Strengthening Europol's mandate

OVERVIEW

On 9 December 2020, along with its counter-terrorism agenda, the European Commission adopted a proposal for a regulation to reinforce the mandate of Europol, the EU law enforcement cooperation agency.

The proposed regulation aims principally at rendering Europol's cooperation with private parties more effective; responding to the agency’s 'big data challenge', by providing a legal basis for processing large and complex datasets, including personal data of data subjects not related to a crime; and reinforcing Europol's role in relation to research and innovation for law enforcement.

The legislative proposal, which would amend the existing Europol Regulation (EU) 2016/794, is accompanied by another legislative proposal to modify Regulation (EU) 2018/1862 on the Schengen information system (SIS), to allow Europol to issue alerts in SIS under a new category.

On 1 February 2022, the European Parliament and the Council reached a provisional agreement on the proposal for a regulation, which was formally adopted by each institution on 4 May and 24 May respectively, and signed into law on 8 June. The regulation entered into force on 28 June 2022.

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

Committee responsible: Civil Liberties, Justice and Home Affairs (LIBE)

Rapporteur: Javier Zarzalejos (EPP, Spain)

Shadow rapporteurs:
- Franco Roberti (S&D, Italy)
- Dragoş Tudorache (Renew, Romania)
- Tom Vandendriessche (ID, Belgium)
- Saskia Bricmont (Greens/EFA, Belgium)
- Patryck Jaki (ECR, Poland)
- Clare Daly (The Left, Ireland)

Procedure completed: Regulation (EU) 2022/99

OJ L 169, 27.6.2022, pp. 1-42
Introduction

According to the EU’s 2020-2025 security union strategy, the European security landscape is characterised by evolving and complex security threats, enhanced by factors such as new technologies, globalisation, interconnectivity and the digital transformation being exploited by criminals and terrorists. The pandemic, which has led to increased reliance on digital infrastructure, has also exposed vulnerabilities that have been seized upon by criminals. This is visible in the surge of cyber-crime, including the growth of child sexual abuse material online, the cyber-enabled theft of intellectual property, cyber-attacks and phishing, damage to critical infrastructure, and the spread of disinformation. At the same time, the more traditional threats, such as drug trafficking, trafficking in human beings, and terrorism have evolved to take advantage of online illicit markets and new technologies. It is considered that ‘almost all criminal activities now feature some online components, such as digital solutions facilitating criminal communications’. This shift brings about significant challenges for EU Member States’ law enforcement, including in relation to the wide use of encryption or the need to process and analyse large datasets.

Evolving from informal intergovernmental cooperation set up in the 1970s, the European Union Agency for Law Enforcement Cooperation (Europol) is today a fully fledged EU body tasked with supporting cooperation between EU Member States’ competent authorities with the purpose of countering serious crime and terrorism. Europol is 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. To fulfil its objectives, the agency carries out a series of tasks, which include acting as the EU criminal information exchange hub and providing operational support and expertise to Member States’ criminal investigations.

Although Europol has had a new mandate since May 2017, aligned with the requirements of the Lisbon Treaty, developments in the European security landscape indicate the need to endow the agency with improved capabilities. Following calls from the Council of the EU and the European Parliament to reinforce the Europol mandate in certain areas, the European Commission announced a legislative initiative in its 2020 work programme. The initiative was also included in the new EU security union strategy of July 2020. On 9 December 2020, the Commission presented, together with its new counter-terrorism agenda, a proposal for a regulation on a revised mandate for Europol, focused on cooperation with private parties, on processing large and complex datasets, and on strengthening the agency’s role on research and innovation for law enforcement. The Commission also envisages enabling Europol to enter alerts on suspects and criminals in the Schengen information system (SIS), through amending the SIS Regulation.

Existing situation

Europol is governed by Article 88 of the Treaty on the Functioning of the EU (TFEU). The article defines Europol’s mission, namely ‘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’. 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 joint investigation teams (JITs). Together with national parliaments, the European Parliament scrutinises Europol’s activities, while the European Data Protection Supervisor (EDPS) ensures oversight of the agency’s data processing activities.

