

European Digital Rights' (EDRi) submission to the European Commission's call for evidence on a "new Europol regulation"

Introduction

European Digital Rights (EDRi)¹ is submitting the following contribution based on the input of members of the "Resist Europol" coalition. The coalition is an open group of activists, researchers, lawyers, journalists, prison and police abolitionists, civil society organisations and more with **a shared concern of the expanding EU policies, practices and agenda driven by criminalisation, surveillance and punishment.**

Its work is aimed at **resisting the continued expansion of Europol**, which is participating in the wider state and social structures of oppression responsible for the societal harms they claim to address. Its mission is to support the emergence and expansion of alternative practices that can lead to **societies where all people and communities are met with care, live in safety and in dignity.**

We thank the European Commission for the opportunity to express our shared concerns with regards to the plans to revise the Europol Regulation, which may include a further expansion of Europol's powers. The evolution of the agency's role and importance in the processing and analysis of personal data is not happening in a void. The reinforcement of the agency's surveillance infrastructure is particularly worrying in a context of increased criminalisation of social movements, solidarity and activism and the deployment of ever more intrusive and punitive technologies in the justice and law enforcement fields.

From this perspective, it is deeply alarming that the Commission's problem definition in the call for evidence is so clearly biased towards views of law enforcement. The objectives seem to solely focus on increasing Europol's data collection, areas of competence and surveillance capacities. However, we would like to stress there are **many issues in European law enforcement** (which have been highlighted by both civil society² and institutional actors³) **for which an EU action would be urgently needed** in order to guarantee justice, accountability and safety. To mention just a few: eradicating police violence, prohibiting discrimination against members of racialised, poor and other marginalised communities, addressing structural racism, etc. None of these problems are mentioned in the Commission's problem definition even though they are

1 European Digital Rights (EDRi) is an association representing more than 50 NGOs across Europe and experts who defend and protect human rights in the digital age: <https://edri.org/>

2 Equinox, Who protects us from the police?, June 2021, <https://www.equinox-eu.com/wp-content/uploads/2021/10/Equinox-Who-Protects-Us-from-the-Police.pdf>

3 Council of Europe Parliamentary Assembly Committee on Equality and Non-Discrimination, Ethnic profiling in Europe: a matter of great concern, 14 December 2020, <https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=28889&lang=en>
Fundamental Rights Agency, Addressing Racism in Policing, 10 April 2024, <https://fra.europa.eu/en/publication/2024/addressing-racism-policing>
Fundamental Rights Agency, FRA guide on preventing unlawful profiling, 5 December 2018, <https://fra.europa.eu/en/project/2017/fra-guide-preventing-unlawful-profiling>

major threats in the everyday life of millions of Europeans.

Europol is not immune to criticism, as its activities rely on the data received from Member States and third countries' law enforcement authorities, carrying the legacy of their racist policing practices. A revision of Europol's mandate could actually be an opportunity to tackle Europol's role in perpetuating discriminatory policing, police brutality, criminalisation and other harmful treatments in law enforcement and we encourage the Commission to address these questions in its evaluation process.

In response to the Commission's consultation call, we would like to share the following recommendations:

- In order to ensure a timely and informed public debate on the future of Europol, **the evaluation for the current Europol Regulation must be carried out before further revisions** can be considered;
- The Commission must add as a primary objective of its evaluation **a fundamental rights impact assessment** and flesh out its plan to carry it out;
- In order to produce a proper and complete fundamental rights impact assessment in both the evaluation and the impact assessment of a new legislative framework, the scope cannot be limited to suspects, but should **encompass, at a very minimum, all individuals whose data is processed by Europol** and thus, their fundamental rights interfered with. In addition, such assessment cannot be restricted to privacy and data protection rights only, but must **include a wider range of fundamental rights affected by Europol's activities**;
- **Any potential future mandate must be respect limits set out in the Treaties.** The objective of transforming Europol into "a truly operational agency" likely clashes with them and must therefore not be pursued.
- **The list of crimes for which Europol is competent should not be expanded** as it risks involving Europol's surveillance infrastructure in the criminalisation of public protest or increasing its policing of online speech. In particular, Europol's Internet Referral Unit's (IRU) activities must be brought in line with the Charter of Fundamental Rights or cease as soon as possible;
- Europol's **data mining practices should be stopped** by repealing the 2022 amendments allowing almost unrestricted data-driven policing. The data collection and processing by Europol must be limited to what is necessary for supporting targeted investigations by Member States' law enforcement authorities;
- Data exchanges with third countries must respect EU primary and secondary law. Cooperation with countries with systematic rule of law issues and human rights violations must be halted urgently;
- The absolute priority for the Commission should be to **improve the oversight, transparency and accountability of Europol.**

