

Revision of the Europol Regulation

This briefing is one in a series of 'implementation appraisals', produced by the European Parliamentary Research Service (EPRS), on the operation of existing EU legislation in practice. Each briefing focuses on a specific EU law that is to be amended or reviewed, as envisaged in the European Commission's annual work programme. 'Implementation appraisals' aim to provide a succinct overview of publicly available material on the implementation, application and effectiveness to date of an EU law, drawing on input from EU institutions and bodies, as well as external organisations. They are provided by the EPRS Ex-Post Evaluation Unit, to assist parliamentary committees in their consideration of new European Commission proposals, once tabled.

SUMMARY

Serious and organised crime is an increasingly dynamic and complex phenomenon, with new criminal markets emerging under the influence of globalisation and digitalisation. It very often goes hand in hand with corruption. As time passes, cybercrime infiltrates nearly every area of criminal activity. Moreover, terrorism continues to constitute a major threat to security in EU Member States. The EU supports operational law enforcement cooperation aimed at tackling serious crimes in line with its aim to establish an area of freedom, security and justice. Based on Article 88 of the Treaty on the Functioning of the EU (TFEU) and [Regulation 2016/794](#), Europol plays a key role in the coordination, organisation and in implementation of investigative and operative action carried out jointly with the Member States, and the collection, processing, analysis and exchange of information. Following a 2019 request by the Council of the EU, the European Commission scheduled its proposal to review the Europol Regulation for December 2020. This [proposal](#) is not based on an evaluation in line with the [Better Regulation Guidelines](#) as prescribed by Article 68 of the Europol Regulation. In this context, this appraisal focuses on a number of pertinent aspects, notably Europol's capabilities in terms of data processing, analysis and exchange, supervision by the European Data Protection Supervisor (EDPS) and joint scrutiny by the European Parliament and national parliaments, together with a brief presentation of the new Commission proposal, relevant positions by the European Parliament and questions raised by its Members.

1. Background

[Serious and organised crime](#) are two increasingly dynamic and complex phenomena. While traditional crimes, such as international drug trafficking, remain a principal cause of concern, the effects of globalisation in society and business have facilitated the emergence of significant new variations in criminal activity. These include migrant smuggling and trafficking in human beings, money laundering and the online distribution of child abuse, terrorist, racist and xenophobic content. As time passes, [cybercrime](#) has infiltrated nearly every area of criminal activity. Moreover, [terrorism](#) continues to constitute a major threat to security in EU Member States. Whereas the fight against jihadist terrorism remains an absolute priority, there is a [growing threat](#) of right-wing terrorism. Nationalist/separatist and left-wing/anarchist terrorists remain active in a number of Member States.

The EU aims to establish an [area of freedom, security and justice](#) (AFSJ). In this area, the free movement of persons should be ensured in conjunction with appropriate measures with respect to external border controls, asylum and migration, and with respect to preventing and combating crime. The coordination of [operational cooperation on internal security](#) remains in the hands of the Council. Still, the EU plays an increasingly important role in supporting operational cooperation among national law enforcement authorities by coordinating their [crime prevention](#) measures, facilitating the [exchange of information](#) contained in a number of [EU](#) and [national](#) information systems, taking part in [joint investigations](#) and [judicial cooperation in criminal matters](#), and adopting [minimum rules concerning the definition of serious criminal offences and sanctions](#).

The European Union Agency for Law Enforcement Cooperation ([Europol](#)) is one of the key AFSJ agencies supporting cooperation among the EU Member States in the area of cross-border law enforcement. In doing so, it liaises closely with other EU bodies and agencies, including [eu-LISA](#) (operational management of large-scale IT systems), [CEPOL](#) (law enforcement training), the European Union Agency for Criminal Justice Cooperation ([Eurojust](#)), the European Anti-Fraud Office ([OLAF](#)), the European Public Prosecutor's Office ([EPPO](#)), the European Monitoring Centre for Drugs and Drug Addiction ([EMCDDA](#)) and the European Border and Coast Guard Agency ([Frontex](#)).

Article 88 TFEU defines Europol's mission and provides that regulations adopted jointly by the European 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) the 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 [joint investigation teams](#). Any operational action by Europol must be carried out in liaison and in agreement with the authorities of the Member State or States whose territory is concerned. The application of coercive measures remains the exclusive responsibility of the competent national authorities.

2. Europol Regulation and its application

Introduction

In 2013 the Commission presented a [proposal](#) for a new regulation governing Europol. The Parliament and the Council subsequently reached an agreement on Regulation 2016/794¹ (the [Europol Regulation](#)). The regulation started applying from 1 May 2017 to all EU Member States except Denmark, which has an [opt-out](#) in the area of justice and home affairs, but still cooperates with Europol through a [specific agreement](#).² In accordance with Article 3 of the Europol Regulation, Europol's mandate is to strengthen EU Member States' competent authorities' action 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'.

