Empowering the police, removing protections: the new Europol Regulation

statewatch

About this report

Authors: Jane Kilpatrick, Chris Jones

Research: Chris Jones, Jane Kilpatrick, Romain Lanneau, Yasha Maccanico

Our thanks to Chloé Berthelemy and Eric Töpfer for their comments, insights and suggestions.

Cover image: Europol

Published by *Statewatch*, November 2022

This report was produced as part of the project 'Building the biometric state - EU agencies and interoperable databases', supported by *Privacy International*.

About Statewatch

Statewatch produces and promotes critical research, policy analysis and investigative journalism to inform debates, movements and campaigns for civil liberties, human rights and democratic standards.

statewatch.org

(+44) (0) 203 393 8366

c/o MayDay Rooms
88 Fleet Street
London EC4Y 1DH
UK

Support our work: make a donation

Scan the QR code or visit: statewatch.org/donate

Join our mailing list

statewatch.org/about/mailing-list

Registered UK charity number: 1154784
Registered UK company number: 08480724
Registered company name: The Libertarian Research & Education Trust
Registered office: 88 Fleet Street, London EC4Y 1DH, UK.

Contents

Abbreviations used in this report

AP	Analysis Project
API	Advance Passenger Information
BMS	Biometric Matching System
CIR	Common Identity Repository
FRO	Fundamental Rights Officer
DPO	Data Protection Officer
DSC	Data Subject Categorisation
EAS	European Analysis System
ECRIS-TCN	European Criminal Records Information System for Third-Country Nationals
EDPS	European Data Protection Supervisor
EES	Entry/Exit System
EIS	Europol Information System
EMPACT	European Multidisciplinary Platform Against Criminal Threats
EPPO	European Public Prosecutor's Office
ESP	European Search Portal
ETIAS	European Travel Information and Authorisation System
JPSG	Joint Parliamentary Scrutiny Group
MID	Multiple-Identity Detector
MOCG	Mobile Organised Crime Group
OLAF	European Anti-Fraud Office
PeDRA	Personal Data for Risk Analysis
PNR	Passenger Name Record
SIENA	Secure Information Exchange Network Application
SIS	Schengen Information System
VIS	Visa Information System

1. New powers for European police

In 2022 the legal basis of the European Union Agency for Law Enforcement Cooperation, better known as Europol, was revised. Changes were needed, argued the European Commission, because "Europe faces a security landscape in flux, with evolving and increasingly complex security threats." This created "pressing operational needs,"[1] and reforms to the 2016 Regulation governing the agency[2] were agreed by the Council of the EU and the European Parliament in early June, coming into force 20 days later.[3]

The changes make the agency responsible for a vast number of new tasks and massively expand the scale and scope of the agency's ability to access and process data. Given Europol's role as a 'hub' for information processing and exchange between EU member states and other entities, the new rules thus increase the powers of all police forces and other agencies that cooperate with Europol. However, despite this increase in data powers, the new rules significantly lower the data protection requirements governing the agency.

This report aims to provide an overview of the powers and problems introduced by the revised legal basis, so that civil society, elected officials, and anyone with an interest in the matter is able to understand the role of the agency better. It is based on an analysis of Europol's legal basis, other relevant legislation, and publicly-available documentation.

Historical background

Europol has existed since the early 1990s, when the Europol Drugs Unit was set up through an international convention. Then, as now, its primary purpose was to gather, analyse and share information amongst the member states and other entities, such as international organisations or non-EU states. Its role was expanded by ministerial decision prior to the signing of the Europol Convention in 1995.[4] This was followed by a Council Decision in 2009, seemingly to avoid the parliamentary scrutiny that would be required by the Lisbon Treaty.

The European Parliament was, along with the Council, fully-involved in the decision-making for a Regulation that was approved in 2016. Controversial amendments to that Regulation were proposed in late 2020 and came into force in June 2022, massively expanding the agency's tasks and data processing powers at precisely the time when a number of data protection scandals were coming to light.

With the new powers now being implemented, it remains to be seen whether those responsible for supervising the agency's work – its management board, European and national parliamentarians, data protection authorities as well as Europol's own internal compliance functions, the Data Protection Officer and the new Fundamental Rights Officer – will have the resources and willingness necessary to ensure it complies with the law. Even if they do, the fact of the matter remains: the law has been changed to give the agency greater power, with less independent supervision and scrutiny.

[1] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2016/794, COM(2020) 796 final, 9 December 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0796

[2] 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), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0794

[3] Regulation (EU) 2016/794 (consolidated version), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0794-20220628

[4] 'EDU's mandate "extended"', *Statewatch*, 1 November 1994, https://www.statewatch.org/statewatch-database/edu-s-mandate-extended/

2. Key points

Scope of action

The 2022 amendments give the executive director the power to request that an investigation be opened into a crime involving just one member state, where it "affects a common interest covered by a Union policy," rather than where it falls within Europol's objectives. Previously, a crime had to affect two or more member states. There is still no obligation for the member state(s) to comply with such a request, but there is a requirement for Europol to inform the European Public Prosecutor's Office and Eurojust of these requests and the replies received, which appears to be a way to put pressure on national authorities.

The tasks the agency must undertake have been vastly expanded by the 2022 amendments and now include supporting national "special intervention units", supporting the identification of and investigation into suspects that present "a high risk for security", managing the EMPACT cooperation platform for joint police operations, and assisting in setting "research and innovation" priorities for the EU's security research programme.

Purposes of processing and data categories

While the law continues to include relatively tightly defined categories of persons on whom Europol may process data, **how the police define terms such as "suspect," "contact" or "associate" is open to interpretation** – as demonstrated by a case that has come to light recently, in which a peaceful activist was branded a terrorist by the Dutch police and had his data shared with Europol.

Europol is now allowed to process **vast quantities of data transferred to it by member states on people who may be entirely innocent and have no link whatsoever to any criminal activity.** This legalises an activity that was previously illegal, and for which Europol was admonished by the European Data Protection Supervisor.

The agency can now process "investigative data" which, as long it relates to "a specific criminal investigation", does not have to relate to any of the data subject categories set out in the Europol Regulation – that is to say, **it could cover anyone, anywhere** ("investigative data" can be received from member states, EU bodies, international organisations and non-EU states).

Europol has been granted the power to conduct "research and innovation" projects, which will likely be geared towards the use of big data, machine learning and 'artificial intelligence' techniques. For those projects, **it may process special categories of personal data (such as genetic data or ethnic background)** and may use any data it receives from member states, EU bodies, international organisations, third states or private parties in those projects, **without requesting permission.**

Scale of data processing

The scale of Europol's data processing has increased substantially in recent years, and the recent legal reforms are intended to increase this further: the number of objects stored in the Europol Information System (EIS) at end of 2021 was more than 1.5 million, **an increase of more than 280% since 2016**; and the number of searches in the EIS **increased by 753% between 2016 and 2021**, when there were more than 12 million searches.

A proposal to revise the rules on information exchange between national law enforcement authorities will further increase the amount of data transmitted to Europol, by making it mandatory to copy the agency into messages sent via SIENA (Secure Information Exchange Network Application)

Sources of data

New powers for Europol to enter "information alerts" in the Schengen Information System, based on information received from third states, and proposals for it to provide "third country-sourced biometric data" for the Prüm network raise **the possibility of Europol being used as a data-laundering hub for information obtained in breach of the law, and for third states to use Europol as a conduit for harassing political opponents and dissidents**.

The 2022 amendments to the Europol Regulation **substantially loosen restrictions on international data transfers**, empowering the management board to authorise transfers of personal data to third states and international organisations **without a legal agreement in place.**

Priority states for cooperation with Europol include dictatorships, authoritarian and repressive regimes, such as Algeria, Egypt, Turkey and Morocco.

There is **no longer a requirement for the agency to "publish on its website and keep up to date a list of adequacy decisions**, agreements, administrative arrangements and other instruments relating to the transfer of personal data".

Europol can now contact private parties to retrieve personal data (via national units, which must request the data in accordance with their national law), but the member state through which Europol makes the request does not have to have jurisdiction over the crime in question.

In an "online crisis situation" or in cases involving the online dissemination of child sexual abuse material, **Europol can receive personal data directly from private parties.**

Europol can now **receive personal data obtained from private parties via third countries or international organisations**, and when the agency receives personal data from a private party established in a third country, **it can forward the data and "the results of its analysis and verification" on the basis of a Management Board decision**, without a legal agreement in place.

Europol may now receive and process information "originating from private persons", if received via a national unit, a third country contact point, or a third country or international organisation authority, but cannot contact private persons to obtain data.

Interoperability: large-scale and networked databases

Europol now has access to all six of the EU's centralised justice and home affairs databases, and legal reforms under negotiation may see it obtain access to the 'Prüm' network of national police databases, which currently cover DNA, fingerprints and vehicle registration data, and will likely come to include facial images and police records.

Within the interoperability architecture, **Europol has a key role in the "watchlisting" and profiling of individuals wishing to travel to the EU**, and is developing a 'European Travel Intelligence Centre' to ensure the comprehensive profiling and surveillance of international travellers.

Supervision and scrutiny

Europol's Data Protection Officer has been given an expanded set of tasks and powers, but **the possibilities for independent external oversight by the European Data Protection Supervisor have been substantially limited.**

The Management Board breached the new Regulation as soon as it came into force, by failing to consult the EDPS on implementing decisions setting out how Europol would process large datasets in order to provide "data subject categorisation".

The threshold for referring new data processing activities to the European Data Protection Supervisor (EDPS) for external scrutiny has been raised, and the EDPS has raised concerns over "recurrent issues" with the "risk assessment methodology" Europol uses to determine whether or not to refer a new data processing activity to the EDPS.

If Europol determines that the new processing operations "are particularly urgent and necessary to prevent and combat an immediate threat," **it can simply consult the EDPS and then start processing data without waiting for a response.**

The agency is now required to employ a Fundamental Rights Officer, although the rules provide less independence for this official than their counterpart at Frontex. **Europol's FRO is appointed by the Management Board "upon a proposal of the Executive Director," and "shall report directly to the Executive Director".**

The Joint Parliamentary Scrutiny Group (JPSG), made up of national and European parliamentarians and responsible for political supervision of Europol's work, has received some new powers (mainly with regard to information that must be shared with it by Europol) and must be consulted on Europol's multiannual work programme. However, its conclusions and recommendations remain non-binding upon the agency.

The JPSG is also mandated to set up a "a consultative forum" to provide "independent advice in fundamental rights matters," which is similar to a requirement that applies to Frontex. However, unlike Frontex's consultative forum, the JPSG's is not granted any particular powers by the new rules aside from being able to give advice.

3. Scope of action

3.1 Competence

Europol is competent for serious crime and terrorism.[5] The agency does not have executive powers – that is, its agents are not able to stop, detain or arrest anyone, unlike its counterpart agency in border control, Frontex, which now has a growing 'standing corps' of border guards who can be granted such powers. Its primary purpose is to receive, process and provide information to EU member states and its other 'partners'. The purpose of its information processing is, of course, ultimately intended to enable arrests and prosecutions. Other tasks entrusted to the agency include providing administrative support to policing networks and projects, and guiding the development of "research and innovation" activities for law enforcement agencies.

Aside from one exception (outlined below), a crime must concern two or more member states for Europol to become involved in an investigation. It may also become involved in investigations into "related criminal offences," of which there are three types:

- those committed to procure the means necessary to commit crimes for which Europol is competent;
- those committed to "facilitate or perpetrate acts" for which Europol is competent; and
- those committed to ensure impunity for acts for which Europol is competent.

While the agency's formal role is to "support and strengthen" the action of member states' law enforcement authorities, it has been granted increasing possibilities to "initiate, conduct or coordinate… a criminal investigation."[6]

Previously, Europol could request that member states open an investigation into "a crime falling with the scope of its objectives," where it affected two or more member states. The 2022 amendments give the executive director the power to request that an investigation be opened into a crime involving just one member state, where it "affects a common interest covered by a Union policy," rather than where it falls within Europol's objectives.[7] There is still no obligation for the member state(s) to do so, although there is some enthusiasm for such a power within the EU institutions, and a requirement for Europol to inform Eurojust and the EPPO about any such requests (and the response from member states)[8] seems to be a way to apply further pressure on national authorities to accept proposals sent from The Hague.

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

[6] Article 6(1), Regulation 2016/794 (consolidated version)

[7] Article 6(1a), Regulation 2016/794 (consolidated version)

[8] Article 6(4), Regulation 2016/794 (consolidated version)

3.2 Tasks

While the crimes for which Europol is competent have not been changed by the 2022 amendments, the tasks the agency must undertake have been vastly expanded. While the majority of these simply reflect the formal legalisation of tasks that the agency had already been carrying out on the basis of policy decisions (for example, the conclusions of the Justice and Home Affairs Council), the number of new activities is substantial.

They include:

- supporting national "special intervention units" (the ATLAS network, which amongst other things has previously expressed an interest in using drones fitted with explosives "as tactical support weapons and particularly to breach windows"[9]);
- supporting the identification of and investigation into suspects that present "a high risk for security";
- managing EMPACT (the European Multidisciplinary Platform Against Criminal Threats), which has been described as a "co-operation platform of the relevant Member States, EU institutions and agencies, as well as third countries and organisations (public and private)," that is used to organise, manage and evaluate joint police operations;[10] and
- assisting the European Commission in drawing up work programmes for the security research programme, currently known as 'Civil Security for Society'.[11]

A table setting out Europol's pre-existing and new tasks is contained in Annex I.