1. An evaluation for the current Europol Regulation must be carried out before further revisions can be considered

The first evaluation of the 2016 Europol Regulation was originally scheduled for May 2022, but this deadline was extended to June 2027 with the 2022 revision of the Europol Regulation. In the call for evidence, it is anticipated that the evaluation of the current Europol Regulation and the

impact assessment for a revision of Europol's mandate will run in parallel.

This approach and the repeated postponement of the 2016 mandate evaluation are highly problematic for two main reasons.

First, although an evaluation may feed into the impact assessment of a new legislative initiative, they constitute two separate processes which should not be conflated. The current Commission's plan of designing the evaluation of the 2016 mandate in a way that solely supports a new legislative proposal is fundamentally biased and pre-empts the results of what should remain an independent evaluation. It is apparent from the call for evidence that the Commission has already made up its mind about the shortcomings of the 2016 mandate, its corresponding solutions and the necessity of a revamped mandate. It is therefore expected that **the evaluation outcomes will only support such political vision and fail to provide reliable evidence of necessity and proportionality of the new proposed measures.**

Second, running these processes in parallel hinders a proper public, informed and timely debate about Europol's activities and their impacts on justice, safety and fundamental rights in Europe. For EDRi, it is imperative that the European Parliament and national parliaments are given an opportunity to scrutinise and debate the evaluation report, as foreseen by Article 68(2) of the Europol Regulation, before an impact assessment for a revision of Europol's mandate is carried out by the Commission. The same applies to scrutiny by civil society organisations and other relevant stakeholders to the extent that the main findings of the evaluation report are to be made public. **The foreseen process gives virtually no time or space to enable such debate and scrutiny. As a result, the Commission is acting against its obligations under the Article 68 of the Europol Regulation.**

In November 2023, the Commission presented a proposal on combatting migrant smuggling and trafficking in human beings, which included a significant expansion of Europol's powers, especially when it comes to its digital surveillance capabilities. This expansion of Europol's capacities and operational powers would apply to all categories of offences for which the agency is competent. The rushed proposal was presented without a proper impact assessment contrary to the Interinstitutional Agreement of 13 April 2016 on Better Law-Making.

The 2023 proposal to amend the Europol Regulation is currently in trilogue. In their adopted positions, both Council and the European Parliament have made substantial amendments to the Commission's proposal, which removed a large part of the expanded powers for Europol.

Against this backdrop, **we consider a proposal to expand Europol's powers in Q2 2026 highly premature as there is no evidence for the necessity of this expansion or the urgency.** The next proposal must be evidence-based and allow for proper democratic scrutiny of the first evaluation report before any new expansion of Europol's power can be considered.

With regards to the content, we note with great concerns that the scope of the evaluation foreseen in the call for evidence does not include any assessment of the impacts of Europol's past and current activities on fundamental rights. Europol repeatedly violated fundamental

rights in the past years, for example by circumventing its own data protection limitations⁴ or by illegally denying data subject rights.⁵ It is therefore crucial to assess how the current rules have failed to prevent these violations, how its accountability and oversight mechanisms have worked in these circumstances and how Europol's various current activities and actions comply with the principle of necessity and proportionality. **We recommend that the Commission adds as a primary objective of its evaluation a fundamental rights impact assessment and fleshes out its plan to carry it out.**

2. The fundamental rights impact assessment cannot be limited to suspects and to privacy and data protection rights

Regarding the impact on fundamental rights of the future new Europol mandate, the call for evidence merely notes that "certain measures may interfere with the fundamental rights of *suspects* or, more generally, their privacy and data protection rights (Articles 7 and 8 of the Charter)." (emphasis added).