For Europol to fulfil its objectives, Article 4 envisages a series of tasks for the agency, including it serving as a hub for criminal information-exchange and providing operational support and expertise to Member States' criminal investigations. Here it should be noted that Europol not only processes information that has been provided to it in accordance with [its mandate](#) but also has access to a number of interoperable [EU information systems](#) in the area of security, migration and external border management, notably the [Schengen Information System](#).

Europol has set up several units providing specialised expertise for combatting certain types of crime, including the European Cybercrime Centre ([EC3](#)), the European Counter Terrorism Centre ([ECTC](#)), the EU Internet Referral Unit ([IRU](#)), the European Migrant Smuggling Centre ([EMSC](#)) and the European Financial and Economic Crime Centre ([EFECC](#)). Furthermore, Europol provides strategic analyses and threat assessments in the areas of serious and organised crime ([SOCTA](#)), terrorism ([TE-SAT](#)) and cybercrime ([IOCTA](#)). These analyses feed into the Council's strategic and operational priorities of the Union for fighting crime ([EU policy cycle](#)). Europol also assists in the operational implementation of

those priorities. Moreover, Europol has established an [innovation lab](#) aimed at supporting investigators and law enforcement agencies in making the most of emerging technologies (e.g. [big data](#), [5G](#), [artificial intelligence](#)). This activity lacks a firm legal basis in the Europol Regulation, including safeguards with respect to [ethical and fundamental rights](#).

Last but not least, in accordance with Article 5, Europol may participate in the activities of joint investigation teams (JITs) dealing with crime falling within Europol's objectives. Europol currently does not have the right to initiate a criminal investigation of a crime falling within its objectives. This, together with the constraints placed on operational action by the Treaty, limits Europol's competences. However, in accordance with Article 6 it may request Member States' authorities to initiate an investigation. Member States should respond to such requests within a month.

As regards Europol's organisational structure, Article 7 obliges each Member State to establish a Europol national unit ([ENU](#)) serving as the liaison body between Europol and the competent authorities of that Member State. This ENU should supply Europol with information necessary for it to fulfil its objectives. Each ENU has to designate at least one liaison officer to be attached to Europol. Based on Articles 9-15, Europol's administrative and management structure comprises a [management board](#) composed of one representative of each Member State and one representative of the Commission. The Management Board adopts Europol's [multiannual programming](#) and annual work programmes, but also its [budget](#), [annual activity report](#) and internal rules for the selection of Europol's executive director. It also proposes a shortlist of candidates for the posts of [executive director](#) (currently Catherine de Bolle) and deputy executive directors to the Council, and appoints a [data protection officer](#). The executive director manages Europol and is accountable to the Management Board.

In accordance with Article 68, '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'. However, in view of the December 2019 [Council conclusions](#) stressing the need for European law enforcement to address ongoing technological developments, the Commission planned a review of the Europol Regulation; the relevant [proposal](#) will be discussed in greater detail in Section 3. Despite the absence of a Commission evaluation and other EU-level reports or studies comprehensively assessing the application of the Europol Regulation, there is general agreement among all EU institutions as regards the [added value](#) of the activities undertaken by Europol to [make Europe safer](#). If anything, there are frequent calls for Europol to play a key role in stepping up the fight against [serious crime](#) and [terrorism](#).

At the same time, Europol's activities have to comply with fundamental rights, notably the right to privacy and to [data protection](#). In this regard, the Europol Regulation allocates a key role to the European Data Protection Supervisor ([EDPS](#)). The European Parliament and national parliaments have also sought to strengthen their oversight of Europol's activities on the basis of the provisions in the Europol Regulation allowing for joint parliamentary scrutiny. The regulation envisages a [Joint Parliamentary Scrutiny Group](#), which has become operational in recent years. Therefore, this appraisal will focus on:

- 1) the processing, analysis and exchange of information by Europol and its relationship with other EU bodies, third countries, international organisations and private parties in this regard;
- 2) data protection safeguards and supervision; and
- 3) joint parliamentary scrutiny.

Processing, analysis and exchange of information

Based on Article 17 of the Europol Regulation, the agency can only process information that has been provided to it: a) by Member States in accordance with their national law; b) by EU bodies (Article 24), third countries and international organisations (Article 25); and c) (indirectly) by private parties and private persons (Articles 26 and 27). Europol may also directly retrieve and process information, including personal data from publicly available sources.