To ensure alignment with the Lisbon Treaty, the previous Europol Decision (Council Decision 2009/371/JHA) was replaced by the Europol Regulation (Regulation (EU) 2016/794), which entered into force on 1 May 2017 and applies to all EU Member States, except Denmark, which has an opt-out from the Treaty’s justice and home affairs provisions. The regulation strengthens Europol’s data management and protection regime; creates a new parliamentary oversight body, the Joint Parliamentary Scrutiny Group (JPSG) and reforms the way Europol exchanges information.
with its partners. Finally, it provides for individuals' right of access to their personal data and a right to obtain compensation for unlawful data processing. The regulation's review was envisaged by 1 May 2022 and every five years thereafter.

During four years of implementation, the Europol Regulation has revealed some shortcomings, particularly in relation to the agency's processing, analysis and exchange of information activities, and in terms of data protection. For example, the regulation provides for strict rules as regards the categories of data subjects whose personal data may be processed by Europol (i.e. persons believed to be linked to a crime, either as convicted persons, suspects, contacts or associates of suspects, victims, witnesses or informants). However, Europol's processing of large datasets sent by Member States or collected from public sources led to compliance issues. In what is known as Europol's 'big data challenge', the EDPS admonished the agency for processing large datasets (including personal data of individuals not linked in any capacity to a crime) in non-compliance with the Europol Regulation. Europol's plans to develop policies for using operational data for data science purposes, including the testing, development and training of algorithms, also led to an EDPS inquiry. Moreover, Europol has argued, among other things, in favour of a less cumbersome regime for exchanging data with third countries and the possibility to receive data from private parties directly (currently, such data may only be sent through a Member State's national unit or authority). Some of these aspects are included in the proposal to amend the Europol Regulation.

Parliament's starting position

In a December 2018 resolution, Parliament called 'for the active involvement of EU agencies such as Europol and CEPOL in EU security research projects' and for Europol to be tasked with further research and development projects in this field. It also welcomed the new provision in the future SIS II allowing Europol, unless legal or operational reasons required otherwise, to be informed of any new alert or any hit linked to terrorism in SIS.

In its July 2020 resolution on preventing money laundering and terrorist financing, Parliament called for the strengthening of EU agencies, including Europol, in this area and noted that a strengthened mandate 'should go hand-in-hand with adequate parliamentary scrutiny'. Parliament also underlined the priority of 'strengthening Europol's capacity to request the initiation of cross-border investigations, particularly in cases of serious attacks against whistleblowers and investigative journalists ...'.

On 17 December 2020, Parliament, Council and the Commission agreed the Joint Declaration on the common legislative priorities for 2021, which includes strengthening Europol's mandate as a priority file. The same day, the European Parliament adopted a resolution on the EU security Union strategy. While welcoming the Commission's proposal to strengthen the mandate of Europol, Parliament also underlined that the 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'. Moreover, it called for the alignment of Europol's data protection regime with Regulation (EU) 2018/1725 (processing of personal data by EU institutions, bodies, offices and agencies). Finally, Parliament demanded a review of the agency's activities, as envisaged in the Europol Regulation (i.e. by 1 May 2022).

European Council and Council starting position

On 18 October 2018, in its conclusions on internal security, the European Council called for measures that 'provide Member States' law enforcement authorities, Europol and Eurojust with adequate resources to face the new challenges posed by technological developments and the evolving security threat landscape, including through pooling of equipment, enhanced partnerships with the private sector, interagency cooperation and improved access to data'.

In October 2019, EU justice and home affairs ministers discussed the role of new technologies in the area of internal security. They expressed support for the creation of an innovation lab at Europol
that could ‘act as an observatory of new technological developments and drive innovation, including by developing common technological solutions for member states in the field of internal security’\(^2\) and stressed the need for stronger cooperation with the private sector. On 2 December 2019, the Council acknowledged ‘the urgent operational need for Europol to request and receive data directly from private parties’, while respecting fundamental rights, such as the protection of personal data and the principles of consent by Member States, voluntary transmission and absence of feedback to third parties on the use of the data.

At an informal meeting on 21 October 2020, the EU interior ministers adopted a declaration entitled ‘Ten points on the future of Europol’, formally approved by the Council as a resolution on 9 November 2020. The declaration stresses the added value of the agency and argues the main focus must be to strengthen its core tasks. Europol should make use of technological innovation for law enforcement, including the development and use of artificial intelligence for analysis and operational support. Moreover, the legal framework must be amended to allow Europol to process large amounts of data, while guaranteeing a high level of data protection. Europol must also be able to cooperate effectively with private parties, and information exchange mechanisms with third countries must be rendered more effective.