[9] 'EU: Special forces network seeks explosive drones for anti-terrorism operations', *Statewatch*, 10 November 2021, https://www.statewatch.org/news/2021/november/eu-special-forces-network-seeks-explosive-drones-for-anti-terrorism-operations/

[10] 'EU joint police operations target irregular migrants', *Statewatch*, 1 February 2014, https://www.statewatch.org/statewatch-database/eu-joint-police-operations-target-irregular-migrants-by-chris-jones/

[11] 'Civil Security for Society (the European security research programme)', https://eubudgets.tni.org/section4/#6

Police racism: old wine in new bottles?

The European Commission's consultation on the reform of Europol's legal basis took place as Black Lives Matter protests erupted across the globe. In this context, *Statewatch*'s submission to the consultation noted that "Europol's work cannot be isolated from… widespread and well-founded accusations of racist and discriminatory policing practices".[12]

This was not a new observation. In a 2019 publication, Eric Töpfer charted the ways in which racist police discourse and practices directed at Gyspy, Roma and Traveller communities were rebranded as action against "itinerant" and "mobile" organised crime groups. These were then transformed into a Europe-wide "threat", with significant help from Europol.[13]

In 2011, the police agency thought it was appropriate to include the following sentence in its annual *Organised Crime Threat Assessment*: "Bulgarian and Romanian (mostly of Roma ethnicity), Nigerian and Chinese groups are probably the most threatening to society as a whole."[14] Töpfer notes that after academics were invited to review Europol's assessments in 2013, "references to Roma suddenly disappeared from the reports." They now include statements such as: "Mobile organised crime groups (MOCGs) continue to travel long distances from region to region and country to country committing organised property crime."

That report goes on to veer wildly between condemning the use of ethnic classifiers for criminal groups and actively supporting it: "Nationality, ethnicity… such approaches are often reductive and do not necessarily highlight the most characterising element of the network. In some cases, classifying criminal networks according to national or even ethnic homogeneity can be relevant for an investigation," it argues.[15] Elevating "MOCGs" to a pan-European priority appears to be, at least in part, a case of placing old wine in new bottles.

In this context, *Statewatch*'s submission to the consultation called for a broad public debate and thorough evaluation of Europol's powers and practices, including the practices of the member states from which it receives so much data. Instead, the opposite happened. The 2016 Regulation obliged the Commission to produce, by 1 May 2022, an evaluation of Europol's "impact, effectiveness… efficiency… [and] working practices."[16]

With the law undergoing changes, no such evaluation was produced.[17] There is of course no guarantee that it would offer a more critical examination of Europol's working practices: such reports are usually an exercise in validating the desires of interior ministries and other officials. But whatever the scale and scope of its scrutiny, it is now not due until 1 May 2027.[18]

[12] 'Europol: plans afoot to legalise unlawful acts', *Statewatch*, 9 July 2020, https://www.statewatch.org/news/2020/july/europol-plans-afoot-to-legalise-unlawful-acts/
[13] Eric Töpfer, 'The EU's Fight Against "Itinerant Crime": Antigypsyist Policing Under a New Name?', *Dimensions of Antigypsyism in Europe*, ENAR/Central Council of German Sinti and Roma, 2019, https://www.enar-eu.org/Book-Dimensions-of-Antigypsyism-in-Europe/
[14] Europol, 'Organised Crime Threat Assessment 2011', p.26, https://www.europol.europa.eu/media-press/newsroom/news/europol-organised-crime-threat-assessment-2011
[15] Europol, 'European Union Serious and Organised Crime Threat Assessment (SOCTA) 2021', p.20, https://www.europol.europa.eu/publication-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-socta-2021
[16] Article 68, Regulation 2016/794 (original version)
[17] A group of Green MEPs asked the European Commission reform was being proposed before the evaluation had taken place. The Commission said: "The proposal does not affect the obligation… to carry out an evaluation by 1 May 2022." See: Saskia Bricmont, Gwendoline Delbos-Corfield, Patrick Breyer, 'Evaluation of the Europol Regulation', question for written answer E-006360/2020, 20 November 2020, https://www.europarl.europa.eu/doceo/document/E-9-2020-006360_EN.html
[18] Article 68, Regulation 2016/794 (consolidated version)

4. Purposes of processing and data categories

Europol can process personal data for six purposes, with those purposes applying to different categories of individual.

Purpose	Categories of individuals
"Cross-checking": running searches of data held by Europol to try to identify connections between information related to convicts, suspects and "likely criminals"[19]	Suspects Convicts Likely criminals "Personal data that do not relate to the categories of data subjects listed in Annex II"
Strategic or thematic analysis	Suspects Convicts Likely criminals Witnesses Victims and potential victims Contacts and associates Informants "Personal data that do not relate to the categories of data subjects listed in Annex II" (for operational analysis only)
Operational analysis	
Facilitating information exchange between Member States, Europol, other Union bodies, third countries, international organisations and private parties	
Research and innovation projects	To be defined for each project
Producing 'most wanted' lists	Not specified in the Regulation

For the purposes of cross-checking, a (relatively) limited amount of data can be stored and accessed. For the purpose of analysis or facilitating information exchange, a staggering number of data categories may be involved, although this is hardly surprising, given the nature of police work. A full list of the data categories available for both purposes is included in Annex II.

While these categories may seem relatively well-defined, in practice they are open to the interpretations of national police forces, which supply the majority of the data held by Europol. It is oft-remarked that one person's terrorist is another's freedom fighter. In a case that has recently come to public attention, it appears that for the Dutch police, pacifist activists belong firmly in the terrorist camp. Frank van der Linde was put under surveillance by the Dutch police and labelled a terrorist. His data was subsequently passed on to Europol, which only deleted it after van der Linde tried to exercise his right to access the data the agency held on him.[20] The case is ongoing.

[19] "Likely criminals" is the term used throughout this report in place of the more unwieldy language used in the Europol Regulation: "persons regarding whom there are factual indications or reasonable grounds under the national law of the Member State concerned to believe that they will commit criminal offences in respect of which Europol is competent." See: Annex IIB, Regulation 2016/794 (consolidated version)

[20] 'Europol told to hand over personal data to Dutch activist labelled "terrorist" by Dutch police', *Statewatch*, 16 September 2022, https://www.statewatch.org/news/2022/september/europol-told-to-hand-over-personal-data-to-dutch-activist-labelled-terrorist-by-dutch-police/

Much of the data stored by Europol is used for Analysis Projects (APs). APs are composed of Europol analysts, who make use of the vast quantities of data stored in the Europol Analysis System (EAS) in the framework of criminal investigations. The results of their work are then provided to national authorities.

APs are structured by specific crimes (AP Cola deals with the production and trafficking of cocaine), themes (AP Asset Recovery does as its name suggests) or even specified nationalities ("AP Copper supports the prevention and combating of crimes involving ethnic Albanian criminal groups and associated organised crime groups"[21]). The work of AP Dolphin has often been of interest to researchers and activists: it "gathers intelligence and information… linked to terrorist groups… and other violent extremist groups active in the EU."[22] Given the tendency of the police to gather and store data on protestors, activists and campaigning movements – whether violent or not[23] – van der Linde's case is likely only the tip of the iceberg.

For the purposes of operational analysis and, "in exceptional and duly justified cases," cross-checking, the 2022 amendments empower Europol to process "personal data that do not relate to the categories of data subjects listed in Annex II [to the Regulation]." This is referred to as "investigative data", which must relate to "a specific criminal investigation".

Europol may process investigative data when a member state, Eurojust, the European Public Prosecutor's Office or a third country supplies it and Europol concludes that neither cross-checking nor operational analysis would be possible without the processing of personal data that, under normal circumstances, would be prohibited. After any judicial proceedings concerning that investigation have ended, the data should be deleted – unless there is a "related criminal investigation" ongoing in the EU, in which case storage can continue.

If Europol decides it needs the data for cross-checking, its assessment "shall be recorded and sent to the EDPS for information," but only after the investigation in question has ended. When a third country provides investigative data used for either cross-checking or operational analysis, "the Data Protection Officer may, where appropriate, notify the EDPS thereof." Presumably, it is up to the DPO to decide what is appropriate in this context.

The new rules also say that when a third country provides investigative data and Europol considers that the amount of data is "manifestly disproportionate or were collected in obvious violation of fundamental rights," it must be deleted. Quite how this safeguard is to be enforced remains, for now, a mystery. The Management Board is obliged to adopt decisions setting out "the conditions relating to the provision and processing" of investigative data,[24] although the text indicates that those decisions should cover the ongoing processing and

[21] Europol, 'Europol Analysis Projects', 6 December 2021, https://www.europol.europa.eu/operations-services-and-innovation/europol-analysis-projects

[22] Ibid.

[23] In the UK, "over more than four decades, at least 139 police officers were given fake identities to closely monitor the inner workings of more than 1,000 political groups." See: Paul Lewis and Rob Evans, 'Secrets and lies: untangling the UK 'spy cops' scandal', *The Guardian*, 28 October 2020, https://www.theguardian.com/uk-news/2020/oct/28/secrets-and-lies-untangling-the-uk-spy-cops-scandal. In France, the police were recently authorised to gather data on peoples' political beliefs and trade union activity, and the German state has a lengthy history of gathering data on activists. See: 'France: Green light for police surveillance of political opinions, trade union membership and religious beliefs', *Statewatch*, 13 January 2021, https://www.statewatch.org/news/2021/january/france-green-light-for-police-surveillance-of-political-opinions-trade-union-membership-and-religious-beliefs/; 'Suspicion files: German police databases on political activists', *Statewatch*, 10 April 2018, https://www.statewatch.org/analyses/2018/suspicion-files-german-police-databases-on-political-activists/

[24] Article 18a(5), Regulation 2016/794 (consolidated version)

storage of the data, and not the conditions that determine its admissibility for processing in the first place.

The final two grounds for processing listed above (research and innovation, and producing most wanted lists) were introduced by the 2022 amendments to the Europol Regulation, which also added "private parties" to the list of bodies with which Europol can facilitate the exchange of information (on this latter point, see further below).

"Research and innovation" is one of the key new tasks granted to Europol by the 2022 amendments. Even before the new powers had been proposed by the European Commission, the agency had set up an 'Innovation Lab' and an 'Innovation Hub' intended to monitor emerging technologies and their usefulness for law enforcement, and take part in projects aiming to develop them. Technologies of interest include big data, machine learning and augmented reality, amongst other things.[25]

Europol has been empowered to use "special categories" of personal data for its research projects (such as biometric or genetic data, data on racial or ethnic origin, sexual orientation, and so on), providing "appropriate safeguards" are put in place.[26] Furthermore, when it is provided with information by a member state, EU body, international organisation or third country for cross-checking, analysis or facilitating information exchange, it may also use that data in research and innovation projects, without requiring any explicit permission from the information provider.[27]

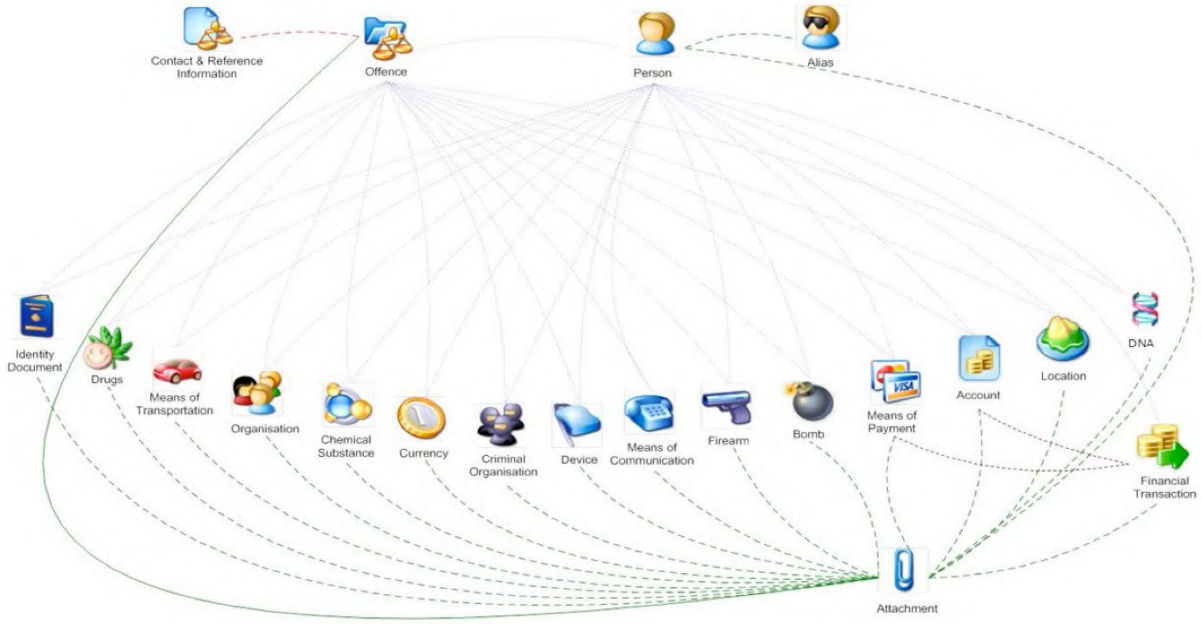


Figure 1: 'Object types' in the Europol Information System (EIS). Source: Europol presentation[28]

[25] 'Police seeking new technologies as Europol's "Innovation Lab" takes shape', *Statewatch*, 18 November 2020, https://www.statewatch.org/news/2020/november/eu-police-seeking-new-technologies-as-europol-s-innovation-lab-takes-shape/
[26] Article 30(2), Regulation 2016/794 (consolidated version)
[27] Article 29(1), Regulation 2016/794 (consolidated version)
[28] Europol presentation, 'EIS & QUEST', 3 February 2021, https://www.statewatch.org/media/1847/eu-europol-eis-presentation-2020.pdf

The big data challenge: "operational needs" versus the law

National law enforcement authorities were (and still are) responsible for ensuring the legality of data transfers to Europol.[29] However, for a number of years many of them had been sending vast quantities of personal data to The Hague and leaving it to Europol to assess whether it was allowed to process the data or not. As the EDPS has noted, ignoring this safeguard is dangerous: making data available to a European level police force "significantly magnifies the potential impact and risks for the data subject already existing at national level."[30]

Catherine de Bolle, Europol's executive director, raised the issue (referred to as the "big data challenge") with the European Data Protection Supervisor, who promptly opened an investigation. This concluded that the practice could not continue. The EDPS formally admonished the agency for breaking the law, and urged Europol "to implement all necessary and appropriate measures to mitigate the risks created by such personal data processing activities to data subjects," to be set out in an action plan.[31]

The plan duly appeared two months later, but when the EDPS raised questions about some of the measures it contained, Europol refused to make changes – particularly regarding the demand to set a maximum retention period for "large datasets lacking a DSC [data subject categorisation]." Instead, the agency asked the EDPS to accept limits that were included in the proposed amendments to the Europol Regulation, at that time under negotiation in the European Parliament and the Council of the EU. These were not retroactive: that is to say, they would only apply to data sent to Europol after the amendments came into force.

