations, and the investigation of terrorism and terrorist financing.

Operational support and expertise

Another core purpose of Europol is to support Member States' investigations into crimes covered by Europol's mandate, including through high-quality analytical support. The framework within which Europol acts consists of various policy documents, particularly the 2015 European Agenda on Security and the EU Policy Cycle for Serious and Organised Crime. Currently Europol's priority areas for operational support and expertise are aligned to the European Agenda on Security: serious and organised crime (including migrant smuggling), cybercrime and terrorism.

In the area of serious and organised crime, Europol's support for Member States focuses on the priorities identified in the EU Policy Cycle 2018-2021: fighting Mafia-type organised groups; increasing operational support through the European Migrant Smuggling Centre, including deploying operational and analytical support to migration hotspots; and using EU IRU expertise to identify online content on the provision of irregular migration, to refer it for removal. In addition the fight against trafficking in human beings will be enhanced through a new dedicated task force.

In the area of cybercrime, Europol focuses on three major types of criminal activity: cybercrime by organised groups generating large profits; child sexual exploitation, and other crimes that cause serious harm; and those activities affecting critical infrastructure and information systems in the EU. The main driver of these efforts is the EC3.

Regarding counter-terrorism, Europol's efforts are focused on increasing the sharing of information and cooperation between Member States and with other partners. The ECTC has been building up operational capabilities to enhance this information exchange and support major counter-terrorism investigations in Member States. Another priority is the fight against online radicalisation through the EU IRU. Moreover, Europol relies on the possibilities afforded by the Terrorist Finance Tracking Programme and by the integration of FIU.net to fight against terrorist financing. In this context, the possibility to request bank account data and access to PNR will enhance Europol's efforts in supporting investigations into terrorist financing. In addition, Europol is able to deploy a First Response Network (network of dedicated counter-terrorist experts from all EU Member States), in the event of a serious attack in Europe.

Finally, proof of Europol's positive contribution to the fight against serious crime in Europe are, among other things, the numerous successfully completed operations during the past 20 years, as well as the various training and capacity building exercises.

MAIN REFERENCES

De Amicis G., Kostoris R.E., Vertical Cooperation, in Handbook of European Criminal Procedure, Kostoris R. (eds). Springer, Cham, 2018.

Gless S., Europol, in Research Handbook on EU Criminal Law, by V. Mitsilegas, M. Bergström, and Th. Konstadinides, Edward Elgar Publishing Limited, 2016.

Odink I., Updated rules for Europol, EPRS, European Parliament, May 2016.

ENDNOTES

[1] The Regulation confirms Europol's legal continuity with the body instituted by the previous Council Decision.

[2] An important contributor to Europol, the UK's future relationship with the agency will have to be redefined post-Brexit.

[3] Predecessors: Jürgen Storbeck, Germany (head of the EDU and the first Europol Director, 1999-2005); Max-Peter Ratzel, Germany (2005-2009) and Rob Wainwright, United Kingdom (2009-2018).

[4] These are: **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**. The crimes in bold are those added by the Regulation. Terrorism is included both in the list and in Article 3, indicating that Europol's mandate covers terrorism with a cross-border dimension as well as terrorism affecting a single Member State.

DISCLAIMER AND COPYRIGHT

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)