**Preparation of the proposal**

On 29 January 2020, the European Commission published its work programme. Under the ‘Promoting our European way of life’ priority, the Commission announced its intention to adopt a legislative proposal on the strengthening of Europol’s mandate, based on Article 88 TFEU. In preparing the proposal, the Commission used diverse methods and forms of consultation, including a consultation on the inception impact assessment (IIA), as well as targeted consultation of stakeholders by way of a questionnaire, experts’ interviews and thematic stakeholder workshops.

The Commission also mentions a number of studies and reports that fed into the proposal, in particular the Study on the practice of direct exchanges of personal data between Europol and private parties (September 2020). The study’s recommendations include revising the Europol Regulation to allow for direct exchange of personal data with private parties and giving Europol a more extensive data-processing mandate. It also argues in favour of using Europol as a platform for ‘channelling requests from Law Enforcement Authorities to private parties’. However, an EPRS implementation appraisal on the revision of the Europol Regulation points to a number of flaws in the study, including that it does not properly reflect the positions of national data protection authorities and private parties; and that it did not set out the issue within the context of other EU initiatives, such as the proposed e-evidence regulation.

The Commission’s impact assessment accompanying the legislative proposal highlights three main problems that a revised Europol mandate should address, all linked to criminal exploitation of the opportunities offered by the digital transformation and new technologies.

**Lack of effective cooperation between private parties and law enforcement authorities**

Currently, Europol can receive data from private parties only indirectly, through the intermediary of a Member State’s Europol national unit (ENU), or through contact points in third countries with which Europol exchanges personal data. Moreover, if private parties do share data with Europol, the agency may process these data only for the purpose of identifying the relevant ENU; it must then transfer the data to the ENU and delete it. The ENU may afterwards decide to resubmit the data to Europol. If, however, Europol cannot identify the relevant ENU within four months, then it must delete the data. Europol may not send requests to private parties to obtain personal data. However, private parties have come to hold significant amounts of personal data relevant to law enforcement. The impact assessment identifies issues with increased risk of delays, loss of information and a lack of legal certainty for private parties when submitting personal data to Europol. For instance, private...
parties do not have a contact point when they want to share multi-jurisdictional or non-attributable data sets with law enforcement. It is also time and resource intensive for national authorities to analyse multi-jurisdictional and non-attributable data sets through national and intergovernmental solutions, or for them to exchange data with private parties established in other jurisdictions, while Europol cannot help Member States to cooperate effectively with private parties, owing to legal restrictions. Private parties face difficulties when receiving requests from multiple jurisdictions.

**Big data challenge for law enforcement authorities**

Criminal investigations provide law enforcement authorities with large and complex datasets that they need to process. However, this requires intensive resources, in particular when the data relates to cross-border crimes. While Europol has received high volumes of data from Member States in order to support criminal investigations – as the European Cybercrime Centre or the European Counter-Terrorism Centre have developed the necessary expertise and capabilities to this end – structural legal concerns related to processing them have come to the fore. As mentioned, the EDPS has admonished the agency for processing personal data of individuals not linked to a crime. In its ‘Europol big data challenge’ decision, the EDPS highlights that it is not possible for the agency to establish from the outset that all the information contained in the large datasets received complies with the limitations of the Europol Regulation, therefore leading to the unlawful processing of personal data of a vast number of people, beyond the categories allowed (Annex II of the regulation). Moreover, the principle of data minimisation is breached as the data continues to be stored by Europol beyond the time limits allowed. In this context, the Commission impact assessment points out that the Europol Regulation does not take account of the specific requirements for the processing of large and complex datasets. In particular, digital forensics requires the storage of the entire dataset for the duration of the criminal investigation and, possibly, subsequent judicial proceedings; moreover, it involves the processing of data that is not relevant for a criminal investigation. Furthermore, the regulation does not allow for an initial processing by Europol of personal data submitted by Member States with the sole purpose of determining whether such data pertains to the specific categories of data subjects set out in Annex II.

**Gaps on innovation and research relevant for law enforcement**

Law enforcement authorities are facing the challenge of criminals exploiting new technologies for their crimes. While various tools, such as artificial intelligence, could address this issue, not all Member States have the resources to invest in technological innovation or the skills to process the large data sets required to this end. In this context, Europol is seen as the suitable forum to help Member States in the area of innovation for law enforcement, by coordinating their efforts. However, the Europol Regulation does not give the agency a mandate to this end. Nor does it provide a clear legal basis for Europol to contribute to research and innovation activities relevant for law enforcement and to implement its own research projects, although the agency may currently perform certain related activities. In addition, the regulation does not provide a legal basis for the processing of data for the training, testing and validation of algorithms for the development of tools, including AI-based tools, for law enforcement, which triggered an EDPS inquiry.