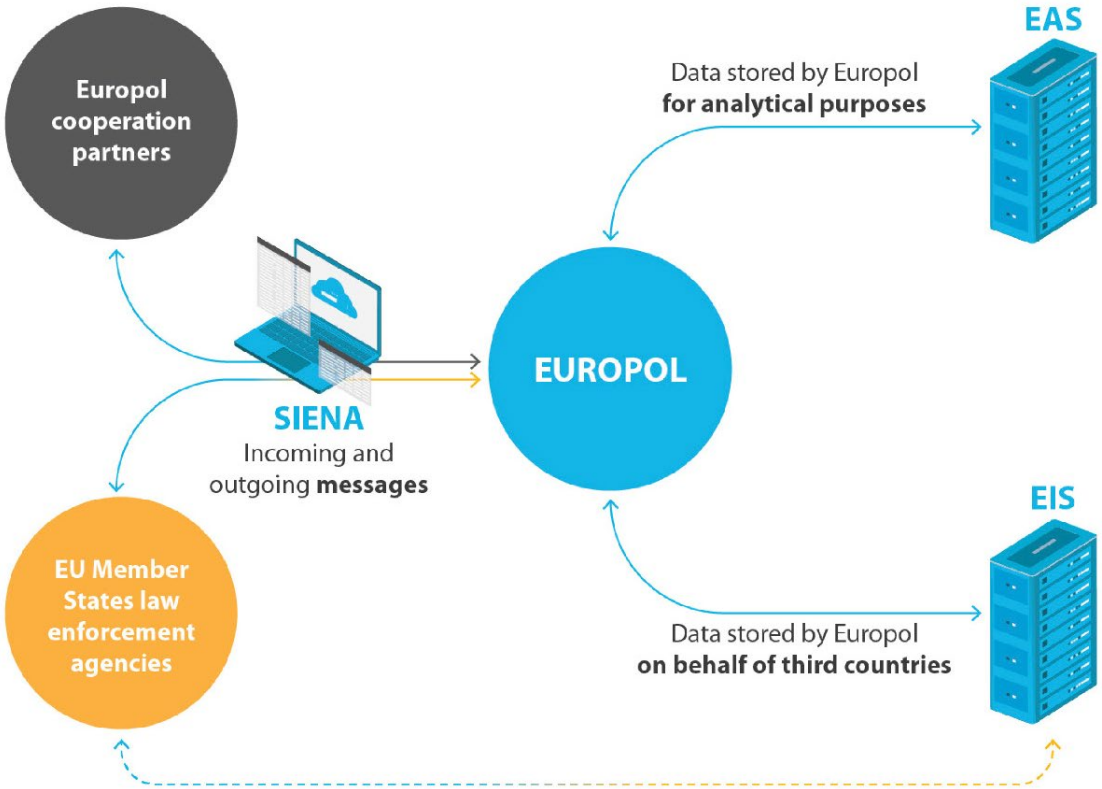
The EDPS did not like this idea. Nevertheless, despite acknowledging that the practices had no legal basis, it gave Europol some leeway. All data the agency received from the day after the EDPS order was published should be categorised or deleted within six months; all data it held on the day of the order should be categorised or deleted within 12 months.

A victory for data protection? Not quite. In response to the EDPS order, the French Presidency of the Council inserted new provisions into the proposed amendments to the Europol Regulation, which "would aim to further clarify the situation of the data currently in the possession of Europol, in particular in the context of the decision of the EDPS of 3 January 2022".[32] With the blessing of the European Parliament, the provisions made it into the final Regulation, effectively word for word.

The EDPS is now seeking to have them overturned in court, stating in no uncertain terms that "the provisions seriously undermine legal certainty for individuals' personal data and threaten the independence of the EDPS".[33] It remains to be seen what EU judges make of the matter, but separate provisions in the new amendments have now legalised the process of transferring large datasets to Europol for "data subject categorisation" processes.[34]

[29] Article 38(5), Regulation 2016/794 (consolidated version)
[30] 'EDPS Decision on the retention by Europol of datasets lacking Data Subject Categorisation', 1 October 2022, https://edps.europa.eu/system/files/2022-01/22-01-10-edps-decision-europol_en.pdf
[31] Ibid.
[32] 'Europol: Council Presidency proposes workaround for illegal data processing', *Statewatch*, 25 January 2022, https://www.statewatch.org/news/2022/january/europol-council-presidency-proposes-workaround-for-illegal-data-processing/
[33] EDPS, 'EDPS takes legal action as new Europol Regulation puts rule of law and EDPS independence under threat', 22 September 2022, https://edps.europa.eu/press-publications/press-news/press-releases/2022/edps-takes-legal-action-new-europol-regulation-puts-rule-law-and-edps-independence-under-threat_en
[34] Article 18a, Regulation 2016/794 (consolidated version)

5. Scale of data processing



The structure of the EIS, EAS and SIENA. Source: European Court of Auditors[35]

The amount of data processed by Europol – and thus made available to member states and other 'partners' – has grown substantially in recent years. For example, the number of objects stored in the Europol Information System (EIS) increased by 280% between 2016 and 2021, and the number of persons recorded in the EIS increased by 133% (figures are unavailable for 2021).

The EIS is a vast data store that can be searched by EU member state authorities as well as other bodies with which Europol has a cooperation or working agreement. The main purpose is "to provide a quick reference to data available on serious international crime," making it possible to "detect possible hits between different investigations."[36] Most of the data is inserted by EU member state authorities, but by a fine margin: as of 31 March 2020, there was nearly an even split between data provided by EU member state agencies (782,918 objects) and third party authorities (731,885 objects). Germany is by far the largest EU member state contributor to the EIS;[37] it is unknown which third parties provide the most information. However, a Europol presentation from February 2021 noted that there are "daily feeds by the FBI" via a dataloader.[38]

[35] European Court of Auditors, 'Europol support to fight migrant smuggling: a valued partner, but insufficient use of data sources and result measurement', 2021, https://op.europa.eu/webpub/eca/special-reports/europol-19-2021/en/index.html

[36] Europol presentation, 'EIS & QUEST', 3 February 2021, https://www.statewatch.org/media/1847/eu-europol-eis-presentation-2020.pdf

[37] 'EU: Beefing up police databases: plans for increased input, data quality roadmap, automation', *Statewatch*, 24 November 2020, https://www.statewatch.org/news/2020/november/eu-beefing-up-police-databases-plans-for-increased-input-data-quality-roadmap-automation/

[38] Europol presentation, 'EIS & QUEST', 3 February 2021, https://www.statewatch.org/media/1847/eu-europol-eis-presentation-2020.pdf

The addition of private parties as a potential data source (see below) will further swell Europol's databanks, as will the growing trend for national and other authorities to transmit vast quantities of data to Europol, now legalised by the 2022 amendments. It is worth recalling that the amount of information involved in the "big data challenge" alone reportedly amounted to "4 petabytes – equivalent to 3m CD-ROMs or a fifth of the entire contents of the US Library of Congress."[39]

The usage of Europol's systems has also grown enormously: indeed, at a rate far quicker than the amount of data it holds. The number of searches in the EIS increased by 753% between 2016 and 2021, a growth likely due in large part to concerted efforts to ease access to Europol's systems for national police forces. For example, QUEST (Query Europol's Systems) is an interface that gives police officers direct access to data held in the EIS and Europol's Analysis Projects, removing the need to go through the Europol National Unit and opening up access to a far greater number of potential users.[40]

At the same time, the amount of information exchanged via the Secure Information Exchange Network Application (SIENA) has also increased, almost doubling between 2016 and 2021. SIENA is used for information exchange between Europol liaison officers, analysts and experts, EU member state authorities, and third parties (such as EU agencies or non-EU states). A proposed Directive under discussion in the EU institutions would make SIENA the default mode of communication for national law enforcement authorities in many situations. It would also require that all information sent via the network be copied to Europol (currently, this is optional), further increasing the amount of data processed by the agency.[41]

Data processing by Europol	**2016**[42]	**2019**[43]	**2021**[44]
number of SIENA messages exchanged	869,858	1,242,403	1,542,606
number of SIENA cases initiated	46,437	84,697	122,898
number of entities connected to SIENA	757 organisational entities	1,744 operational mailboxes	-
total number of objects in the Europol Information System	395,357	1,453,186	1,502,499
number of person objects in the Europol Information System	103,796	241,795	-
number of searches performed in the Europol Information System	1,436,838	5,356,135	12,256,546

[39] Apostolis Fotiadis, Ludek Stavinoha, Giacomo Zandonini, Daniel Howden, 'A data 'black hole': Europol ordered to delete vast store of personal data', *The Guardian*, 10 January 2022, https://www.theguardian.com/world/2022/jan/10/a-data-black-hole-europol-ordered-to-delete-vast-store-of-personal-data

[40] Europol presentation, 'EIS & QUEST', 3 February 2021, https://www.statewatch.org/media/1847/eu-europol-eis-presentation-2020.pdf

[41] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on information exchange between law enforcement authorities of Member States, repealing Council Framework Decision 2006/960/JHA, COM(2021) 782 final, 8 December 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2021:782:FIN

[42] European Commission, SWD(2020) 543 final, 9 December 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2020:543:FIN

[43] Ibid.

[44] Europol, 'Consolidated Annual Activity Report 2021', p.61, https://www.europol.europa.eu/publications-events/publications/consolidated-annual-activity-report-caar-2021

6. Access to data

When an EU member state, EU body, third country or international organisation (but not a private party) provides information to Europol, they are entitled to place restrictions as to the purposes for which it can be processed and who may access it. If the information provider fails to categorise its data in this way, it can agree that Europol may do so on its behalf.[45]

Thus, the French authorities could decide that certain pieces of data should only be accessible to particular member states, or Frontex could decide that certain data should only be accessible to EU member states and not to any of the third countries that have access to Europol's databases. How strictly this works in practice is unknown. As one well-placed think tank, the *Centre for European Reform*, commented with regard to the potential for the UK to access data held in the EU's Schengen Information System after Brexit, "the UK could ask Europol or a friendly EU or Schengen country to run searches on its behalf, as the US and Canada do."[46]

Data submitted to Europol should be categorised either by the provider or Europol itself according to a '4x4' system of handling codes. This requires the assignment of a letter and a number to the source of the information, and to the information itself (for example A1, B1 or A3).

Source	Accuracy
(A) Where there is no doubt as to the authenticity, trustworthiness and competence of the source, or if the information is provided by a source which has proved to be reliable in all instances.	(1) Information the accuracy of which is not in doubt.
(B) Where the information is provided by a source which has in most instances proved to be reliable.	(2) Information known personally to the source but not known personally to the official passing it on.
(C) Where the information is provided by a source which has in most instances proved to be unreliable.	(3) Information not known personally to the source but corroborated by other information already recorded.
(X) Where the reliability of the source cannot be assessed.	(4) Information not known personally to the source and which cannot be corroborated.

This model was, ironically, imported into Europol from the UK policing model by the former executive director, Rob Wainwright (the UK previously used a 5x5x5 system and has now switched to 3x5x2[47]).

[45] Article 19, Regulation 2016/794 (consolidated version)
[46] Camino Mortera-Martinez, 'Plugging in the British: EU justice and home affairs', *Centre for European Reform*, 25 May 2018, https://www.cer.eu/publications/archive/policy-brief/2018/plugging-british-eu-justice-and-home-affairs
[47] College of Policing, 'Intelligence report', updated 26 January 2022, https://www.college.police.uk/app/intelligence-management/intelligence-report

7. Sources of data

Europol is able to receive data from and transmit data to:

- **member states**;
- **EU bodies, third countries and international organisations**; and
- **private parties**.

It may also "directly retrieve and process information, including personal data, from **publicly available sources**, including the internet and public data," and has access under certain conditions to all the EU's **large-scale justice and home affairs databases**.

The retrieving and processing of information (including personal data) may take place "by such means… necessary for the performance of its tasks," as long as the law provides for it. Any other legal rules that govern access to these data sources should take precedence over the Europol Regulation "in so far as they provide for stricter rules on access and use than those laid down by this Regulation."[48]

7.1 Member states

Europol can receive data from:

- national law enforcement agencies;
- Internet Referral Units (IRUs);
- Financial Intelligence Units (FIUs);
- other competent authorities.