Article 18 establishes the purposes for which Europol may process information, including personal data: cross-checking aimed at identifying connections or other links between information or other relevant links between information related to suspected or convicted persons for a crime falling within the competence of Europol (or persons who, it is believed, on factual and reasonable grounds, will commit such a crime); carrying out strategic, thematic or operational analysis; and facilitating an information-exchange between Member States, Europol, other EU bodies, third countries and international organisations. Data processing for the purpose of operational analysis must be performed by means of specific [analysis projects](#). In this regard it has been observed that 'if Europol makes full use of its new competences and focuses on operational analyses, including data mining, its role could develop into a pace-setter as a 'main detector of criminal activities' within the EU'.³

However, the processing of large datasets sent by Member States to Europol or collected by Europol from publicly available sources has raised several compliance issues (cf. the '[big data challenge](#)'), notably as regards the processing of data of individuals not linked to any criminal activity. On 17 September 2020, the EDPS [decided](#) to admonish Europol (in accordance with Article 43(3)(d), further discussed in Section 2.2.) inter alia for non-compliance with Article 18. It urged Europol to implement all necessary and appropriate measures to mitigate the risks created by its personal data processing activities to data subjects.

Article 20 determines the conditions under which Member States may have access to information stored by Europol. In particular, they may 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 only have 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 obtaining the agreement of the provider of the data. Europol has expressed '[a clear business need](#)' for its legal framework to be adapted in order for Member States to be allowed to have direct access to data processed at Europol in the context of major investigations focusing on high-value targets or the most dangerous organised crime groups. Further to Article 21, Eurojust and OLAF may also have indirect access to Europol information for the purposes of launching cross-checks to identify links or to do strategic, thematic or operational analysis. It should be recalled here that this and other parts of the text do not yet reflect the role of the EPPO, as its [founding regulation](#) was only adopted in 2017.

In accordance with Article 25, Europol transfers of data to third countries and international organisations are subject a) to an 'adequacy decision' by the Commission, adopted in accordance with Article 36 of [Directive \(EU\) 2016/680](#) (which stipulates that the third country or the international organisation should ensure an adequate level of data protection); b) or to an EU international agreement concluded on the basis of Article 218 TFEU. Furthermore, a number of cooperation agreements predate the Europol Regulation.⁴ In accordance with Article 25(4), by 14 June 2021, the Commission should assess the data protection compliance of these agreements' provisions, and if appropriate, it should submit to the Council a recommendation for a decision authorising the opening of negotiations for an EU international agreement.

In 2018, negotiations commenced between the EU and [Turkey](#), [Algeria](#), [Egypt](#), [Morocco](#), [Tunisia](#), [Lebanon](#), [Israel](#) and [Jordan](#) on the exchange of personal data between Europol and the respective competent authorities of these countries for fighting serious crime and terrorism. In the hyperlinked resolutions, Parliament has expressed concerns regarding the level of personal data protection in these countries. More recently, as regards [New Zealand](#), in line with Court of Justice of the European Union (CJEU) case law,⁵ the European Parliament has insisted on the level of data protection provided for in the future agreement to be 'essentially equivalent to the level of protection provided for in EU law', including in measures related to police cooperation under Chapter 5 TFEU.⁶ At the same time, Europol has expressed an [operational need](#) for a less cumbersome regime for the exchange of personal data with third countries, without an adequacy decision or international agreement.

Finally, Article 26 stipulates the conditions for the exchange of data with private parties. Europol may receive (bulk) personal data from private parties, as long as Europol only processes it to identify the Member State, third country or international organisation concerned. These may then decide to resubmit the data to Europol within four months after the transfer took place. The data transfers between Europol and private parties are therefore indirect, via ENUs 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 concerned, for the prevention of imminent crime or, if the crime is publicly available, for any reason to combat cybercrime. The [Council conclusions](#) adopted in December 2019 acknowledge 'the urgent operational need for Europol to request and receive data directly from private parties' on the understanding that 'fundamental rights such as the protection of personal data and the principles of consent by the Member States, voluntary transmission and absence of feedback, are to be respected.' The Council called on the Commission to take the December 2019 Council conclusions 'into account in the framework of its review of the Europol Regulation, when examining the practice of direct exchange of personal data with private parties' and 'to consider adapting the schedule for the above review as necessary, especially in view of the need for European law enforcement to address ongoing technological developments'.

Commission study on the practice of direct exchanges of personal data between Europol and private parties

In accordance with Article 26(10), the Commission was to evaluate the practice of direct exchanges of personal data with private parties by 1 May 2019. In this regard, on 12 November, 2020, the European Commission published a [study](#) conducted for its Directorate-General on Home Affairs (DG HOME) by the consultancy Milieu. The study is mainly based on responses received to a stakeholder consultation and semi-structured interviews followed by an online workshop. It notably establishes shortcomings in the current system under Article 26(2), under which Europol is only allowed to process personal data with the sole purpose of identifying the ENU, which can then resubmit the personal data to Europol. On the one hand, it might be difficult for Europol to identify the ENU (jurisdiction) responsible. On the other hand, ENUs may not resubmit the data (though this could be for legitimate reasons). Also it is argued that ENUs are not sharing data they received from private parties with Europol to a sufficient degree, while again acknowledging that there might be legitimate reasons for not doing so. The study concludes that there is a need for the Europol Regulation to be amended 'to allow for direct exchanges of personal data with private parties, and to empower Europol with a more extensive data processing mandate'. Furthermore, it recommends 'channelling requests from Law Enforcement Authorities to private parties through a dedicated platform, such as Europol'.