EPRS has conducted an initial appraisal of the Commission’s impact assessment. It concludes that, despite attempting to explain the existing problems in detail, the impact assessment presents a number of shortcomings, in terms of the range of policy options considered, the impact of the policy options, and its analysis of the fundamental rights impact, which could have been more thorough.

**The changes the proposal would bring**

On 9 December 2020, the European Commission presented the new proposal to amend 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 in research and innovation, as part of a package of counter-terrorism measures. The proposal is based on
Article 88 TFEU. Owing to its Treaty opt-out, Denmark is not taking part in the adoption of the regulation. Ireland has notified its intention to take part in the regulation's adoption and application.

The proposal seeks to strengthen Europol's mandate within the tasks and mission established by the Treaty with regard to three main aspects: enabling Europol to cooperate effectively with private parties; allowing Europol to process large and complex datasets, addressing thus the big data challenge for law enforcement; and strengthening the agency's role on research and innovation. In addition, the proposal aims to assign a series of new tasks to Europol, to strengthen the data protection framework applicable to the agency, and to provide legal clarifications concerning certain existing tasks of the agency. The Commission had specified that the adoption of the proposal would not affect the obligation to conduct an evaluation under Article 68 of the Europol Regulation, by 1 May 2022 (with the proposal adopted, the obligation is now considered fulfilled).

Cooperation with private parties

The proposed legislative initiative enables Europol to cooperate effectively with private parties by setting new rules (Articles 26 and 26a). First, Europol will be able to receive personal data directly from private parties, in order to identify the national units concerned and provide them with the information necessary to establish jurisdiction, including the results from the processing of that data. The agency may also ask Member States to request private parties to share additional information. Europol will not be allowed to request personal data directly from private parties. Moreover, Europol may receive personal data from private parties established in third countries, but it may only transfer such data to either a Member State or a third country if there is an agreement for the exchange of personal data with that country or an EU adequacy decision.

Second, Europol may transfer personal data to private parties, on a case-by-case basis, under certain conditions, including for the purpose of informing that private party that data received were insufficient to identify the ENU concerned. If the private party is not established in the EU or in a third country with which Europol may exchange personal data (on the basis of an agreement or adequacy decision), then the Executive Director of Europol may authorise the transfer under strict conditions; such transfers may not be 'systematic, massive or structural'. Third, Europol may make its infrastructure available for exchanges between Member States and private parties. Where the crime that is the object of the data exchanged falls outside Europol's competences, the agency will not have access to the data. In addition, and linked to crisis response, Europol will be enabled to exchange personal data with private parties to prevent the large-scale dissemination of online terrorist or violent extremism content relating to ongoing or recent events.

Processing large and complex datasets

The proposal introduces the possibility for Europol to conduct an initial analysis of personal data received in order to establish whether such data falls within the categories of data subjects set out in Annex II (Article 18(5)(a)). On the proposal of the Europol Executive Director, the Management Board must further specify the conditions for processing such data, after consulting the EDPS. Moreover, Europol is empowered to process personal data outside the established categories in certain situations (Article 18(a)):

- when a Member State or the European Public Prosecutor's Office (EPPO) sends an investigative case file to the agency for operational analysis in support of that specific criminal investigation (which must fall within Europol's mandate);
- when Europol assesses it cannot perform the operational analysis without processing personal data outside the categories allowed.

The personal data in the investigative case file may be processed for as long as that investigation continues; Europol may also store the investigative case file and the outcome of the operational analysis beyond the end of the investigation, at the request of the case file provider, for the sole purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process and
Strengthening Europol's mandate

for as long as the related judicial proceedings are ongoing. Upon a proposal from the Executive Director and after consulting the EDPS, the Management Board will further specify conditions for the processing of such data.

The same provisions apply when a third country that may share personal data with Europol (under an agreement or an adequacy decision) transmits an investigative case file to the agency for operational analysis, which supports a specific criminal investigation in a Member State or Member States. Europol must inform the EDPS; it must also verify that such data were not obtained through violating fundamental rights and that the amount of personal data is not manifestly disproportionate in relation to the investigation in the Member State.