In order to cooperate with Europol, **EU member states must establish a Europol national unit**, "which shall be the liaison body between Europol and the competent authorities of that Member State." The unit must have "access to national law enforcement data and other relevant data necessary for cooperation with Europol." Europol and national authorities (e.g. a particular police force or body, rather than the national unit) may also cooperate directly, but any information exchanged must be copied to the national unit, unless it requests otherwise.[49]

National units and competent authorities are under a legal obligation to "supply Europol with the information necessary for it to fulfil its objectives," and must ensure that their supply of information complies with national law. They are relieved from the obligation to supply information if doing so would be contrary to essential national security interests, jeopardise an ongoing investigation or an individual's safety, or in cases where the information concerns "specific intelligence activities in the field of national security."[50]

The way in which national authorities can transmit data to Europol (and access data held by the agency) varies from state to state. As noted in a report by the European Court of Auditors on Europol's role in investigations on migrant smuggling, "access to Europol's systems is centralised in some countries while investigators have direct access in others," which "limit[s] their ability to send the relevant information to Europol in a timely manner."[51]

National **Financial Intelligence Units (FIUs)** must also supply data to Europol, although only in response to "duly justified requests made by Europol through the Europol national

[48] Article 17(2), Regulation 2016/794 (consolidated version)
[49] Article 7, Regulation 2016/794 (consolidated version)
[50] Ibid.
[51] European Court of Auditors, 'Europol support to fight migrant smuggling: a valued partner, but insufficient use of data sources and result measurement', 2021, p.17, https://op.europa.eu/webpub/eca/special-reports/europol-19-2021/en/index.html

unit or, if allowed by that Member State, by direct contacts between the FIU and Europol."[52] FIUs are national bodies "responsible for receiving and analysing suspicious transaction reports and other information relevant to money laundering, associated predicate offences or terrorist financing." They must be granted "access, directly or indirectly, in a timely manner, to the financial, administrative and law enforcement information that they require to fulfil their tasks properly."[53]

The agency's databanks are also swelled by information gathered by **National Internet Referral Units (IRUs)**. The work of IRUs involves police officers scouring the web for material that breaches the terms and conditions of online service providers (for example, YouTube or Facebook) and referring it to those companies for removal. The agency hosts a central IRU database at its headquarters in The Hague, which is fed information from web surveillance carried out by national police units and Europol staff. In 2021 Europol's IRU apparently "monitored content on more than 400 online platforms and assessed a total of 19,677 pieces of content."[54]

Although the IRU sits within the European Counter Terrorism Centre, its remit has been expanded beyond terrorism.[55] In 2021, it took part in four "action days", targeting:

- right-wing violent extremism and terrorism;
- "the Internet Archive platform (archive.org), aiming to strengthen the public-private partnership and to enhance content moderation";
- online terrorist propaganda and violent jihadist ideology; and
- social media content related to migrant smuggling during the "Belarusian Crisis".[56]

According to a Council of the EU report, as of 31 March 2020, just over half of the data in the Europol Information System (almost 783,000 items) came from EU member states. Non-EU states provided almost 732,000 items.

Germany was by far the largest contributor of data, followed by the Netherlands, Belgium, Finland and the UK.[57,58] Around half the member states use automated data loaders to transfer national information to Europol, removing the burden of having to enter data manually, and having to repeatedly enter the same data in different systems. In 2011, 13 member states were apparently using data loaders;[59] according to a Europol report, by early 2021 this had apparently increased by just two, to 15. Member states were also demanding

[52] Article 12, Directive (EU) 2019/1153 of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offences, and repealing Council Decision 2000/642/JHA, https://eur-lex.europa.eu/eli/dir/2019/1153/oj

[53] Article 32, Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32015L0849#d1e2543-73-1

[54] Europol, 'Consolidated Annual Activity Report 2021', p.8, https://www.europol.europa.eu/publications-events/publications/consolidated-annual-activity-report-caar-2021

[55] Chris Jones, 'Policing the internet: from terrorism and extremism to "content used by traffickers to attract migrants and refugees', *Statewatch*, 28 March 2016, https://www.statewatch.org/news/2016/march/statewatch-analysis-policing-the-internet-from-terrorism-and-extremism-to-content-used-by-traffickers-to-attract-migrants-and-refugees/

[56] Europol, 'Consolidated Annual Activity Report 2021', p.21, https://www.europol.europa.eu/publications-events/publications/consolidated-annual-activity-report-caar-2021

[57] 'EU: Beefing up police databases: plans for increased input, data quality roadmap, automation', *Statewatch*, 24 November 2020, https://www.statewatch.org/news/2020/november/eu-beefing-up-police-databases-plans-for-increased-input-data-quality-roadmap-automation/

[58] Following the final departure of the UK from the EU legal order on 31 December 2020, Europol retained the data the UK had provided. Cooperation continued under the terms of the Trade and Cooperation Agreement, and the two parties have now also signed a working arrangement.

[59] 'General report on Europol's activities in 2011', Council doc. 10036/12, 24 May 2012, https://www.statewatch.org/media/documents/news/2012/may/eu-europol-annual-report-2011.pdf

"Support for additional Third Party dataloaders,"[60] although what precisely this means is unclear.

7.2 EU bodies, third countries, international organisations

Europol is entitled to "exchange all information, with the exception of personal data," with EU bodies, third countries and international organisations, provided it is "necessary for the performance of its tasks." Such exchanges should be governed by the rules on data protection in EU institutions, agencies and bodies,[61] as well as any specific rules governing EU bodies. Europol may also sign working arrangements with other EU bodies, although these cannot permit the exchange of personal data.[62] For this, there are different sets of rules for EU bodies on the one hand, and for third countries and international organisations on the other. Annex II to this briefing lists Europol's current cooperation agreements.

7.2.1 Personal data: EU bodies

Europol may transmit personal data to EU bodies that are legally entitled to process it[63] "if those data are necessary and proportionate for the legitimate performance of tasks of the recipient Union body," and "necessary for preventing and combating crime falling within the scope of Europol's objectives and in accordance with this Regulation".[64] When Europol receives a request from another EU body for personal data, it must verify the competence of that body to process it.[65]

When it comes to receiving personal data from EU bodies, the Europol Regulation states that the agency may receive such data "insofar as necessary and proportionate for the legitimate performance of its tasks."[66] Three other EU bodies are specifically mentioned in the Europol Regulation: the European Public Prosecutor's Office (EPPO), Eurojust (the European Union Agency for Judicial Cooperation) and OLAF (the European Anti-Fraud Office).

The requirement to establish the EPPO comes from Article 86 the Lisbon Treaty. The EPPO describes itself as the "independent public prosecution office of the European Union," responsible for "investigating, prosecuting and bringing to judgment crimes against the financial interests of the EU."[67] However, five member states do not participate – including Hungary and Poland, who have faced repeated accusations of corruption and embezzlement relating to EU funds.[68]

Europol is required to "establish and maintain a close relationship with the EPPO,"[69] which includes supporting the EPPO's investigations by "providing information and analytical support". The EPPO must also be granted "hit/no hit" access to data held by Europol "related

[60] 'EIS & QUEST', 3 February 2021, https://www.statewatch.org/media/1847/eu-europol-eis-presentation-2020.pdf
[61] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32018R1725
[62] Article 23, Regulation 2016/794 (consolidated version)
[63] In accordance with Article 72(2) of Regulation (EU) 2018/1725, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32018R1725#d1e4403-39-1
[64] Article 23(6), Regulation 2016/794 (consolidated version)
[65] Article 24(2), Regulation 2016/794 (consolidated version)
[66] Article 23(5), Regulation 2016/794 (consolidated version)
[67] https://www.eppo.europa.eu/en/mission-and-tasks
[68] Costanza di Francesco Maesa, 'Repercussions of the Establishment of the EPPO via Enhanced Cooperation', *eucrim*, 3/2017, https://eucrim.eu/articles/repercussions-establishment-eppo/#docx-to-html-fn8
[69] Article 20a(1), Regulation 2016/794 (consolidated version)

to offences that fall within the EPPO's competence".[70] In case a search results in a "hit", Europol has to assess whether it can share the information or not.[71] Europol is also obliged to report to the EPPO any criminal conduct it learns of that may fall within the EPPO's competence.[72]

Eurojust and OLAF also have access to data held by Europol on the basis of a "hit/no hit system,"[73] although Eurojust may be granted more extensive access to Europol's data. If the two agencies sign a working arrangement permitting it, then Eurojust can be granted the power to search all the data held by Europol that has been provided to it for "cross-checking aimed at identifying connections or other relevant links between information".[74] However, at the time of writing, the working arrangement between the two agencies dated back to 2009.[75] Similar to the obligations regarding the EPPO, Europol and the member states are obliged to engage in "coordination, cooperation or support in accordance with the mandate of Eurojust or OLAF," if they find information that indicates it is necessary.[76]

Amongst the other EU bodies with which Europol cooperates, its work with Frontex has come in for substantial critical scrutiny. A working agreement was signed between the two agencies in December 2015.[77] This allows Europol to receive personal data from Frontex "regarding persons who are suspected, on reasonable grounds, by the competent authorities of the Member States of the European Union of involvement in cross-border criminal activities," as defined in the agreement. This refers to activities "within the mandate of both Parties… in particular facilitation of illegal migration, trafficking in human beings, and other cross-border criminal activities."[78]

In July 2022 it was revealed that senior Frontex officials had ignored the advice of the agency's own data protection officer in drafting new rules for a project known as PeDRA: Personal Data for Risk Analysis. PeDRA had been functioning since 2016 "as a way for Frontex and… Europol to exchange data in the wake of the November 2015 Paris attacks by Islamic militants that French authorities had linked to Europe's then snowballing refugee crisis."[79]

Following the entry into force of the 2019 Frontex Regulation, the plan was to increase the border agency's ability to collect personal data to share with Europol. This went as far as including genetic data, sexual orientation and the scraping of social media profiles, and collecting data on victims and witnesses of "cross-border crime" as well as suspects. The plan appears to have faltered, for now: the minutes of an extraordinary meeting of the Frontex Management Board, held two weeks after media revelations about PeDRA, state:

> *"The MB [Management Board] was informed about the EDPS opinion on MB Decisions 68/2021 adopting the rules on processing personal data by the Agency and 69/2021 adopting the rules on processing operational personal data by the*

[70] Article 20a(3), Regulation 2016/794 (consolidated version)
[71] Article 20a(3), Regulation 2016/794 (consolidated version)
[72] Article 20a(4), Regulation 2016/794 (consolidated version)
[73] Article 21(1), Regulation 2016/794 (consolidated version)
[74] Article 21(2), Regulation 2016/794 (consolidated version)
[75] 'Agreement between Eurojust and Europol', 1 October 2009, https://www.europol.europa.eu/cms/sites/default/files/documents/Agreement_between_Eurojust_and_Europol.pdf
[76] Article 21(5), Regulation 2016/794 (consolidated version)
[77] Europol and Frontex, 'Agreement on Operational Cooperation', 4 December 2015, https://www.europol.europa.eu/cms/sites/default/files/documents/Agreement_on_Operational_Cooperation_between_the_European_Police_Office_Europol_and_the_European_Agency_for_the_Management_of_Operational_Cooperation_at_the_External_Borders_of_the_Member_States_of_the_European_Union_Frontex.pdf
[78] Ibid.
[79] Luděk Stavinoha, Apostolis Fotiadis and Giacomo Zandonini, 'EU's Frontex tripped in its plan for 'intrusive' surveillance of migrants', *Balkan Insight*, 7 July 2022, https://balkaninsight.com/2022/07/07/eus-frontex-tripped-in-plan-for-intrusive-surveillance-of-migrants/

Agency. The MB urged the Agency to present the amened [sic] draft decisions to the MB as soon as possible."[80]

7.2.2 Personal data: third countries and international organisations

Where necessary for the performance of Europol's tasks, the agency may also transfer personal data to non-EU countries and international organisations.[81] Until the entry into force of the 2022 amendments to the Europol Regulation, such exchanges were regulated by adequacy decisions approved by the European Commission, an international agreement between the EU and the state or organisation in question, or a cooperation agreement between Europol and that body, with the executive director able to sidestep these requirements in certain cases.[82]

There are currently 18 "operational agreements" in force, permitting the exchange of personal data. Europol also has a working arrangement with the UK that governs the exchange of personal data,[83] even though this is not supposed to be within the scope of working arrangements.[84] Annex II to this briefing lists all the cooperation agreements currently in place.

The 2022 amendments to the Europol Regulation loosen restrictions on international data transfers substantially. The Europol Management Board is now able to directly authorise transfers of personal data to third states and international organisations, so long as "appropriate safeguards with regard to the protection of personal data are provided for in a legally binding instrument," or where there is no law in place but where Europol concludes "that appropriate safeguards exist with regard to the protection of personal data."[85] Given the agency's track record on data protection issues, its ability to reach that conclusion should be called into question.

Equally concerning is the nature of the regimes with which Europol wishes to cooperate. The amendments on data transfers were included in the revised Europol Regulation due to the difficulties the EU has faced in reaching agreements with states on Europol's priority list for cooperation – Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia and Turkey. As *Statewatch* pointed out in response to the public consultation on the proposed changes to Europol's legal basis:

"The document refers to "long and complex negotiations" for international agreements hindering the possibilities for cooperation. Particular countries are not named, although it may be presumed that this refers at least in part to current negotiations with MENA states. Amongst those countries are dictatorships whose law enforcement authorities routinely abuse fundamental rights, including through torture

[80] 'Minutes of the Extraordinary Management Board Meeting 27 July 2022, via videoconferencing', 3 October 2022, https://prd.frontex.europa.eu/wp-content/themes/template/templates/cards/1/dialog.php?card-post-id=2722&document-post-id=10865

[81] Article 25, Regulation 2016/794 (consolidated version)

[82] Article 25 of the 2016 Regulation allowed the executive director to authorise transfers of personal data to international organisations or third states for five different reasons and in individual cases: "Derogations may not be applicable to systematic, massive or structural transfers." See: Article 25, Regulation 2016/794 (original version), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0794#d1e2199-53-1

[83] Article 11 is entitled 'Specific conditions for the exchange of personal data,' and deals with just that. See: Working and Administrative Arrangement, September 2021, https://www.europol.europa.eu/cms/sites/default/files/documents/wa_with_united_kingdom_-_implementing_the_tca.pdf

[84] As the agency's own website states: "Europol is permitted to conclude working arrangements which, similar to strategic agreements, govern the practical aspects of exchanging non-personal data and regulate all the practical aspects of the cooperation." See: Europol, 'Partners & Collaboration', updated 5 August 2022, https://www.europol.europa.eu/partners-collaboration

[85] Article 25(4a)(b), Regulation 2016/794 (consolidated version)

and ill-treatment. Many of the countries in question do not have data protection laws… "Long and complex negotiations" are exactly what should be expected in an attempt to reach an agreement with a dictatorship on the exchange of personal data between police forces."[86]

There are oversight requirements in relation to any such transfers, with Europol obliged to inform the European Data Protection Supervisor about "categories of transfers" based on an assessment by Europol that "appropriate safeguards exist with regard to the collection of personal data." A "category of transfers of personal data" is a term introduced by the 2022 amendments, defined as:

"…a group of transfers of personal data where the data relate to the same specific situation, and where the transfers consist of the same categories of personal data and the same categories of data subjects."