EDRi would like to point out that **this approach is completely inadequate, incomplete and arbitrary** for the following reasons:

- The 2016 Europol Regulation permits Europol to process personal data about **many more data subject categories than just "suspects"**, namely convicted persons, persons who are suspected to commit a crime in the future, contacts and associates, victims, witnesses and informants. Impacts of Europol's activities and surveillance powers on their fundamental rights might largely differ depending on their status.
- Since 2022, the Europol Regulation permits Europol to effectively process personal data about the entire population through large data sets. The data-mining processing to find unknown persons of interest (e.g. suspects) is highly intrusive and represents a particularly **serious interference with fundamental rights of the entire population** - which we consider amounting to mass surveillance and thus disproportionate (see section 5 below). Unless the new legislative proposal deletes the provisions allowing for the processing of personal data of individuals with no link to criminal activity, the fundamental rights impact assessment scope must, at the very minimum, include all individuals, regardless of their status.
- The rights to data protection and to privacy are not the sole fundamental rights and freedoms impacted by Europol's activities. It is therefore **too restrictive to limit the impact assessment to those rights only**. We recommend to expand the scope to encompass other fundamental rights and freedoms, such as but not limited to freedom of expression and information, freedom of assembly and association, the right to liberty and security, the right to non-discrimination, the right to effective remedy and to a fair trial, the presumption of innocence and the right of defence, the right to asylum and the rights of the child.

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

5 EDRi, Rather delete than comply: how Europol snubbed data subject rights, 28 September 2022, <https://edri.org/our-work/rather-delete-than-comply-how-europol-snubbed-data-subject-rights/>

Lastly, we would like to stress that Europol's core activity is processing of personal data and therefore *does* (not "may") entail an interference with the rights to privacy and data protection as per the jurisprudence of the Court of Justice of the European Union. The false assumption that the interference is indeterminate could negatively impact the quality of the fundamental rights impact assessment. **We recommend that the Commission pay serious attention to the varying degrees of interference with fundamental rights that the proposed measures *will* entail.**

3. The limits on Europol's powers in the Treaties must be respected

We note the ambition of the current Commission to make Europol a "truly operational police agency and more than double its staff over time."

Europol was deliberately founded without executive powers as TFEU Article 88(3) explicitly requires that any operational action of Europol must be carried out in liaison and agreement with the Member State(s) whose territory is concerned, and that application of coercive measures is the exclusive responsibility of the competent national authorities.

In our opinion, the 2022 revision of the Europol Regulation and the 2023 Commission proposal grant Europol *de facto* executive powers in a way that may be contrary to TFEU Article 88.

Europol can request and receive personal data directly from private parties, despite Article 88(2) explicitly stating that Europol's tasks may include the "collection, storage, processing, analysis and exchange of information, in particular that *forwarded by the authorities of the Member States or third countries or bodies.*" (emphasis added).

In the Commission's analytical document for the 2023 proposal, the definition of "coercive" appears overly restrictive as it only encompasses measures that "impose a specific constraint" on a person such as their arrest or performing a house search. However, data extraction and analysis from seized mobile devices performed by Europol's staff are equally intrusive and can be compared to a house search (arguably even more considering the amount and intimate nature of information stored on smartphones which may reveal more details about a person's thoughts, preferences, opinions and private life).

Future revisions of Europol's mandate must respect the limitations in the Treaties where Europol's mission is to support Member States' competent authorities and only facilitate information exchange between them. Proposals that require national competent authorities to unconditionally share certain information with Europol and proposals that grant Europol independent powers to analyse large data sets on a massive scale (e.g. the biometric data provision in the 2023 Commission's proposal) exceed the boundaries of a mission to support Member States.

4. Any expansion of crimes for which Europol is competent should not lead to Europol being involved in criminalisation of public protest or policing online speech

One of the objectives of the envisaged initiative is to maximise "the relevance of Europol's

support by adjusting its mandate so as to cover all emerging forms of crime and threats within the limits set out in Article 88 TFEU."