Europol's role in research and innovation

The legislative initiative aims to strengthen Europol's role in research and innovation by introducing new related tasks for the agency: i) assisting the Commission in identifying key research themes, drawing up and implementing EU framework research programmes relevant to Europol's mandate (Article 4(a)); ii) supporting the screening of foreign direct investments (FDI) into the EU for security implications as regards technologies used by Europol or Member States for the prevention and investigation of crimes under Europol's mandate (Article 4(b)); iii) supporting Member States in relation to research and innovation activities relevant to the agency's objectives and implementing such activities, including the development, training, testing and validation of algorithms for the development of tools (Article 4(1)(t)).

Article 18(2)(e) allows the processing of personal data for research and innovation, while Article 33a sets out additional safeguards to this end. These include the prior authorisation of the Executive Director for any project and informing the Management Board and the EDPS prior to its launch; and specific rules on processing and accessing the data, and on their deletion, etc.

Other new tasks proposed and legal clarification of existing tasks

Besides the three main issues above, the Commission proposes other new tasks for Europol:

- **enabling the agency to enter data into the Schengen information system (SIS),** subject to consultation of the Member States and authorisation of the Executive Director, on the suspected involvement of a third country national in an offence under Europol's mandate, based on information received from third countries/international organisations (Article (1)(r)). The proposal is linked to another legislative initiative to amend Regulation (EU) 2018/1862 on the Schengen information system, thereby introducing a new alert category to be entered in SIS by Europol. The EDPS issued a specific opinion on this proposal on 10 March 2021;

- **strengthening Europol's cooperation with third countries** in specific situations and on a case-by-case basis, by allowing the Executive Director of the agency to authorise the transfer or categories of transfers of personal data to third countries (Article 25(5));

- **strengthening cooperation with the EPPO,** in line with the rules on transmission of personal data to EU bodies applicable to Europol; a working arrangement between Europol and the EPPO will have to be concluded (Article 20(a));

- **strengthening cooperation with the European Anti-Fraud Office (OLAF),** with Europol sending OLAF any information linked to possible illegal activity affecting the EU's financial interests (Article 21(8));

- **enabling joint operational analysis between Europol and Member States** in specific investigations (Article 20(2a)): in the context of analysis projects, Member States may enable Europol to make information directly available to selected Member States.

The proposal clarifies some aspects from a legal point of view and codifies existing tasks, inter alia:

- in specific cases where Europol considers that a criminal investigation should be initiated, Europol may ask the competent authorities of a single Member State (instead of two or
more currently) to initiate, conduct or coordinate an investigation of a crime which affects a common interest covered by a Union policy, without the requirement of a cross-border dimension of the crime concerned;

- Member States may make the result of Europol operational and forensic analysis available to their relevant authorities, for use according to applicable restrictions and national criminal procedural law throughout the entire lifecycle of criminal proceedings;
- Europol may provide operational support on the ground to Member States' authorities in operations and investigations, at their request and in accordance with national law;
- Europol staff may give evidence in judicial proceedings in the Member States if authorised by the Executive Director.

**Data protection, fundamental rights and oversight**

The proposal aims to strengthen the data protection framework applicable to Europol by aligning its data protection regime with Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by EU institutions, bodies, offices and agencies, as requested by Parliament. Among others, the proposal adds biometric data to the categories of sensitive data that may be processed only when strictly necessary and proportionate for preventing and combatting crime under Europol’s mandate (Article 30(2)); provides further details on the function of Data Protection Officer of Europol (Articles 41(a) to (c)); and includes a new article on keeping records of categories of data processing activities to reflect current practice (Article 39(a)).

Moreover, the Commission recognises the proposal’s impact on fundamental rights, as enshrined in the EU Charter. However, it argues that it thoroughly assessed the policy options’ impact on fundamental rights in preparation for the proposal, which led to the rejection of those options that could have had a serious adverse impact and to the inclusion of detailed safeguards for those policy options that required a necessary limitation of the exercise of fundamental rights.

The proposal also aims to introduce a new obligation on the Commission in Article 68 (evaluation and review of the regulation), namely to submit a report to Parliament and Council, after three years from its entry into force, evaluating the operational benefits of the new competences assigned to Europol as regards: research and innovation for the development, training, testing and validation of algorithms (Article 18(2)(e)); the initial processing by Europol of personal data with the sole purpose of determining whether such data pertains to the specific categories of data subjects in Annex II of the Europol Regulation (Article 18(5a)); processing of personal data outside the categories of data subjects set out in Annex II for the purpose of operational analysis in a specific criminal investigation or when Europol assesses that it cannot carry out the operational analysis without processing personal data outside the categories allowed (Article 18a); the exchange of personal data with private parties (Articles 26 and 26a). The report must assess the impact of these activities on fundamental rights and freedoms as enshrined in the EU Charter.