This could of course amount to a substantial amount of data on a substantial amount of people. If the transfers are based on the existence of a "legally binding instrument", no reporting to the EDPS is required, although records of such transfers (as well as those not based on law but authorised by the management board) must be kept and made available for EDPS inspection if requested.[87]

The revised Europol Regulation also undermines transparency and oversight regarding international data transfers in another way: there is no longer a requirement for the agency to "publish on its website and keep up to date a list of adequacy decisions, agreements, administrative arrangements and other instruments relating to the transfer of personal data".[88]

A further way in which Europol is being transformed into a hub for the receipt and transmission of international police data is through new rules on various EU databases, in particular the Schengen Information System and the Prüm network. This is discussed further below, in the section of this briefing dealing with interoperability.

7.3.3 Private parties

With the 2022 reform of Europol's legal basis, the police agency received new powers to exchange data with private parties, defined as "entities and bodies established under the law of a Member State or third country, in particular companies and firms, business associations, non-profit organisations and other legal persons".[89] The main changes allow Europol to contact private parties to retrieve personal data (via national units, who must request the data in accordance with their national law), and make it easier for Europol to receive personal data obtained from private parties via third countries or international organisations.

Europol can now request that national authorities obtain certain data from private parties on its behalf.[90] Specifically, the law now states that Europol can ask national units "to obtain, in accordance with their national law, personal data from private parties which are established or have a legal representative in their territory, for the purpose of sharing those data with Europol."[91] The Regulation makes it explicit that this does not require that the requested member state actually has jurisdiction over the crime in question:

[86] 'Europol: plans afoot to legalise unlawful acts', *Statewatch*, 9 July 2020, https://www.statewatch.org/news/2020/july/europol-plans-afoot-to-legalise-unlawful-acts/
[87] Article 25(8) Regulation 2016/794 (consolidated version)
[88] This was formerly mandated by Article 25(3), Regulation 2016/794 (original version)
[89] Article 2(f), Regulation 2016/794 (consolidated version)
[90] Article 26(6b), Regulation 2016/794 (consolidated version)
[91] Article 26(6b), Regulation 2016/794 (consolidated version)

> *"Notwithstanding the jurisdiction of Member States over a specific crime, Member States shall ensure that their competent authorities can process the requests referred to in the first subparagraph in accordance with their national law for the purpose of supplying Europol with the information necessary for it to identify the national units concerned."*[92]

This would appear to offer myriad ways in which data that would not be available to Europol in one member state can simply be accessed via another member state with a less restrictive legal regime: the rules have been changed so that the police can go data shopping. A further change to the rules states that if Europol receives data directly from private parties and wishes to retain it, it must identify a relevant national unit, which in turn must resubmit the data to Europol.[93]

The amendments that ease the exchange of data with third countries (see the previous section) are also intended to facilitate the increased exchange of personal data with private parties. When Europol receives personal data from a private party established in a third state, it can now "forward those data and the results of its analysis and verification" to another third country on the basis of a Management Board decision authorising such a transfer,[94] even if there is no international agreement or adequacy decision in place.[95]

Europol's communication infrastructure may also now be used for the exchange of information between states and private parties. Where those exchanges concern crimes that fall within Europol's mandate, the data should be shared with the policing agency. If they do not, Europol is to be considered a processor of that data, but will not have access to it.[96]

The revised Regulation contains a new article on "online crisis situations",[97] defined as:

> *"…the dissemination of online content stemming from an ongoing or recent real world event which depicts harm to life or to physical integrity, or calls for imminent harm to life or to physical integrity, and aims to or has the effect of seriously intimidating a population, provided that there is a link, or a reasonable suspicion of a link, to terrorism or violent extremism and that the potential exponential multiplication and virality of that content across multiple online services are anticipated".*[98]

The inspiration here is clearly incidents such as the Christchurch terrorist attacks in New Zealand, where 51 people were killed and 40 injured in attacks on two mosques. The attacks were live-streamed online by the killer.[99] In an "online crisis situation", Europol is now empowered to receive personal data directly from private parties for the purpose of analysis and comparison.[100] Similar provisions apply to situations involving "the online dissemination of child sexual abuse material".[101]

Europol may now also receive and process information "originating from private persons", if received via a national unit, a third country contact point, or a third country or international organisation authority.[102] However, if personal data is received from a person in a country

---

[92] Ibid.
[93] Article 26(2), Regulation 2016/794 (consolidated version)
[94] Article 26(4), Regulation 2016/794 (consolidated version)
[95] Article 25(4a), Regulation 2016/794 (consolidated version)
[96] Article 26(6c), Regulation 2016/794 (consolidated version)
[97] Article 26(1)(a), Regulation 2016/794 (consolidated version)
[98] Article 3(t), Regulation 2016/794 (consolidated version)
[99] Andrew Griffin, 'New Zealand attack video spreads across Twitter, YouTube and Reddit despite pleas from police not to share it', *The Independent*, 15 March 2019, https://www.independent.co.uk/tech/new-zealand-attack-video-shooting-mosque-christchurch-reddit-youtube-twitter-a8824131.html
[100] Article 26a, Regulation 2016/794 (consolidated version)
[101] Article 26b, Regulation 2016/794 (consolidated version)
[102] Article 27, Regulation 2016/794 (consolidated version)

not subject to a data protection adequacy decision, an international agreement with the EU, or a Management Board decision authorising personal data exchanges, "Europol shall forward that information only to a Member State or to such third country."[103] Europol cannot contact private persons to retrieve information of any kind.

7.2.4 Public sources

The Europol Regulation is not particularly informative regarding the use of public sources. It says that the agency "may directly retrieve and process information, including personal data, from publicly available sources, including the internet and public data."[104] The previous legal basis, a 2009 Council Decision, provided slightly more information, referring to "media and public data and commercial intelligence providers."[105] A 2012 booklet by Europol's Data Protection Office went further:

> *"…criminals, especially terrorist groups, often communicate through public websites. These groups will issue threats, claim credit for attacks or spread indoctrination material over the internet. So-called 'terror manuals' offer detailed instructions on how to organise attacks or build weapons and bombs.*
>
> *Europol may monitor those websites and analyse their information. From a European Union perspective, this adds significant value, since the evaluation of large amounts of data and the scrutiny of innumerable web pages in many different languages requires considerable technical and human resources that would not be available to a single Member State."*[106]

The document referred to the "Check the Web portal," which has since been incorporated into the work of the Internet Referral Unit (see above). Given that the booklet was written in 2012, it is reasonable to assume that the number of online public data sources available to the agency has increased exponentially.

7.3 Interoperability: large-scale and networked databases

One way in which Europol's access to data has been increased in recent years is through the ability to access large-scale EU databases and information systems. Following legal changes in recent years, the policing agency now has access to all six of the EU's centralised justice and home affairs databases, and legal reforms currently underway may see it obtain access to the 'Prüm' network of national police databases.

Although Europol has access to each of these systems via separate legal bases, the technical means by which they can be accessed by the agency – and other authorities – will be 'streamlined' through the introduction of the EU's "interoperability" architecture. This establishes a:

- European Search Portal (ESP, granting a user the ability to make simultaneous searches of any database(s) to which they have access);
- Shared Biometric Matching System (sBMS, facilitating biometric searches across the interconnected systems);
- Multiple Identity Detector (MID, which will be used for the automated detection of suspected false or fraudulent identities, through the large-scale comparison of "identity data")

[103] Article 27, Regulation 2016/794 (consolidated version)
[104] Article 17(2), Regulation 2016/794 (consolidated version)
[105] Article 25(4), Council Decision, 2009/371/JHA, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32009D0371
[106] 'Data protection at Europol', 2012, https://www.europol.europa.eu/sites/default/files/documents/europol_dpo_booklet_0.pdf

- Common Identity Repository (CIR, a new centralised database that will hold "identity data" from each of the underlying systems, bar the Schengen Information System; identity data consists of name, nationality, date of birth, sex/gender, fingerprints, facial image, and travel document information)

To date, the limited statistics available indicate that Europol makes rather limited use of its access to centralised EU databases. The introduction of the interoperability architecture is intended to change this situation, by simplifying law enforcement authorities' ability to access data that is, primarily, collected for administrative purposes: four of the six centralised databases primarily exist for immigration (EES, ETIAS, VIS) or asylum (Eurodac) purposes.

The current interoperability architecture – which largely only exists on paper, as many of the systems are under construction – is also intended to be a building block for the increased collection and integration of data sources in the future. Indeed, this is already happening: the "central router" that will be established under the revised 'Prüm' framework will be connected to the Common Identity Repository to allow simultaneous searches of national databases, Europol data and the CIR. An online 'map' produced by *Statewatch* provides a visual representation of the interoperability architecture and information on the systems and agencies involved.[107]

[107] https://statewatch.org/eu-agencies-and-interoperable-databases

7.3.1 Common Identity Repository (CIR)

The CIR is currently under construction, and the last publicly-stated date for its implementation was the end of 2023.[108] However, the initial plan was for it to be in place before then, and further delays would not be surprising. A recent Europol report suggests that the interoperability timeline as a whole has been put back further.[109]

Purpose

- Aiding the correct identification of persons registered in the EES, Eurodac, ECRIS-TCN, ETIAS, VIS
- Supporting the functioning of the Multiple-Identity Detector (MID)
- Easing access by national law enforcement authorities and Europol to data held in the EES, Eurodac, ECRIS-TCN, ETIAS and VIS

Data stored

- 'Identity data' – names, dates of birth, nationality, fingerprints, facial images and travel document information – from the five underlying databases (EES, Eurodac, ECRIS-TCN, ETIAS, VIS)

Conditions for access by Europol

- A search in the CIR by Europol must be for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences, Europol (as well as national authorities)
- A search must relate to "a specific case"
- There must be "a suspicion" that data on the person in question (whether a "suspect, perpetrator or victim") is stored in one of the underlying databases

Procedure for access

- Where a search by Europol leads to a 'hit' in the CIR, a response will be provided "indicating which of those EU information systems contains matching data"
- A request must be made to access the data in accordance with the rules concerning the underlying information system, although it should be noted that simply knowing which information system holds data on a person allows inferences to be drawn about that individual

[108] 'EU: Interoperability: Letter confirms delays in implementation of "complex and challenging" plan', *Statewatch*, 22 February 2022, https://www.statewatch.org/news/2022/february/eu-interoperability-letter-confirms-delays-in-implementation-of-complex-and-challenging-plan/

[109] The agency's report on the implementation of ETIAS refers to "the new milestones of the EU interoperability agenda endorsed by the Justice and Home Affairs Council on 11-12 July 2022, which set the new entry into operation date for ETIAS to mid-November 2023." Conclusions of that meeting are not publicly available. It should also be noted that an eu-Lisa report produced just a month prior to Europol's, in September 2022, refers to the December 2021 timeline as still being in force.

7.3.2 Entry/Exit System (EES)

Purpose

- To monitor the dates, places and times at which temporary visitors (e.g. tourists or businesspeople) enter and exit the Schengen area. The system will automatically calculate the amount of time they are permitted to stay in the Schengen area and issue automatic alerts to national authorities on individuals who stay longer than permitted, with the aim of having them removed from the Schengen area (whether via deportation or 'voluntary return'). The intention was to have the EES up-and-running by May 2021, but the date was subsequently put back to the end of May 2023.

Data stored

- Biographic: surname(s), first name(s), date of birth, nationality(ies), sex, type and number of the travel document(s), three letter code of the issuing country, date of expiry of the validity of the travel document(s);
- Biometric: four fingerprints, facial image;
- Other: dates, times and locations of border crossings, various other data items depending on the category of individual.

Conditions for access by Europol

Consultation of the EES must be:

- "necessary to support and strengthen action by Member States in preventing, detecting or investigating terrorist offences or other serious criminal offences falling under Europol's mandate"
- "necessary and proportionate in a specific case"
- based on "evidence or reasonable grounds... to consider that the consultation of the EES data will contribute to the prevention, detection or investigation of any of the criminal offences in question, in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence falls under a category covered by this Regulation."

If the aim of the access is "identifying an unknown suspect, perpetrator or suspected victim of a terrorist offence or other serious criminal offence," a further condition must also be met: "the consultation, as a matter of priority, of the data stored in the databases that are technically and legally accessible by Europol has not made it possible to identify the person in question."

Procedure for access

- An authorised unit within Europol must submit a reasoned request to the unit within Europol that is nominated as the central access point (the latter "shall act independently" of the former).