The study suffers from a number of shortcomings. It does not address (the need for) independent judicial control, nor does it properly reflect the positions of national data protection authorities (DPAs) and private parties. First, the study should have considered the linkages between Europol's being enabled to exchange data directly with private parties and the current negotiations on giving law enforcement bodies access to [electronic evidence in criminal matters](#) by means of production and preservation orders. In line with the principles of [Better Regulation](#), there is a need to ensure *coherence* between the various EU legal frameworks applicable to law enforcement bodies' access to personal data held by private parties at EU and national level, notably in terms of effective and independent judicial control. Second, the stakeholder consultation did not receive sufficient responses from the DPAs. Therefore, its outcome is not representative of their views. Third and last, [issues related to conflicts of law, jurisdiction and potential liabilities of online service providers](#) could have been considered and assessed in greater depth. In this regard, there seems to be an inconsistency between the reported position of private parties in this study and their subsequent contributions to the Commission's [public consultation](#) leading up to the new proposal (see Section 3.1.) as regards their support for Europol to exchange data with them directly.

Data protection safeguards and supervision

Data protection is a fundamental right, recognised as such by [Article 8 of the Charter of Fundamental Rights of the European Union](#) (EU Charter). The first paragraph presents the right to data protection; the second and the third paragraph reference a number of specific data protection principles, including that of lawfulness and fairness of processing, purpose limitation, and independent supervision. The Lisbon Treaty also included data protection as a principle in Article 16 TFEU. At the same time, [Declaration 21](#) to the Lisbon Treaty recognised the specificities of data processing by police and judicial authorities, which must still uphold EU primary law and EU Charter privacy guarantees.

On this basis, data protection principles have been further specified as regards their application to the public and the private sector (Regulation 2016/ 679, or the [General Data Protection Regulation](#)), and to law enforcement ([Directive 2016/680](#)).⁷ Even though it operates in the area of law enforcement, Europol retains its own data protection regime. And even though Europol is an EU agency, data protection provisions applicable to processing by EU agencies in the context of police and judicial cooperation contained in [Regulation 2018/1725](#) do not apply to Europol for the moment. Article 98 of Regulation 2018/1725 obliges the Commission to review this situation by April 2022. At this stage, it is difficult to establish whether the fragmentation and divergences between the closely related legal regimes may have undermined the effective protection of fundamental rights and/or hampered operational cooperation.

The Europol Regulation provides all individuals with the right to obtain information on whether or not personal data relating to them are processed by Europol (Article 36); to ask for rectification, erasure and restriction (Article 37) of such data; and, in more general terms, that their data are processed in accordance with data protection principles (Article 28), notably in a fair and lawful way. In terms of oversight, Europol has established, in accordance with Article 41, a Data Protection Function (DPF), headed by a [data protection officer](#) (currently Daniel Drewer) whose task it is to ensure the application of the regulation's provisions concerning the processing of personal data. In the context of his activities, Europol's DPF has established an online collaboration platform – the Europol Data Protection Experts Network ([EDEN](#)). Further to Article 42, each Member State has also established a national supervisory authority that monitors independently, in accordance with national law, the permissibility of the transfer, the retrieval and any communication to Europol of personal data by the Member State concerned, including as regards their compliance with the rights of data subjects.

Pursuant to Article 43, the EDPS monitors Europol's data processing activities and ensures their compliance with the data protection safeguards built into the regulation. The EDPS's oversight of Europol's data processing activities includes: conducting [inquiries](#); investigating complaints (cf. Article 47 on the right to lodge a complaint with the EDPS); 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 or the CJEU. The Europol Regulation also institutes a Cooperation Board (Articles 44, 45), made up of the EDPS and a representative of the supervisory authority of each Member State. The Cooperation Board has an advisory role and, among other tasks, may issue guidelines, recommendations and best practices.

Joint Parliamentary Scrutiny

In accordance with Article 51, a Joint Parliamentary Scrutiny Group (JPSG) consisting of members of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) and members of national parliaments 'politically monitor Europol's activities in fulfilling its mission, including as regards the impacts of those activities on the fundamental rights and freedoms of natural persons'. The JPSG has held seven meetings (the sixth was cancelled due to Covid-19). In accordance with Article 2 of the JPSG's [Rules of Procedure](#), it is composed of a maximum of four members per national parliament and 16 Members of the European Parliament. Further to Article 3 of the JPSG Rules of procedure, JPSG

meetings are alternatively hosted by the Member State holding the rotating presidency of the Council of the European Union (first half of the year) and by the European Parliament (second half of the year). The [last JPSG meeting](#) was held remotely and hosted by the European Parliament on 28 September, 2020. During their meetings, JPSG members have discussed topics such as Europol's [multiannual work programme](#), data protection, cooperation with other EU agencies, third countries, the implications of the UK's departure from the EU, and right-wing terrorism. They have also made use of their right to address oral and [written questions](#) to Europol, including on Europol cooperation with the private sector and its role in operational cases related to the assassination of investigative journalists.