The proposal also aims to strengthen parliamentary oversight of Europol and its accountability. Article 51 is thus modified to include the obligation to provide the JPSG with annual information about: i) the number of cases in which Europol issued follow-up requests to private parties or requests to Member States for the transmission of personal data; ii) the number of cases where Europol processed personal data outside the Annex II categories in order to support Member States in a specific criminal investigation; iii) the number of cases when Europol issued alerts in SIS and the number of hits these alerts generated; and iv) the number of pilot projects in which Europol processed data to train, test and validate algorithms for law enforcement.

**Advisory committees**

The European Economic and Social Committee (EESC) adopted its opinion on the strengthening of Europol’s mandate on 9 June 2021. The EESC welcomes the Commission proposal in all its aspects, but considers that bolder steps may need to be taken in the future, including to allow Europol to act
on its own initiative. The EESC also welcomes the creation of a new alert category in SIS. Finally, it is in favour of an independent review of Europol’s role and responsibilities, associating civil society.

The Committee of the Regions (CoR) did not plan a specific opinion on the proposal; however, in its opinion on the [counter-terrorism agenda for the EU](https://www.earc.europa.eu/en/) adopted on 14 October 2021, the CoR states its support for a reinforced mandate for Europol.

### National parliaments

The deadline for the submission of reasoned opinions on grounds of subsidiarity and proportionality expired on 30 March 2021, with none of the national parliaments raising subsidiarity concerns. Nevertheless, some parliaments, such as the [Dutch Senate](https://www.wettensoed.nl/), raised some concerns, in the framework of the political dialogue with the Commission, related to the fundamental rights safeguards; to the risks arising from the possibility of third countries making direct financial contributions to Europol; and to the ownership of the data transferred to Europol by private parties.

### Stakeholder views

In reply to the Commission’s [public consultation](https://ec.europa.eu/home-affairs/what-we-do/bureau-europol/europol-consultation-2021_en), digital and internet service provider associations emphasised the need for a voluntary system, which must also be in full compliance and aligned with fundamental rights and relevant legislation, most notably the General Data Protection Regulation (GDPR). Second, they asked for clarifications regarding the scope of crimes covered by the new regime, also pointing out that it should avoid overlap or conflict with existing and future EU law instruments (European Investigation Order Directive and the draft regulation on European production and preservation orders for electronic evidence). In fact, some contributions emphasised that a prior thorough review of the Europol Regulation under Article 68 would have been preferable, as well as finalising the e-evidence negotiations, before issuing the proposal.

[Statewatch](https://www.statewatch.org/) concurred that prior evaluation of Europol’s mandate and tasks was necessary and also argued there was no need to expand Europol’s mandate to increase its engagement with private parties. Moreover, Statewatch considered the agency should not be processing data of non-suspects, while cooperation with non-EU states based on the negotiation of international agreements should not change, in order to uphold fundamental rights standards. Finally, Europol should not be given a role in entering data from third countries in SIS.

The European Data Protection Supervisor (EDPS) issued its [opinion](https://edps.europa.eu/) on the proposed amendments to the Europol Regulation on 8 March 2021. The EDPS recommends, not least, that the prohibition of systematic, massive or structural transfers should apply to all exchanges with private parties, including in the EU and that Europol should carry out an assessment of the possible security risks posed from the opening of its infrastructure for use by private parties. Moreover, the opinion concludes that safeguards should be strengthened with regard to derogations related to processing large and complex data sets, while further conditions and thresholds should be set for the processing of personal data outside the categories of data subjects listed in Annex II in support of a criminal investigation. The EDPS also asks for better definition of the scope of the research and innovation activities, as well as some concepts in the proposal, such as ‘categories of transfers’.

In its May 2021 [position paper](https://www.ccbe.org/), the Council of Bars and Law Societies of Europe (CCBE) considers the adoption of the proposal premature in light of the Europol Regulation’s evaluation. The CCBE also notes that any direct or indirect access to citizens’ data must be proportionate and limited to what is strictly necessary.