7.3.3 Eurodac

Purpose

- Eurodac was established as a database of asylum-seekers' fingerprints, used for determining the EU member state responsible for an asylum application.
- A proposal currently under negotiation will expand the system's purpose and thus the number of individuals whose data is stored, turning Eurodac into "a common European database to support EU policies on asylum, resettlement and irregular migration."
- In particular, the revamped Eurodac will be used to store data on undocumented individuals apprehended within the EU, with the aim of facilitating their deportation. The age limit for data storage will also be lowered, from 14 to six; and the amount of data to be stored will also be increased.

Eurodac is used to process data on the following groups:

- Individuals who have lodged an application for international protection
- Individuals apprehended in connection with irregular border-crossings
- Third-country nationals or stateless persons found irregularly staying in a Member State (currently data is compared, not stored; this will change under the new rules)
- Individuals disembarked following a search and rescue operation (a new category introduced by the proposals currently under discussion)

Data stored

Until the new rules are approved, only fingerprints and some technical items of data are stored in Eurodac.

- Biometric: 10 fingerprints, facial image.
- Biographic: surname(s), forename(s), name(s) at birth, previously used names and aliases, nationality(ies), place/date of birth, member state of origin (i.e. the member state in which the person was registered), place and date of application, sex, type and number of travel document, three-letter country code and validity period
- Other: various, depending on the situation.

Conditions for access by Europol

- Comparison of Europol data with Eurodac data is allowed "only if comparisons with fingerprint data stored in any information processing systems that are technically and legally accessible by Europol did not lead to the establishment of the identity of the data subject"
- Search must be "necessary to support and strengthen action by Member States in preventing, detecting or investigating terrorist offences or other serious criminal offences falling under Europol's mandate"; "necessary in a specific case (i.e. systematic comparisons shall not be carried out)"; and there must be "reasonable grounds to consider that the comparison will substantially contribute to the prevention, detection or investigation of any of the criminal offences in question"

Procedure for access

- An authorised unit within Europol must submit a reasoned request to the unit within Europol that is nominated as the verifying authority (the latter "shall act independently" of the former)

Statistics:

- 2021: 20 comparisons by Europol, 446 law enforcement searches by member states
- 2020: two comparisons by Europol, 206 law enforcement searches by member states

7.3.4 European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN)

Purpose

- The ECRIS-TCN contains information on non-EU nationals who have been convicted in one or more EU member state, in order to make it easier for national authorities to find information on convictions handed down elsewhere in the EU.
- Convicted individuals who hold the nationality of both an EU and non-EU state will also be registered in the ECRIS-TCN, despite strident protests from legal experts (and, initially, the European Parliament) that this breaches the principle of non-discrimination.

Data stored

- Biometric: fingerprints and facial images (the latter are stored only if they are collected under the national law of the convicting member state)
- Biographic: surname, first names, date of birth, place of birth (town and country), nationality or nationalities, gender, previous names (if applicable), parents' names (if included in the criminal record), pseudonyms or aliases (if available), identity number, or the type and number of the person's identification documents, as well as the name of the issuing authority (if available)
- Other: the code of the convicting member state (e.g. DE for Germany, FR for France)

Conditions for access

Europol may access the ECRIS-TCN[110] "to identify the Member States holding information on previous convictions of third-country nationals," for six reasons:

- to collect, store, process, analyse and exchange information, including criminal intelligence;
- to notify the member states of any information and connections between criminal offences concerning them;
- to coordinate, organise and implement investigative and operational actions to support and strengthen actions by the competent authorities of the member states that are carried out with other member state authorities, with joint investigation teams, or in liaison with Eurojust;
- participate in joint investigation teams, as well as propose that they be set up;
- provide information and analytical support to member states in connection with major international events; and
- support member states' cross-border information exchange activities, operations and investigations, as well as joint investigation teams, including by providing operational, technical and financial support.

Procedure for access

- If a search in the ECRIS-TCN leads to a hit(s), Europol must make a request to the relevant member state(s) to access information contained in the criminal record. However, it should be noted that even being made aware of the fact that information exists in the ECRIS-TCN regarding a particular individual can be used to draw inferences and assumptions about them.

[110] Article 14, Regulation 2019/816

7.3.5 European Travel Information and Authorisation System (ETIAS)

Purpose

- The purpose of the ETIAS is to ensure the vetting of citizens of countries who do not currently require a visa to enter the Schengen area - for example the UK, USA, Canada, Japan, multiple Latin American states, Ukraine and others.
- These individuals will have to pay a fee and file a "travel authorisation" application to be able to travel to the EU. That application will be stored at the ETIAS Central Unit, operated by Frontex, and may also be viewed by officials in one of the member states, each of which will operate an ETIAS National Unit.
- Applications will be automatically compared against a host of EU, Europol and Interpol databases to examine whether individuals are a “security, migration or health” risk. While most will receive automatic approval, those generating hits (or generating another cause for concern) will be sent for further scrutiny by officials. A new "watchlist" (operated by Europol) and a profiling mechanism (referred to as "screening rules", based on "risk indicators") will also be used to filter applications (see ‘Travel intelligence: watchlists and profiling’, below, for further information).

Data stored

- Biometric: none (all travel authorisation applicants will have four fingerprints and a photograph taken for inclusion in the Entry/Exit System when they enter the Schengen area)
- Biographic: names, date and place of birth, nationality, education, occupation, travel document data, and more
- Other: none

Conditions for access by Europol

Consultation by Europol must be:

- "necessary to support and strengthen action by Member States in preventing, detecting or investigating terrorist offences or other serious criminal offences falling under Europol’s mandate"
- "necessary and proportionate in a specific case"
- limited to searching with certain data, including but not limited to names, nationality, email address, IP address
- based on evidence or reasonable grounds indicating that consultation will "contribute to the prevention, detection or investigation of any of the criminal offences in question, in particular where there is a substantiated suspicion that the suspect, perpetrator or victim of a terrorist offence or other serious criminal offence falls under a category of traveller covered by this Regulation."

Procedure for access

A reasoned request must be sent to "a specialised unit of duly empowered Europol officials" for examination to ensure it meets the conditions. The request must include specific justifications for requesting access to particular types of data, namely:

- member state of first intended stay and, optionally, the address of first intended stay;
- whether the applicant has been convicted in the previous 25 years of a terrorist offence, certain criminal offences (and if so, when and where), whether they have stayed in a specific war or conflict zone over the previous 10 years and the reasons for the stay, whether they have been the subject of a return decision in the previous 10 years.

Travel intelligence: watchlists and profiling

Europol has a key role in the EU's burgeoning 'travel intelligence' architecture, which involves the increased collection and processing of data on international travellers – for example, by making use of data gathered from EU and other databases, information taken from airlines and other travel providers, and other sources. The agency explicitly plans to develop this in the years to come, in order to ensure the pervasive profiling of individuals crossing the EU's borders, for the purpose of ensuring "security".

The ETIAS plays a key role in this. The ETIAS Central System will contain a "watchlist", made up of "data related to persons who are suspected of having committed or taken part in a terrorist offence or other serious criminal offence or persons regarding whom there are factual indications or reasonable grounds, based on an overall assessment of the person, to believe that they will commit a terrorist offence or other serious criminal offence."

Europol and the member states are empowered to enter data in the watchlist, which can include names, date of birth, information on travel documents, home and email address, phone number and more. Europol and the member states are responsible for reviewing and verifying the accuracy and relevance of the data they have entered in the watchlist "regularly, and at least once a year."

As a group of legal scholars has argued: "Watchlisting severely affects the rights of those targeted, and yet its necessity or efficacy has not been reliably established and, in practice, it is extraordinarily difficult to challenge," in particular because it generally affects foreign nationals, who are likely to face difficulties in accessing remedies.[111] Europol's latest progress report on ETIAS says that it was "moving forward with implementing the management of ETIAS watchlist," with "business processes… being finalised."

Profiling is also key to the world of "travel intelligence". Both the ETIAS and the VIS are to make use of "screening rules" and "risk indicators" to determine which applications require enhanced scrutiny from officials. Those rules and indicators will be established by the ETIAS Screening Board, involving Europol, Frontex and member state representatives. It "shall take into consideration the recommendations issued by the ETIAS Fundamental Rights Guidance Board," but those recommendations have no binding nature.

This is just one part of a larger plan for Europol to establish a "fully-fledged European Travel Intelligence Centre," which amongst many other things will include "[enhanced] cooperation with private partners relevant for the collection of travel intelligence."[112] It will also involve the increased examination and exchange of Passenger Name Record (PNR) and Advance Passenger Information (API) data. A working group set up by Frontex and Europol concluded that: "Border management should also rely on automated targeting or screening systems for performing risk management on the travellers with advance information," which "would require legislative change and most likely the use of AI to combine those sources effectively."[113] According to its work programme, Europol has a "roadmap" for its travel intelligence plans.[114] It is not currently available to the public.

[111] Ramzi Kassem, Rebecca Mignot-Mahdavi and Gavin Sullivan, 'Watchlisting the World: Digital Security Infrastructures, Informal Law, and the "Global War on Terror"', *Just Security*, 28 October 2021, https://www.justsecurity.org/78779/watchlisting-the-world-digital-security-infrastructures-informal-law-and-the-global-war-on-terror/

[112] Europol, 'Programming Document 2022-24', 22 December 2021, pp.42-3, https://www.europol.europa.eu/publications-events/publications/europol-programming-document

[113] 'EU: Agencies propose a "European System for Traveller Screening" that "could include AI technology"', *Statewatch*, 19 May 2022, https://www.statewatch.org/news/2022/may/eu-agencies-propose-a-european-system-for-traveller-screening-that-could-include-ai-technology/

[114] Ibid., p.22

7.3.6 Schengen Information System (SIS)

Purpose

Europol has access to SIS alerts on:

- refusal of entry to and stay in the Schengen area
- persons wanted for arrest for surrender or extradition purposes
- persons wanted for arrest for surrender purposes
- persons wanted for arrest for surrender purposes
- persons wanted for arrest for extradition purposes
- missing persons or vulnerable persons who need to be prevented from travelling
- persons sought to assist with a judicial procedure
- persons and objects for discreet checks, inquiry checks or specific checks
- objects for seizure or use as evidence in criminal proceedings
- unknown wanted persons for the purposes of identification under national law

Europol is now also able to propose that member states create "information alerts on third-country nationals in the interests of the Union" in the SIS. These are to be based on data shared with Europol by third states, and should relate to individuals suspected of being involved in terrorism or serious crime. This raises the possibility that third states could request the insertion of data on political opponents and dissidents, as has happened with Interpol's systems[115] – the same problem that arises with the possibility for Europol to provide "third-country sourced biometric data" for the Prüm network. When an official comes across an individual subject to an information alert, further information on that individual must be transmitted to the member state that issued the alert.[116]

Data stored

- Biometric: can include fingerprints, photographs, palm prints and DNA
- Biographic: names, date of birth, gender, nationality(ies), reason for alert, copy of or information on identity documents, amongst other things
- Other: various

Conditions and procedure for access by Europol

Unlike other large-scale EU information systems, the law does not put in place specific conditions or procedures for access by Europol to the SIS. However, if a search by Europol (for example, with the name of someone it is investigating) leads to a 'hit' in the SIS, it is obliged to inform the member state that issued the alert. Where that member state provides Europol with further information, the agency can then process that information for the purpose of cross-checking and/or analysis.

Statistics

Europol (as well as Eurojust and Frontex) have access to the SIS, but no statistics are currently collected on their usage of the system. National authorities make millions of searches annually.[117]

[115] 'Abuse of the Interpol system by Turkey', *Stockholm Center for Freedom*, September 2017, https://stockholmcf.org/wp-content/uploads/2017/09/Abuse-Of-The-Interpol-System-By-Turkey_September-20-2017.pdf

[116] Article 37a and 37b, Regulation (EU) 2018/1862 (consolidated version)

[117] eu-LISA, 'Report on the technical functioning of Central SIS II 2019-20', May 2022, https://www.eulisa.europa.eu/Publications/Reports/Report%20on%20SIS%20II%20tech%20funct%202019-2020.pdf; eu-LISA, 'SIS II – 2018 statistics', February 2019, https://www.eulisa.europa.eu/AboutUs/Documents/MB%20Decissions/2019-059_SIS%20II%20statistics%202018%20PUBLIC.pdf

7.3.7 Visa Information System (VIS)

Purpose

The primary purpose of the VIS is to aid the implementation of the common visa policy, by storing data on all short-stay Schengen visa applicants. It has seven sub-objectives, which include aiding in the fight against drug and "visa shopping" and preventing security threats. Amendments approved in 2021 will see the system expanded to include data on long-stay visas and residence permits, and to lower the age limit from 12 to six years of age.

The VIS is used to process data on the follow groups:

- Individuals who have lodged an application for a short term visa
- Individuals who have lodged an application for a long-stay visa
- Individuals who have lodged an application for a residence permit

Data stored

- Biometric: facial image/photograph, 10 fingerprints
- Biographic: names, date of birth, sex, travel document information, details of the person issuing an invitation or liable for the visa applicants' costs during their stay, address, occupation and employer or name of educational establishment
- Other: member state of destination and duration of intended trip, member state of first entry, intended date of arrival and departure, place and date of application

Once changes to the VIS agreed in 2021 are put into practice, visa applications are to be treated in a similar fashion to travel authorisation applications, with automated cross-checking of multiple databases and the profiling of all applicants against "risk indicators".

Conditions for access

- "Europol may access the VIS within the limits of its mandate and when necessary for the performance of its tasks."
- The member state that entered data into the VIS must give Europol consent to process it, should a search by Europol lead to a 'hit' against that data.

Procedure for access

- "Europol shall designate a specialised unit for the purpose of this Decision with duly empowered Europol officials to act as the central access point to access the VIS for consultation."