As revealed by [EPRS research](#), Parliamentary scrutiny over Europol remains rather limited.⁸ There is also a lack of coherence in terms of the level of scrutiny of AFSJ agencies that cooperate closely with each other.⁹ In particular, the JPSG may request the chair of the Management Board and the executive director to appear before it. However, the powers the European Parliament and the JPSG have over the Management Board (in terms of participation) and the executive director (in terms of appointment) are comparatively weak, as indicated by the italicised parts of the provisions in the Europol Regulation cited below.

In accordance with Article 14(4), the Management Board *may* invite a JPSG representative to attend its meetings as a *non-voting observer* and only when the opinion of the JPSG representative is relevant for the topics being discussed by the Management Board, among them Europol's programming document or budgetary aspects related to the fulfilment of Europol's activities. In practical terms, a JPSG representative is invited to attend a Management Board meeting twice a year.¹⁰ Furthermore, in accordance with Article 54(2), before the candidate for executive director selected by the Council is appointed, they *may* be invited to the LIBE committee, which gives a *non-binding* opinion. The above-mentioned EPRS research also shows that the European Parliament has greater say in the appointment procedure for executive directors of other EU agencies.¹¹ At the same time, the JPSG does have a right to be consulted regarding Europol's multiannual programme before it is adopted by the Management Board in accordance with Article 12(1). Finally, in accordance with Article 51(5), the JPSG may draw up 'summary conclusions' on the political monitoring of Europol and submit those conclusions to the European Parliament and the Member States' national parliaments. The European Parliament forwards them for information purposes to the Council, the Commission and Europol. As regards this provision, it has been observed by academia that 'Europol does not have to fear direct consequences of this parliamentary scrutiny.'¹²

Access by the European Parliament to information processed by Europol is regulated in accordance with Article 52 and 67. However, as Europol mainly relies on information provided to it by the national authorities, these can effectively prevent disclosure to the European Parliament by denying their consent in accordance with the '[principle of originator control](#)'.¹³ Here, however, it has been suggested that the 'networking platform' of the JPSG might provide an outcome as national parliaments could 'provide valuable influence in accessing information from national sources that Member States would normally be distrustful of sharing with the EP.'¹⁴

3. The new Commission proposal

Public consultation

In its [2020 work programme](#), the Commission announced the goal of strengthening Europol's mandate as a priority under the portfolio 'Promoting our European way of life'. On 14 May 2020, the Commission launched a public consultation on the [inception impact assessment](#) (IIA), with a deadline of 9 July 2020. The main envisaged changes to the Europol Regulation described in the IIA are:

- strengthening Europol's capacity to request the initiation of cross-border investigations;
- strengthening Europol's tasks to address emerging threats, inter alia by enhancing Europol's mandate in the areas of research and innovation;

- opening new avenues for data exchanges between Europol and third countries in specific situations and on a case-by-case basis for preventing and countering crimes;
- enabling Europol to directly exchange personal data with private parties;
- strengthening Europol's data protection regime.

The feedback received (20 contributions without duplications) can be found on the [Commission website](#). It is difficult to draw firm conclusions from this limited response. However, it should be pointed out that several contributors insist that evidence of the lack of effectiveness of operational cooperation due to limitations present in Europol's current mandate should have been considered in the context of a full evaluation (as required by Article 68 of the Europol Regulation). It is clear from the responses that enabling Europol to directly exchange personal data with private parties is the most controversial proposal. Private sector contributors deem it necessary to consider the negotiations on the [e-Evidence](#) proposal as a priority, before updating Europol's scope and capability in requesting direct access to data from private parties. NGOs furthermore express the concern that enabling Europol to directly exchange personal data with private parties would allow circumventing national procedural safeguards and accountability mechanisms, while also being incompatible with the EU Charter and national constitutional provisions. In general, both the private sector and NGO contributors question whether allowing Europol to directly exchange personal data with private parties would be compatible with Article 88 TFEU and Article 6 of the Europol Regulation (Europol is not entitled to taking coercive action or to starting investigations on its own initiative, as discussed in Section 2.1.). The Commission also reports having conducted a targeted stakeholder consultation with the help of a questionnaire and a number of expert interviews and targeted thematic stakeholder workshops addressed at experts, including practitioners at national level.¹⁵