In its June 2021 [position paper](https://www.edri.org/), European Digital Rights (EDRi) criticises the expansion of competences attributed to Europol without due consideration of its legal mandate as defined by the Treaties and proper evaluation of the efficiency and human rights compliance of its current missions and practices (e.g. data transfers with third countries). EDRi argues that allowing Europol to enter alerts in SIS runs counter to Treaty provisions and raises legal and human rights concerns.
In October 2021, 26 civil society organisations addressed an open letter to MEPs, urging them to vote against the report and highlighting the risk of invalidation by the EU Court of Justice.

At the same time, the Meijers Committee (Standing Committee of Experts on International Migration, Refugee and Criminal Law) issued a number of recommendations: including a strict necessity test for the processing of personal data for research and innovation; providing for clear and sufficient safeguards regarding new data processing powers; ensuring that procedural and other legal requirements protecting individual rights are not circumvented when Europol receives personal data directly from private parties; requiring a decision by a public prosecutor or an investigating judge prior to Europol transmitting personal data to private parties; and clarifying Europol’s relationship with EPPO.

In a study conducted for the European Parliament, the authors argue that the proposed reform would radically transform the nature and powers of Europol and its relationship with key stakeholders without introducing adequate safeguards. They formulate a number of recommendations to enhance the proposal, suggesting possible ways forward.

**Legislative process**

In Parliament, the file was assigned to the Committee on Civil Liberties, Justice and Home Affairs (LIBE), rapporteur: Javier Zarzalejos (EPP, Spain). The Committee on Budgets adopted its opinion on 31 May 2021. The LIBE committee adopted its report on 12 October 2021, with 47 votes in favour and 16 against. In parallel, LIBE adopted its report (same rapporteur) on the proposal amending the SIS Regulation as regards the entry of alerts by Europol. LIBE adopted its decision to enter into interinstitutional negotiations on both files, confirmed by a vote in plenary on 21 October 2021.

In its position, the Parliament clarifies the provision on Europol’s right to request the initiation of investigations, stating that Europol should do so in relation to ‘a specific crime which affects a common interest covered by a Union policy but is not of a cross-border nature’. It also clarifies provisions on data protection and the role of Europol’s Data Protection Officer, and proposes to appoint a fundamental rights officer at Europol, responsible for monitoring the agency’s efforts to ensure respect for fundamental rights in all its activities and tasks, notably its research and innovation projects and its exchanges of personal data with private parties. Europol operational staff should receive mandatory training on fundamental rights, including data protection. Regarding Europol cooperation with private parties, Parliament clarifies that Europol could ask Member States to provide it with personal data from private parties established in their territory, but that such requests should be reasoned, targeted and strictly limited to what is necessary. Europol should carry out an assessment of the possible security risks posed by the opening of its infrastructure for use by private parties and, if necessary, take preventive and mitigating measures. Like the Council, Parliament is in favour of extending Europol’s ability to transfer personal data to third countries beyond existing possibilities (adequacy decision or cooperation agreement). Parliament supports the Commission proposal to enable Europol to enter third-country sourced information on third-country nationals in the SIS, clarifying however that priority is given to Member States. Finally, the Parliament stresses that providing Europol with additional capabilities should go hand in hand with reinforcing democratic oversight, transparency and accountability, namely by strengthening the role of the Joint Parliamentary Scrutiny Group.

The Council of the EU adopted its negotiating position in June 2021. Compared with the initial Commission proposal, the Council extended the options for Europol’s cooperation with third countries, introducing the possibility to transfer personal data to third countries, where appropriate safeguards have been provided for in a legally binding instrument (e.g. bilateral agreements) or are established as existing on the basis of Europol’s self-assessment. The Council also clarifies the rules for access to Europol’s data by the EPPO, insisting on the ‘data ownership principle’ (i.e. restrictions indicated by the entity that provided Europol with the information, including third countries and international organisations). Similarly, to process data provided for a research and innovation
Strengthening Europol’s mandate

project, Europol should seek the data owner’s consent. As to new Europol competencies, the Council opposes the proposed role for Europol in screening foreign direct investments and its ability to request the initiation of investigations without a cross-border dimension. The Council considers that ‘information alerts in the interest of the Union’ should be entered into SIS by the Member States rather than by Europol. Europol should support them by proposing the entry of alerts based on data from third countries and international organisations.

**Interinstitutional negotiations** began in October 2021, and on 1 February 2022, the Council and the Parliament reached a [provisional agreement](#) on the revision of the Europol Regulation.