Statistics on law enforcement usage

Europol is not yet connected to the VIS, although it is preparing to do so. At the end 2021, "the Automated Biometrics Identification System (ABIS), necessary to cross-check fingerprints/facial images included in VIS against Europol's biometric data, contained a total of 22,580 biometric records."[118] Member state searches went from just over 7,000 in 2019 to around 16,000 in 2020, then decreased to just over 12,000 in 2021.[119]

[118] Europol, 'Consolidated Annual Activity Report 2021', p.15, https://www.europol.europa.eu/cms/sites/default/files/documents/Consolidated%20Annual%20Activity%20Report%202021.PDF

[119] eu-LISA reports on the technical functioning of the VIS.

7.3.8 The 'Prüm' network

Purpose

- To enable cross-border searches by law enforcement authorities of national DNA, fingerprint and vehicle registration databases
- The types of database included in the Prüm network may be expanded to include facial recognition and "police records" systems, under a 2021 proposal[120]

Data stored

- Fingerprints
- DNA samples
- Vehicle registration data
- Facial images (whether mugshots or images captured from crime scenes, e.g. by CCTV cameras)
- Police records (defined as "any information available in the national register or registers recording data of competent authorities, for the prevention, detection and investigation of criminal offences"[121]), through a new European Police Records Index System (EPRIS)

The Prüm system is a network of national databases, rather than a centralised EU database of any kind. However, under the 2021 proposal, a "central router" would be set up to handle searches, obviating the need for an interconnection between every single participating member state, and making further interconnections between different systems possible. Indeed, the central router will also be connected to the Common Identity Repository, allowing simultaneous searches of the Prüm network and the EU's large-scale databases.

The involvement of Europol

Europol currently has no direct access to the systems that make up the Prüm network, but the 2021 proposal will change this. If agreed as proposed, member states will be able to search "third country-sourced biometric data held at Europol,"[122] and Europol will be able to compare "third country-sourced data" against national biometric, vehicle registration and police records databases.[123]

This would give "European authorities the possibility to penalise dissidents or other people who are facing politically-motivated persecution from third countries."[124,125] It may also impact asylum adjudication procedures by making it possible for third states to label people as security threats. There is also "absolutely no guarantee that the biometric data concerns only convicted and suspected terrorists and other serious criminals," and "this assessment may be made by third countries with questionable human rights records, increasing the risk to individuals' rights."[126]

[120] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on automated data exchange for police cooperation ("Prüm II"), COM(2021) 784 final, 8 December 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2021:784:FIN
[121] Ibid., Article 4
[122] Ibid., Article 49
[123] Ibid., Article 50
[124] EDRi, 'Respecting fundamental rights in the cross-border investigation of serious crimes', *European Digital Rights*, 7 September 2022, p.11, https://edri.org/wp-content/uploads/2022/10/EDRi-position-paper-Respecting-fundamental-rights-in-the-cross-border-investigation-of-serious-crimes-7-September-2022.pdf
[125] Similar problems exist with Interpol's databases: 'Abuse of the Interpol system by Turkey', *Stockholm Center for Freedom*, September 2017, https://stockholmcf.org/wp-content/uploads/2017/09/Abuse-Of-The-Interpol-System-By-Turkey_September-20-2017.pdf
[126] 'Respecting fundamental rights in the cross-border investigation of serious crimes', p.12

8. Supervision and scrutiny

8.1 Data protection

Given the vastly-expanded scale of Europol's data-processing activities, a reinforcement of the supervision and scrutiny of the agency might have been expected. In fact, the opposite is true. As the EDPS remarked after the new amendments entered into force, they "weaken the fundamental right to data protection and do not ensure an appropriate oversight".[127] Although Europol's Data Protection Officer has been given an expanded set of tasks and powers,[128] the requirements for independent external oversight have been substantially lowered.

In a speech to the Europol Joint Parliamentary Scrutiny Group, a body made up of national MPs and MEPs tasked with providing "political supervision" of Europol's activities, the EDPS highlighted some of these concerns. The "balance between data protection and operational needs" has been shifted by the 2022 amendments, he said, in particular the new powers that allow Europol to process large datasets.[129]

Those powers raise "the risk that data relating to individuals that have no established link to a criminal activity will be treated in the same way as the personal data of individuals with such a link." Europol's Management Board is responsible for approving decisions on how these powers will be implemented – but the Board's first attempt to pass those decisions bypassed the EDPS, in breach of the law.[130]

The EDPS also referred to "recurrent issues, such as deficiencies in the risk assessment methodology applied by Europol" in its data protection impact assessments. While Europol is obliged in certain cases to consult the EDPS on new data processing operations, the new rules "[raise] the threshold for filing a prior consultation requests [sic] with the EDPS and [allow] Europol to start processing activities with high risks before the EDPS issues an opinion."

Whereas Europol previously had to consult the EDPS on new data processing operations if they involved special categories of data or presented "specific risks for the fundamental rights and freedoms… of data subjects,"[131] the rules now start by excluding certain types of processing operations from scrutiny – namely, those in "individual operational activities that do not include any new type of processing that would involve a high risk to the rights and freedoms of the data subjects." It is up to Europol to assess whether a "high risk" is involved.[132] The fact that the EDPS is concerned about its ability to make those assessments should set alarm bells ringing.

The time limits for the EDPS to respond to requests for consultation have also been lowered compared to the 2016 Regulation. Previously, the EDPS had two months to provide an opinion. That period could also be suspended, although if no opinion was provided within

[127] EDPS, 'Amended Europol Regulation weakens data protection supervision', 27 June 2022, https://edps.europa.eu/press-publications/press-news/press-releases/2022/amended-europol-regulation-weakens-data_en
[128] Article 41b, Regulation 2016/794 (consolidated version)
[129] EDPS, 'Joint Parliamentary Scrutiny Group (JPSG), Speaking points', 24 October 2022, https://edps.europa.eu/system/files/2022-10/22-10-24_jpsg_ww_speech1_en.pdf
[130] 'Europol management board in breach of new rules as soon as they came into force', *Statewatch*, 3 November 2022, https://www.statewatch.org/news/2022/november/europol-management-board-in-breach-of-new-rules-as-soon-as-they-came-into-force/
[131] Article 39(1), Regulation 2016/794 (original version)
[132] Article 39(1), Regulation 2016/794 (consolidated version)

four months it was to be treated as a green light for the new data processing activities.[133] Now – in accordance with the rules on data protection in EU institutions[134] – the period is six weeks, which may be extended by one month. Yet, if Europol determines that the new processing operations "are particularly urgent and necessary to prevent and combat an immediate threat," it can simply consult the EDPS and then start processing without waiting for a response – although any EDPS advice must be "taken into account retrospectively".[135]

That said, the EDPS has been granted some new powers. The data protection body can now order Europol "to bring processing operations into line with this Regulation," can "order the suspension of data flows to a recipient in a Member State, a third country or an international organisation," and can impose a fine upon Europol in certain circumstances where it fails to meet data protection requirements or comply with orders from the EDPS.[136]

8.2 Fundamental rights

One novelty introduced by the 2022 amendments is the new post of Fundamental Rights Officer (FRO) at Europol. This mirrors the post at Frontex created by that agency's 2019 Regulation, although Europol's FRO has far fewer powers (partly a reflection of the agency itself having far fewer competences than Frontex) and is also explicitly less independent than their counterpart at Frontex.[137] Whereas the Frontex FRO is appointed by and responsible to the Management Board (made up of representatives of the member states, the European Commission and the European Parliament in an observer role), Europol's FRO is appointed by the Management Board "upon a proposal of the Executive Director," and "shall report directly to the Executive Director".[138] This contrasts with the procedure for appointment the agency's Data Protection Officer, who is to be appointed by the Management Board without any (formal) involvement of the executive director.[139]

The role of Europol FRO was introduced by the European Parliament. As part of its negotiating strategy, the Council aimed to limit the independence of the FRO. A paper circulated by the French Presidency of the Council stated:

> *"Given the importance that this new function has for the European Parliament, the delegations supported the Presidency's proposal not to block this initiative, but to insist that the officer be appointed on the simple proposal of the Executive Director of Europol, and that he or she is in principle already a member of the Agency's existing staff; this will notably mark the difference with respect to the Data Protection Officer."*[140]

Apart from the aim to include a requirement in the text for the FRO to be "in principle already a member of the Agency's existing staff," the Presidency's proposal was successful.

[133] Article 39(3), Regulation 2016/794 (original version)
[134] Article 90, Regulation 2018/1825
[135] Article 39(3), Regulation 2016/794 (consolidated version)
[136] Article 43, Regulation 2016/794 (consolidated version). The new powers are set out in sub-articles (2)(j),(k) and (l).
[137] It should be noted, of course, that while Frontex's FRO is nominally independent, they were effectively sidelined in their work by the agency's management during the time that Fabrice Leggeri was executive director. It remains to be seen whether the situation improves now Leggeri has departed.
[138] Article 41c, Regulation 2016/794 (consolidated version)
[139] Article11(1)(l), Regulation 2016/794 (consolidated version)
[140] 'Europol: Council Presidency proposes workaround for illegal data processing', *Statewatch*, 25 January 2022, https://www.statewatch.org/news/2022/january/europol-council-presidency-proposes-workaround-for-illegal-data-processing/

8.3 Parliamentary scrutiny

There are two parliamentary for a in which scrutiny of Europol can be exercised: the European Parliament's civil liberties committee (LIBE) and the Joint Parliamentary Scrutiny Group (JPSG), made up of elected officials from EU member state parliaments and the European Parliament. The LIBE committee has no fixed agenda for scrutiny of Europol, but MEPs can submit questions to the agency when they wish, and the committee may hold hearings on particular issues – for example, on 8 November, it questioned Europol and Frontex representatives about the Personal Data for Risk Assessment (PeDRA) project.[141]

The role of the JPSG is more structural, and the 2022 amendments grant the body some new powers. The JPSG meets twice a year. Its membership consists of up to four representatives from each EU national parliament, and up to 16 representatives from the European Parliament. Its role is to "politically monitor Europol's activities in fulfilling its mission, including as regards the impact of those activities on the fundamental rights and freedoms of natural persons."[142]

The chairperson of the Europol management board and the agency's executive director (as well as their deputies) are obliged to appears before the JPSG if so requested, to discuss Europol's activities, "including the budgetary aspects of such activities, the structural organisation of Europol and the potential establishment of new units and specialised centres, taking into account the obligations of discretion and confidentiality."[143] The EDPS must also attend the JPSG at its request, and in any case at least once annually.

Europol is also obliged to transmit a variety of reports and information to the JPSG – for example, on information exchanged with private parties, transfers of personal data to third countries, and on the number of cases in which the agency processed personal data falling outside of the list in Annex II to the Regulation.[144] The JPSG may also request "a detailed description of the process and of the rationale behind the training, testing and validation of algorithms."[145] Many of these new information provision requirements have been introduced as a form of accountability for the agency's new data processing powers. However, any conclusions or recommendations drawn up by the JPSG are non-binding upon the agency.[146]

There is one instance when Europol must at least justify to the JPSG why it has chosen not to follow its advice. This concerns the agency's "multiannual programming document". If the management board "decides not to take into account any of the matters raised by the JPSG," in relation to that document, it must "provide a thorough justification."[147] Two members of the JPSG must also be invited twice a year to attend Europol management board meetings, as non-voting observers.[148]

The new rules also introduce a requirement for the JPSG to establish "a consultative forum" to provide "independent advice in fundamental rights matters."[149] It may be consulted by the JPSG and Europol's management board. This is similar to a requirement that applies to

[141] 'Document collection: Frontex and "operational personal data"', *Statewatch*, https://www.statewatch.org/observatories/frontex/document-collection-frontex-and-operational-personal-data/
[142] Article 51(2), Regulation 2016/794 (consolidated version)
[143] Article 51(2)(a), Regulation 2016/794 (consolidated version)
[144] The full list can be found in Article 51(3), Regulation 2016/794 (consolidated version)
[145] Article 33a(4), Regulation 2016/794 (consolidated version)
[146] Article 51(5), Regulation 2016/794 (consolidated version)
[147] Article 12(1), Regulation 2016/794 (consolidated version)
[148] Article 14(4), Regulation 2016/794 (consolidated version)
[149] Article 52a, Regulation 2016/794 (consolidated version)

Frontex,[150] which has frequently ignored the opinions of its forum.[151] However, while Frontex's forum is established by the agency and its composition determined by the management board, the JPSG consultative forum is to be established by the JPSG itself, making it rather more distant from Europol. It also has far fewer explicit powers than the Frontex consultative forum, for example with regards to access to information. Indeed, the JPSG consultative forum is not granted any particular powers aside from being able to give advice.