TFEU Article 88(1) restricts Europol's mission to "serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy." This is currently articulated through a list of crimes in Annex I of the Europol Regulation.

For EDRi, it is important that any updates to the list of crimes in Annex I are based on evidence and considerations that respect the principles of necessity and proportionality. The reference to serious crime, terrorism and crimes that affect a common interest covered by a Union policy in TFEU Article 88(1) clearly precludes that Europol becomes involved in all criminal investigations in Member States. That also applies to Europol's involvement solely as a data hub, that is facilitating information exchange between Member States and supporting national investigations.

Moreover, any expansion of Europol's work area in Annex I must be for activities that genuinely constitute crimes. Europol is a law enforcement agency, and involvement of Europol in specific activities invariably means that these activities will be treated as crimes. In particular, **migration as such should never be criminalised through the Europol Regulation**, even though some criminal activities are sometimes involved in the context of migration (e.g. human smuggling and trafficking).

According to the call for evidence, measures could include "(i) expanding the areas of activity and tasks as well as the types of crime and threats covered by the Europol Regulation, such as sabotage, hybrid threats or information manipulation."

These suggestions could lead to an expansion of Europol's activities that EDRi would regard as highly problematic. Sabotage is general term that may encompass serious offences (presumably already within Europol's competence), but sabotage is also increasingly used by law enforcement authorities to investigate and prosecute civil disobedience actions by e.g. climate activists.⁶ We are extremely concerned that Europol's involvement in this area could exacerbate the criminalisation of public protest that is taking place in many Member States and lead to disproportionate exchange of personal data about activists via Europol.⁷ **In the broader, worrying context of penal inflation and shrinking civic space all across the EU⁸, it is fundamental that Europol does enable the further repression and surveillance of social movements, human rights organisations and defenders. We therefore warn against expanding the list of crimes for which Europol would be competent to act, especially to "sabotage".**

6 State repression of environmental protest and civil disobedience: a major threat to human rights and democracy, Position Paper by Michel Forst, UN Special Rapporteur on Environmental Defenders under the Aarhus Convention, February 2024, https://unece.org/sites/default/files/2024-02/UNSR_EnvDefenders_Aarhus_Position_Paper_Civil_Disobedience_EN.pdf

7 Statewatch, EU: Definition of "potential terrorists" opens door to broad information-sharing, 2 October 2024, <https://www.statewatch.org/news/2024/october/eu-definition-of-potential-terrorists-opens-door-to-broad-information-sharing/>

8 Civil Liberties, Rule of Law Report 2024, 23 February 2024, <https://www.liberties.eu/f/oj7hht>

On the contrary, we strongly encourage the Commission to evaluate the necessity, impact, effectiveness and efficiency of Europol in certain crime areas and **consider the removal of some of them from Annex I where it is proven unnecessary or inefficient**. In particular, where criminalisation or punitive approaches have been found ineffective, harmful or counterproductive⁹, we recommend to remove them from Europol's mandate.

Hybrid threats and manipulation of information is also a problematic expansion since it covers a range of different activities, many of which should not be regarded as a crime. Disinformation and misinformation is a serious problem for society and public discourse in the EU, but **criminal law is not the appropriate method for addressing this problem**. Such approach would likely lead to restrictive measures failing to comply with the principles of necessity and proportionality. The EU has already taken various steps in the past years to implement adequate and proportionate measures that address some of the root causes of information manipulation, notably in the the Digital Services Act (DSA) (although EDRi argues that more is needed¹⁰). Europol's involvement in e.g. manipulation of information could lead to Europol policing online speech as an Orwellian "ministry of truth", which would be highly inappropriate.