Proposal amending Regulation (EU) 2016/794

The [proposal](#), accompanied by an [impact assessment](#), was published on 9 December 2020. The strengths and weaknesses of this impact assessment will be analysed further in an upcoming EPRS initial appraisal. The Commission proposal seeks to strengthen Europol's mandate by (amended articles **bold** and in brackets): enabling the agency to enter data into the Schengen Information System on the suspected involvement of a third-country national in an offence in respect of which Europol is competent (**Article 4**); strengthening Europol's role on research and innovation (**Article 4**); clarifying that Europol may request, in specific cases where Europol considers that a criminal investigation should be initiated, the competent authorities of a Member State to initiate, conduct or coordinate an investigation of a crime that affects a common interest covered by a Union policy, without the requirement for a cross-border dimension of the crime concerned (**Article 6**); enabling Europol to support Member States and their investigations through big data analysis (**Article 18**); strengthening Europol's cooperation with the EPPO (**Articles 18 and 20**); enabling joint operational analysis between Europol and Member States in specific investigations (**Article 20**); opening new avenues for Europol cooperation with third countries in specific situations and on a case-by-case basis for preventing and countering crimes (**Article 25**); enabling Europol to directly exchange data with private parties (**Article 26**); further strengthening the data protection framework applicable to Europol (**Articles 27, 30, 33, 39 and 41**); further strengthening parliamentary oversight and accountability of Europol (**Article 51**).

4. European Parliament position / MEPs' questions

Resolutions of the European Parliament

In paragraph 26 of its [2020](#) resolution on the [EU security union strategy](#) the European Parliament observes that it '[t]akes note of the Commission's plan to revise Europol's mandate to enable it to become a hub for the exchange of information on law enforcement and for cooperation in the fight against terrorism and serious and organised crime in the EU'. It also 'stresses that this new upgraded mandate should provide Europol with the relevant tools for cooperating more effectively with all the

relevant partners'. At the same time, it 'stresses that such changes should be accompanied by enhanced political accountability, as well as enhanced judicial control and parliamentary scrutiny, with a strong focus on accountability, transparency and respect for fundamental rights'. Furthermore, it 'stresses that the revision of Europol's mandate should fully align the agency's data protection regime with [Regulation 2018/1725](#)'. It also 'demands that an evaluation of the current legal framework for Europol's mandate is presented as provided for by Article 68 of the current Europol Regulation'. Furthermore, in paragraph 42 it 'calls for proper funding and staffing of EU agencies and bodies in fields covered by the AFSJ in order for the EU to deliver on the Security Union Strategy'.

Since 2016, the European Parliament has established two special committees dealing with serious crimes within Europol's mandate. The first focused on money laundering, tax evasion and tax avoidance, culminating in a [resolution](#) in 2017. The second focused on the fight against terrorism, culminating in a [resolution](#) in 2018. These resolutions express strong support for the strengthening of Europol's activities, including those of its specialised units and networks in the areas of counterterrorism and financial and economic crime. At the same time, in a 2017 [resolution](#) on fundamental rights implications of big data the Parliament recalled 'that the collection and processing of personal data for law enforcement purposes must always be adequate, relevant and not excessive in relation to the specified, explicit and legitimate purposes for which they are processed'. Finally, from a more institutional perspective, a 2020 [resolution](#) on preventing money laundering and terrorist financing specifically called for strengthening Europol's 'capacity to request the initiation of cross-border investigations, particularly in cases of serious attacks against whistle-blowers and investigative journalists'.

Selected written questions by MEPs

Beyond the [written questions](#) posed in the context of the JPSG, there have been a number of MEPs' questions related to Europol during the current term (2019-2024). Below is a representative selection of these questions, covering issues such as Europol's competences, resources, cooperation with other EU agencies, intelligence services, international partners and the private sector, as well as issues related to specific areas of serious crime and the related fundamental rights, including data protection standards. Both the questions and the answers provided by the European Commission are reproduced below.

[Written question E-005938/2020](#) by Assita Kanko (ECR, Belgium) of 30 October 2020 on 'A comprehensive inter-agency strategy against cybercrime' asks whether the Commission anticipates the establishment of a high-level working group whereby all EU agencies can exchange best practice and evaluate overall preparedness, especially as the EU moves towards greater interoperability of its systems'. It also queries whether the current human and financial resources allocated to EU agencies for activities related to cybersecurity are sufficient and whether these agencies are capable of attracting sufficiently qualified staff. No Commission reply had been received at the time of writing.

[Written question E-005327/2020](#) by Patrick Breyer (Greens/EFA, Germany) of 29 September 2020 on 'Processing of big data and information on non-suspected citizens by Europol' asks what consequences does the Commission draw from the EDPS decision (C 2018-0548, 20 December 2019) calling into question the legitimacy of Europol's capacity to process big data? The MEP furthermore wishes to know whether, in the Commission's view, Europol is authorised to store and process the data of people who are not suspected of committing a crime or who do not correspond to any of the categories set out in Article 18(5) and Annex II of the Europol Regulation. Finally, the MEP queries what big data Europol receives via its Large File-Exchange Server (LFE) and how much of this is used by the Member States? No Commission reply had been received at the time of writing.