Regarding the processing of personal data, Europol may process investigation data, outside of the Annex II categories, for as long as this supports the specific criminal investigation. Europol may also pre-analyse personal data received, with the sole purpose of establishing whether the data fall under the Annex II categories; if that is not the case, Europol should delete the data. Moreover, Europol is mandated to support Member States by processing large and complex datasets to detect cross-border links in specific criminal investigations. Europol may also process data received from third countries to support a specific criminal investigation in one or more Member States, if the third country has an adequacy decision or international agreement with the EU, a cooperation agreement or a legally binding instrument which includes appropriate safeguards and the data have been acquired in accordance with national criminal law provisions; furthermore, the data should not be collected in violation of fundamental rights and not be manifestly disproportionate to the investigation. The Executive Director of Europol is empowered to transfer personal data to third countries on a case by case basis, under specific circumstances. Other transfers should be allowed only when appropriate safeguards have been provided in a legally binding instrument or where Europol concludes through a thorough assessment that appropriate safeguards exist.

Europol may receive personal data from private parties (lawfully and on a voluntary basis) and may also transfer data to private parties in specific cases where necessary and proportionate, with the purpose of helping Member States to establish jurisdiction. Where data are insufficient to determine the Europol national unit concerned, Europol may inform the private parties, who may then share additional information. With prior authorisation of the Executive Director, Europol may also transfer personal data to private parties not established in the EU or in a country with which there is no agreement or adequacy decision or a legally binding instrument establishing safeguards. Europol is also allowed the possibility to exchange relevant personal data with private parties established in the EU or in a third country with which there is an agreement in situations related to the dissemination of terrorist content or of child sexual abuse materials.

In respect to its new role in research and innovation, Europol is mandated to conduct projects on matters covered by the Regulation. The agency may process personal data only when strictly necessary and the objective of the project cannot be attained through the use of non-personal data. Europol may not process data without the consent of the data originator and respect for fundamental rights must be ensured. For each project, Europol should carry out a data protection impact assessment.

In addition, Europol will help Member States in processing data from third countries or international organisations by proposing to Member States to issue alerts in SIS under a new category of alerts on third-country nationals. The agency, through its Executive Director, will also be able to propose to national authorities to start investigations of non-cross border crimes affecting common EU policies and will support Member States in FDI screening in the area of crimes covered by its mandate. Moreover, the EPPO may access Europol data on a hit/no hit basis. Parliamentary scrutiny of the agency is strengthened, the agency having to provide detailed annual information on the use of the new tools at its disposal, in particular on research and development projects and the establishment of new centres within Europol, and a new fundamental rights officer is established. On the other hand, the [EDPS has criticised](#) the Regulation for having considerably expanded Europol’s mandate.
on processing of personal data without compensating with strong data protection safeguards and without ensuring appropriate oversight.

On 4 May 2022, Parliament adopted the legislative resolution formally approving the provisional agreement, with 480 votes in favour, 143 against and 20 abstentions. Four Commission statements (on the implementation of the mechanism for Europol to propose the issuing of alerts in the Schengen Information System; on relations between Europol and the EPPO; on the provisions for Europol’s cooperation with third countries; and on the strengthening of Europol-Interpol cooperation) and one Council statement on Interpol’s red notices are annexed to the resolution. On 24 May 2022, the Council adopted the act corresponding to Parliament’s position. Regulation (EU) 2022/991, published in the Official Journal on 27 June 2022, entered into force on 28 June 2022. The proposal on the entry by Europol of alerts in SIS, approved in June 2022, is awaiting signature.

EUROPEAN PARLIAMENT SUPPORTING ANALYSIS


OTHER SOURCES

Strengthening Europol’s mandate: cooperation with private parties, processing of personal data, and support for research and innovation, Legislative Observatory (OEIL), European Parliament.

Strengthening Europol’s mandate: entry of alerts in SIS, Legislative Observatory (OEIL), European Parliament.

ENDNOTES

1 These categories are specified in Annex II of the Europol Regulation.

2 Europol began setting up the Innovation Lab, to be composed of four functions: projects; an observatory; a network of innovators; and the EU Innovation Hub for Internal Security. The Innovation Lab has been coordinating Europol’s involvement in Horizon 2020 project proposals and in the implementation of projects already awarded.

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.

€uropean Union, 2022.

epres@ep.europa.eu (contact)

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

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

http://epthinktank.eu (blog)

Third edition. The ‘EU Legislation in Progress’ briefings are updated at key stages throughout the legislative procedure.