[150] Article 108, Regulation 2019/1896, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32019R1896#d1e7316-1-1
[151] 'Frontex: the ongoing failure to implement human rights safeguards', *Statewatch*, 25 January 2022, https://www.statewatch.org/analyses/2022/frontex-the-ongoing-failure-to-implement-human-rights-safeguards/

Annex I: Evolution of Europol's tasks, 2016-22

2016	2022
Collect, store, process, analyse and exchange information, including criminal intelligence	
Notify the Member States, via the national units, of any information and connections between criminal offences concerning them	
Coordinate, organise and implement investigative and operational actions to support and strengthen actions by the competent authorities of the Member States, that are carried out: jointly with the competent authorities of the Member States in the context of joint investigation teams and, where appropriate, in liaison with Eurojust	
Participate in joint investigation teams, as well as propose that they be set up	
Provide information and analytical support to Member States in connection with major international events	
Prepare threat assessments, strategic and operational analyses and general situation reports;	
Develop, share and promote specialist knowledge of crime prevention methods, investigative procedures and technical and forensic methods, and provide advice to Member States	
Support Member States' cross-border information exchange activities, operations and investigations, as well as joint investigation teams, including by providing operational, technical and financial support	
	Provide administrative and financial support to Member States' special intervention units (this is done via Europol hosting the ATLAS Support Office[152])
Provide specialised training and assist Member States in organising training, including with the provision of financial support, within the scope of its objectives and in accordance with the staffing and budgetary resources at its disposal in coordination with the European Union Agency for Law Enforcement Training (CEPOL)	

[152] Europol, 'European Counter Terrorism Centre – ECTC', as updated 28 June 2022, https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc

2016	2022
~~Cooperate with the Union bodies established on the basis of Title V of the TFEU and with OLAF, in particular through exchanges of information and by providing them with analytical support in the areas that fall within their competence;~~	Cooperate with EU justice and home affairs agencies, with the European Anti-Fraud Office and the European Union Agency for Cybersecurity (ENISA), in particular through the exchange of information and provision of analytical support in areas that fall within their respective competences
Provide information and support to EU crisis management structures and missions	
Develop Union centres of specialised expertise for combating certain types of crime falling within the scope of Europol's objectives, in particular the European Cybercrime Centre;	
Support Member States' actions in preventing and combating forms of crime for which Europol is competent and which are facilitated, promoted or committed using the internet, including, in cooperation with Member States, the making of referrals of internet content, by which such forms of crime are facilitated, promoted or committed, to the online service providers concerned for their voluntary consideration of the compatibility of the referred internet content with their own terms and conditions.	Support Member States' actions in preventing and combating forms of crime for which Europol is competent and which are facilitated, promoted or committed using the internet, including by: assisting Member States, upon, in responding to cyberattacks of suspected criminal origin cooperating with the Member States with regard to removal orders that require online "hosting service providers to remove terrorist content or to disable access to terrorist content"[153] referring content to online service providers for their voluntary consideration of its compatibility with their terms and conditions
	Support Member States in identifying persons whose criminal activities fall within the forms of crime listed for which Europol is competent and who constitute a high risk for security

[153] Article 3, Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32021R0784

2016	2022
	Facilitate joint, coordinated and prioritised investigations regarding such persons
	Support Member States in processing data provided by third countries or international organisations to Europol and propose to member states entry of “information alerts” into the Schengen Information System
	Support the implementation of the Schengen evaluation and monitoring mechanism through the provision of expertise and analyses
	Proactively monitor research and innovation activities, support related activities of Member States, and implement research and innovation activities, including projects for the development, training, testing and validation of algorithms for law enforcement purposes
	Contribute to synergies between the research and innovation activities of Union bodies that are relevant for the achievement of Europol’s objectives, including through the EU Innovation Hub for Internal Security
	Support, upon request, Member States’ actions to address online crisis situations, in particular by providing private parties with information necessary to identify relevant online content
	Support Member States’ actions in addressing the online dissemination of online child sexual abuse material;
	Cooperate with national Financial Intelligence Units (FIUs) through Europol national units or by direct contact with the FIUs
Provide strategic analyses and threat assessments to assist the Council and the Commission in laying down strategic and operational priorities of the Union for fighting crime. Europol shall also assist in the operational implementation of those priorities.	Provide strategic analyses and threat assessments to assist the Council and the Commission in laying down strategic and operational priorities of the Union for fighting crime. Europol shall also assist in the operational implementation of those priorities. Europol shall also assist in the operational implementation of those priorities, in particular in the European Multidisciplinary Platform Against Criminal Threats (EMPACT), including by facilitating and providing administrative, logistical, financial and operational support to operational and strategic activities led by Member States.

2016	2022
Europol shall provide strategic analyses and threat assessments to assist the efficient and effective use of the resources available at national and Union level for operational activities and the support of those activities.	Europol shall provide strategic analyses and threat assessments to assist the efficient and effective use of the resources available at national and Union level for operational activities and the support of those activities. Europol shall also provide threat assessment analyses based on the information it holds on criminal phenomena and trends to support the Commission and the Member States in carrying out risk assessments
Europol shall act as the Central Office for combating euro counterfeiting	
	Europol shall assist the Member States and the Commission in identifying key research themes, including by assisting the Commission in drawing up research work programmes, whilst taking all necessary measures to avoid conflicts of interest.
	Europol shall support the Member States in the screening, as regards the expected implications for security, of specific cases of foreign direct investments into the Union under Regulation (EU) 2019/452 of the European Parliament and of the Council (10) that concern undertakings that provide technologies, including software, used by Europol for the prevention and investigation of crimes that fall within Europol's objectives.
Europol shall not apply coercive measures in carrying out its tasks.	Europol shall not apply coercive measures in carrying out its tasks. Europol staff may provide operational support to the competent authorities of the Member States during the execution of investigative measures, at their request and in accordance with their national law, in particular by facilitating cross-border information exchange, by providing forensic and technical support and by being present during the execution of those measures. Europol staff shall not, themselves, have the power to execute investigative measures.
	Europol shall respect the fundamental rights and freedoms enshrined in the Charter of Fundamental Rights of the European Union in the performance of its tasks.

Annex II: Personal data processing by Europol

Personal data processing for cross-checking

Along with the categories of data explicitly listed in the Regulation, the law says: “Additional information held by Europol or national units concerning the persons referred to in paragraph 1 [suspects, convicts or likely criminals] may be communicated to any national unit or to Europol, should either so request. National units shall do so in compliance with their national law.” This provision would seem to render the previous specifications rather pointless, if any “additional information” can be transmitted to or from the agency, provided such transmission is in line with national law.

	Categories of person	
Categories of data	**Suspects and convicts**	**Likely criminals**
surname, maiden name, given names and any alias or assumed name	x	x
date and place of birth	x	x
nationality	x	x
sex	x	x
place of residence, profession and whereabouts of the person concerned	x	x
social security numbers, driving licences, identification documents and passport data	x	x
where necessary, other characteristics likely to assist in identification, including any specific objective physical characteristics not subject to change such as dactyloscopic data and DNA profile (established from the non-coding part of DNA)	x	x
criminal offences, alleged criminal offences and when, where and how they were (allegedly) committed	x	x
means which were or which may have been used to commit those criminal offences, including information concerning legal persons	x	x

departments handling the case and their filing references	x	x
suspected membership of a criminal organisation	x	x
convictions, where they relate to criminal offences in respect of which Europol is competent	x	x
inputting party	x	x

Personal data processing for strategic or thematic analysis, operational analysis, or to facilitate the exchange of information

Categories of data	Categories of person					
	Suspects and convicts	Likely criminals	Contacts and associates	Victims	Witnesses	Informants
(a) personal details:			Data "may be stored as necessary, provided there is reason to assume that such data are required for the analysis of the relationship" with suspect, convicts and likely criminals			
(i) present and former surnames;	x	x		x	x	x
(ii) present and former forenames;	x	x		x	x	x
(iii) maiden name;	x	x		x	x	x
(iv) father's name (where necessary for the purpose of identification);	x	x		x	x	x
(v) mother's name (where necessary for the purpose of identification):	x	x		x	x	x
(vi) sex;	x	x		x	x	x
(vii) date of birth;	x	x		x	x	x
(viii) place of birth;	x	x		x	x	x
(ix) nationality;	x	x		x	x	x
(x) marital status;	x	x		x	x	x
(xi) alias;	x	x		x	x	x
(xii) nickname;	x	x		x	x	x
(xiii) assumed or false name;	x	x		x	x	x

Categories of data	Categories of person					
	Suspects and convicts	Likely criminals	Contacts and associates	Victims	Witnesses	Informants
(xiv) present and former residence and/or domicile;	x	x		x	x	x
(b) physical description:						
(i) physical description;	x	x		x	x	x
(ii) distinguishing features (marks/scars/tattoos etc.);	x	x		x	x	x
(c) means of identification:						
(i) identity documents/driving licence;	x	x		x	x	x
(ii) national identity card/passport numbers;	x	x		x	x	x
(iii) national identification number/social security number, if applicable;	x	x		x	x	x
(iv) visual images and other information on appearance;	x	x		Data "may be stored as necessary, provided there is reason to assume that they are required for the analysis of a person's role as victim or potential victim."	Data "may be stored as necessary, provided there is reason to assume that they are required for the analysis of such persons' role as witnesses."	Data "may be stored as necessary, provided there is reason to assume that they are required for the analysis of such persons' role as informant."
(v) forensic identification information such as fingerprints, DNA profile (established from the non-coding part of DNA), voice profile, blood group, dental information;	x	x				
(d) occupation and skills:						
(i) present employment and occupation;	x	x				
(ii) former employment and occupation;	x	x				
(iii) education (school/university/professional);	x	x				
(iv) qualifications;	x	x				
(v) skills and other fields of knowledge (language/other);	x	x				

Categories of data	Categories of person					
	Suspects and convicts	Likely criminals	Contacts and associates	Victims	Witnesses	Informants
(e) economic and financial information:						
(i) financial data (bank accounts and codes, credit cards, etc.);	x	x				
(ii) cash assets;	x	x				
(iii) shareholdings/other assets;	x	x				
(iv) property data;	x	x				
(v) links with companies;	x	x				
(vi) bank and credit contacts;	x	x				
(vii) tax position;	x	x				
(viii) other information revealing a person's management of his or her financial affairs;	x	x				
(f) behavioural data:						
(i) lifestyle (such as living above means) and routine;	x	x				
(ii) movements;	x	x				
(iii) places frequented;	x	x				
(iv) weapons and other dangerous instruments;	x	x				
(v) danger rating;	x	x				

Categories of data	Categories of person					
	Suspects and convicts	**Likely criminals**	**Contacts and associates**	**Victims**	**Witnesses**	**Informants**
(vi) specific risks such as escape probability, use of double agents, connections with law enforcement personnel;	x	x				
(vii) criminal-related traits and profiles;	x	x				
(viii) drug abuse;	x	x				
(g) contacts and associates, including type and nature of the contact or association;	x	x				
(h) means of communication used, such as telephone (static/mobile), fax, pager, electronic mail, postal addresses, internet connection(s);	x	x				
(i) means of transport used, such as vehicles, boats, aircraft, including information identifying those means of transport (registration numbers);	x	x				
(j) information relating to criminal conduct:						
(i) previous convictions;	x	x				
(ii) suspected involvement in criminal activities;	x	x				
(iii) modi operandi;	x	x				
(iv) means which were or may be used to prepare and/or commit crimes;	x	x				
(v) membership of criminal groups/organisations and position in the group/organisation;	x	x				

Categories of data	Categories of person					
	Suspects and convicts	**Likely criminals**	**Contacts and associates**	**Victims**	**Witnesses**	**Informants**
(vi) role in the criminal organisation;	x	x				
(vii) geographical range of criminal activities;	x	x				
(viii) material gathered in the course of an investigation, such as video and photographic images;	x	x				
(k) references to other information systems in which information on the person is stored:						
(i) Europol;	x	x				
(ii) police/customs agencies;	x	x				
(iii) other enforcement agencies;	x	x				
(iv) international organisations;	x	x				
(v) public entities;	x	x				
(vi) private entities;	x	x				
(l) information on legal persons associated with the data referred to in points (e) and (j):						
(i) designation of the legal person;	x	x				
(ii) location;	x	x				
(iii) date and place of establishment;	x	x				
(iv) administrative registration number;	x	x				
(v) legal form;	x	x				

Categories of data	Categories of person					
	Suspects and convicts	**Likely criminals**	**Contacts and associates**	**Victims**	**Witnesses**	**Informants**
(vi) capital;	x	x				
(vii) area of activity;	x	x				
(viii) national and international subsidiaries;	x	x				
(ix) directors;	x	x				
(x) links with banks.	x	x				
Victims						
(a) victim identification data				x		
(b) reason for victimisation				x		
(c) damage (physical/financial/psychological/other)				x		
(d) whether anonymity is to be guaranteed				x		
(e) whether participation in a court hearing is possible				x		
(f) crime-related information provided by or through victims, including where necessary on their relationship with other persons, for identifying suspects, convicts or likely criminals				x		
Witnesses						
(a) crime-related information provided by such persons, including information on their relationship with other persons included in the analysis work file;					x	
(b) whether anonymity is to be guaranteed					x	

Categories of data	Categories of person					
	Suspects and convicts	**Likely criminals**	**Contacts and associates**	**Victims**	**Witnesses**	**Informants**
(c) whether protection is to be guaranteed and by whom					x	
(d) new identity					x	
(e) whether participation in a court hearing is possible					x	
Informants						
(a) coded personal details						x
(b) type of information supplied						x
(c) whether anonymity is to be guaranteed						x
(d) whether protection is to be guaranteed and by whom						x
(e) new identity						x
(f) whether participation in a court hearing is possible						x
(g) negative experiences						x
(h) rewards (financial/favours)						x

Annex III: Europol's cooperation agreements

	EU bodies	Third countries	International organisations
Working arrangement	European Anti-Fraud Office (OLAF) European Investment Bank (EIB) European Public Prosecutor's Office (EPPO) European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) EUNAVFOR MED	Andorra San Marino United Kingdom Chile Qatar Mexico New Zealand Republic of Korea Israel Kosovo Armenia Japan Kosovo Specialist Chambers and Specialist Prosecutor's Office	
Operational agreement	Eurojust European Border and Coast Guard Agency (Frontex)	Denmark Albania Australia Bosnia & Herzegovina Canada Colombia	Interpol

		Georgia Iceland Moldova Montenegro Norway North Macedonia Serbia Switzerland Liechtenstein Monaco Ukraine United States of America	
Strategic agreements	European Central Bank European Commission European Centre for Disease Prevention and Control (ECDPC) European Union Agency for Law Enforcement Training (CEPOL) European Union Agency for Network and Information Security (ENISA) European Union Intellectual Property Office (EUIPO)	Brazil China Russia Turkey United Arab Emirates	United Nations Office on Drugs and Crime (UNODC) World Customs Organization (WCO)