[Written question P-004562/2020](#) by David McAllister (EPP, Germany) of 13 August 2020 on a 'European police service' asks whether the Commission is to provide more resources for Europol to be further reinforced. It also asks whether the Commission supports the call for security services to be better connected and for the creation of uniform standards for the exchange of information on criminals and their networks. Finally, the MEP queries the Commission's view on a European police service that would have some executive powers and would support national security services. The Commission's

[answer](#) of 15 October 2020 confirms that Europol's budget has been continuously reinforced in recent years. It insists that supporting the exchange of information is an essential element of the EU-level support to national law enforcement authorities. As regards a European police service, the Commission points out that, according to Article 4(2) of the Treaty on European Union, national security remains the sole responsibility of the individual Member States.

[Written question E-002720/2020](#) by Cornelia Ernst (The Left, Germany) of 5 May 2020 on 'Closer cooperation between Europol and intelligence services' asks about Europol's interactions with Member States' intelligence services via the Counter-Terrorism Group (CTG) in terms of locations visited, workshops held and topics covered. In its [answer](#) of 23 July 2020, the Commission clarifies that Europol and CTG members first established a contact with each other in 2016 to explore ways to establish a structured cooperation between intelligence services and Europol, while respecting each other's regulatory frameworks. This has taken the form of joint workshops on counterterrorism issues in 2019, namely a workshop on open sources information for law enforcement and intelligence investigations, and two workshops on face recognition. No workshops took place in 2020. Furthermore, there have been reciprocal visits: by the Europol executive director to the CTG operational platform and by the CTG platform coordinator to the Europol executive director at the agency headquarters, with the aim to build mutual knowledge. Moreover, the CTG presidency has been invited to justice and home affairs ministerial meetings to give an update on the cooperation between competent authorities dealing with counter-terrorism.

[Written question E-004594/2019](#) by Maria Grapini (S&D, Romania) of 23 December 2019 on 'Combating right-wing extremism a top EU priority' asks what measures the Commission is taking to curb right-wing extremism and prevent all forms of violence against any group or community. In its [answer](#) of 26 March 2020, the Commission highlights that it has initiated a number of actions to counter violent right-wing extremism, notably the Radicalisation Awareness Network ([RAN](#)), which it funds, that brings together first-line practitioners to exchange experience on topics such as responding to violent far-right extremist narratives, tackling violent far-right extremism at the local level and at schools, and police prevention work. The [Justice and Home Affairs Council of October 2019](#) agreed to continue work along four strands: creating a better situational overview of violent right-wing violent extremism and terrorism in the EU; developing and sharing good practices; addressing the spread of unlawful right-wing extremist content online and offline; and cooperating with key third countries.

[Written question E-004013/2019](#) by Moritz Körner (Renew, Germany) of 25 November 2019 on 'TFTP bulk data' refers to the [EU-US Terrorist Finance Tracking Programme \(TFTP\) Agreement](#). It queries how it is possible that the data requests to Europol under Article 4 of the TFTP agreement have led to bulk data transfers every month since the entry into force of the TFTP Agreement? It asks about the compatibility of this practice with Article 4. In its [answer](#) of 10 March 2020, the Commission indicates that it follows from the text of Article 4 that, although the amount of data must be minimised as much as possible, this does not exclude the transfer of a batch of data. Only after Europol validates that the conditions of Article 4 have been met, can the designated provider transfer the requested batch of data to the United States' Treasury Department.

FURTHER READING

- M.A. Biasiotti, J. P. Mifsud Bonnici, J. Cannataci, F. Turchi (eds.) [Handling and Exchanging Electronic Evidence Across Europe](#), Springer, 2018.
- S. Carrera, M. Stefan, V. Mitsilegas, [Cross-border data access in criminal proceedings and the future of digital justice](#), CEPS, 2020.
- C. Cîrlig, [Europol: the EU law enforcement cooperation agency](#), briefing, EPRS, European Parliament, September 2019.
- European Court of Auditors, [Special Report, Future of EU agencies – Potential for more flexibility and cooperation](#), 2020.
- F. Coman-Kund, ['Europol's international cooperation between 'past present' and 'present future': reshaping the external dimension of EU police cooperation'](#), *Europol and the world: a law review*, 2018, Vol. 2, p. 1-37.
- D. Drewer and V. Miladinova, [The BIG DATA Challenge: Impact and opportunity of large quantities of information under the Europol Regulation](#), *Computer Law & Security Review*, 2017, Vol. 33/3, pp. 298-308.
- Europol, [Europol Programming Document 2020-2022](#), 2020.
- G. González Fuster, [Artificial Intelligence and Law Enforcement, Impact on fundamental rights](#), Policy Department for Citizens' Rights and Constitutional Affairs, DG IPOL, European Parliament, 2020.
- S. Gless and T. Wahl, 'A comparison of the evolution and pact of police and judicial cooperation in criminal matters: a race between Europol and Eurojust?' In C. Brière and A. Weyembergh (eds.) [The needed balances in EU criminal law: Past, present and future](#), Hart Publishing, 2018, pp. 339-354.
- P. de Hert, 'The Role of the Data Protection Authorities in Supervising Police and Criminal Justice Authorities Processing Personal Data' In C. Brière and A. Weyembergh (eds.) [The needed balances in EU criminal law: Past, present and future](#), Hart Publishing, 2018, pp. 243-256.
- I. Ilić, ['Parliamentary oversight of Europol under Europol Regulation 794/2016: a modified institutional framework'](#), *Queen Mary Law Journal*, 2019, Vol. 10, pp. 51-68.
- F. König, [Big Data, 5G and AI, How Europol could help von der Leyen achieve her goals](#), Hertie School of Governance policy paper, 2020.
- R. Korver, [EU Agencies, Common Approach and Parliamentary Scrutiny](#), European implementation assessment, Ex-post Evaluation Unit, EPRS, 2018.
- K. Milt, [Police cooperation achievements during the legislative term 2014-2019: the role of the European Parliament](#), DG IPOL, European Parliament, 2019.
- M. Schinina, ['What balance between Eurojust and Europol from a parliamentary angle?'](#), in *New Journal of European Criminal Law*, 2020, Vol. 11(2), pp. 123-134.

ENDNOTES

- ¹ [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, OJ L 135, 24.5.2016, pp. 53–114.
- ² Cf. C. Cîrlig, [Europol: the EU law enforcement cooperation agency](#), EPRS, 2019, p. 10.
- ³ S. Gless and T. Wahl, 'A comparison of the evolution and pact of police and judicial cooperation in criminal matters: a race between Europol and Eurojust?' In C. Brière and A. Weyembergh (eds.) [The needed balances in EU criminal law: Past, present and future](#), Hart Publishing, 2018, pp. 339-354, at p. 349.
- ⁴ Cf. F. Coman-Kund, ['Europol's international cooperation between 'past present' and 'present future': reshaping the external dimension of EU police cooperation'](#), *Europol and the world: a law review*, 2018, Vol. 2, pp. 1-37.
- ⁵ CJEU Opinion 1/15, EU-Canada PNR Agreement, EU:C:2017:592 (26.7.2017); judgment of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650; judgement of 16 July 2020, C- 311/18, *Schrems II*, EU:C:2020:559; [EDPS Opinion2/2018](#) - EDPS Opinion on eight negotiating mandates to conclude international agreements allowing the exchange of data between Europol and third countries.
- ⁶ European Parliament resolution of 10 July 2020 on the European Parliament recommendation to the Council and the Commission concerning the conclusion of an agreement, under negotiation, between the European Union and New Zealand on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation

- (Europol) and the New Zealand authorities competent for fighting serious crime and terrorism, [P9_TA\(2020\)0200](#) paragraph 2.
- ⁷ Cf. P. de Hert, 'The Role of the Data Protection Authorities in Supervising Police and Criminal Justice Authorities Processing Personal Data' In C. Brière and A. Weyembergh (eds.) *The needed balances in EU criminal law: Past, present and future*, Hart publishing, 2018, p. 243-256.
- ⁸ R. Korver, [EU Agencies, Common Approach and Parliamentary Scrutiny](#), EPRS, 2018.
- ⁹ M. Schinina, '[What balance between Eurojust and Europol from a parliamentary angle?](#)', in *New Journal of European Criminal Law*, 2020, Vol 11(2), p. 123-134, at p. 133.
- ¹⁰ Europol, Consolidated Annual Activity Report 2018, p. 55: 'With a view to establishing a constructive and fruitful relationship with the JPSG, a key partner in ensuring and continuously strengthening Europol's democratic legitimacy and accountability to the Union's citizens, the MB discussed throughout 2018 the practical implementation of Article 14(4) of the ER and, in October, agreed to invite the JPSG representative to attend two MB meetings per year, namely one MB meeting per semester under the auspices of the respective EU Presidency, concerning items for which the JPSG opinion was deemed relevant to the MB discussions.'
- ¹¹ R. Korver, [EU Agencies, Common Approach and Parliamentary Scrutiny](#), EPRS, 2018, p. 61.
- ¹² S. Gless and T. Wahl (2018), *supra* n.2, at p. 353.
- ¹³ M. Schinina (2020), *supra* n. 6, at p. 132.
- ¹⁴ I. Ilić, '[Parliamentary oversight of Europol under Europol Regulation 794/2016: a modified institutional framework](#)', *Queen Mary Law Journal*, 2019, Vol 10, p. 51-68, at p. 62.
- ¹⁵ Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation, [COM\(2020\) 796 final](#) of 9 December 2020, explanatory memorandum, at p. 8.

DISCLAIMER AND COPYRIGHT

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.

© European Union, 2021.

eprs@ep.europa.eu (contact)

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

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

<http://epthinktank.eu> (blog)