EDRi is already highly critical of Europol's activities through its Internet Referral Unit that according to its own description "detects and investigates malicious content on the internet and in social media."¹¹ Since the IRU (which has no executive powers) sends non-binding notifications to online service providers for their voluntary consideration in a highly opaque manner, there are no effective safeguards against arbitrary censorship of online speech, and no meaningful oversight that these referrals are limited to online content which constitutes criminal offences covered by Annex I. The IRU has the power to create pressure to have content, of which the legality has not been assessed by a competent judicial authority, deleted by private companies, but bear no responsibility or accountability for doing so. Increasing its powers and scope of action would worsen its non-compliance with the principles of legality and necessity under the Charter of Fundamental Rights.

We strongly oppose any further involvement of Europol in policing online speech, whether through IRU referrals or other measures.

5. Europol's data mining practices should be stopped and its data processing limited to what is strictly necessary

In the original 2016 Europol Regulation, Europol was only allowed to process personal data about suspects, convicted persons and persons who are suspected to commit a crime in the future, contacts and associates, victims, witnesses and informants (Annex II of the Europol Regulation). This list contains the categories of individuals that national law enforcement authorities would come in contact with during investigations and targeted intelligence gathering.

⁹ Studies at national level may be a great source of information.

¹⁰ EDRi, EU negotiators approve good DSA, but more work is needed to build a better internet, 25 April 2025, <https://edri.org/our-work/eu-negotiators-approve-good-dsa-but-more-work-is-needed-to-build-a-better-internet/>

¹¹ EU Internet Referral Unit - EU IRU: Monitoring terrorism online <https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc/eu-internet-referral-unit-eu-iru>

Notable, the data protection rules in Annex II prevented Europol from using predictive policing practices where personal data is collected indiscriminately about the entire population, and where data-mining tools, often in the form of opaque AI systems, are used to identify potential unknown suspects. **This type of data-driven policing is inherently discriminatory** and has been documented in numerous studies to exacerbate existing inequalities and further criminalise racialised, marginalised and poor communities.¹²

The 2022 revision of the Europol Regulation introduced legal bases in Articles 18 and 18a for processing personal data in large data sets not limited to the permitted categories of data subjects in Annex II. These amendments were largely a response to an EDPS investigation in 2019, where Europol was admonished for unlawfully collecting personal data about persons unrelated to criminal investigations, and ordered to delete the data.¹³

Specifically, whilst the 2022 amendment nominally retained the categories of data subjects in Annex II for which Europol is allowed to process operational personal data, Europol was allowed to "temporarily" (for up to 18 months or more) process large data sets for the purpose of determining whether the processing complies with the conditions in Annex II.

In effect, Europol is allowed to indiscriminately collect large data sets and then use pre-filtering to determine the individuals which fall into the permitted categories in Annex II. **This incentivises NSA-style mass surveillance and data-mining practices to find unknown suspects or persons of interests.** Moreover Article 18a goes even further by permitting Europol to derogate from its own data protection rules when an operational analysis cannot be carried out in compliance with these rules.

The call for evidence mentions "targeted amendments to the Europol Regulation for Europol to better play its role of information hub (complementing previous targeted amendments)" including "(ii) new legal provisions to overcome the most serious technical and legal obstacles to information access, collection, sharing and analysis."

Since the 2022 amendment legalised Europol's (then) illegal data practices, even retroactively, and arguably went even further by permitting Europol to derogate from its own data protection rules, **EDRi finds it very unclear what limitations "the most serious technical and legal obstacles" refer to.**

The call for evidence also mentions "(iii) simplification of the current legal provisions as well as new provisions corresponding to identified best practices to increase legal certainty". We agree

- 12 ENAR, Data-Driven Policing: The Hardwiring of Discriminatory Policing Practices across Europe, November 2019, available at: <https://www.enar-eu.org/IMG/pdf/data-driven-profiling-web-final.pdf>
Douwe Korff, The EU's own Snowden scandal, 17 January 2022, <https://www.ianbrown.tech/2022/01/17/the-eus-own-snowden-scandal>
Douwe Korff, Opinion on Core Issues in the PNR CJEU Case, November 2021, <https://www.ianbrown.tech/wp-content/uploads/2021/12/KORFF-FREE-Paper-on-Core-Issues-in-the-PNR-Case.pdf>
- 13 EDPS, EDPS orders Europol to erase data concerning individuals with no established link to a criminal activity, 10 January 2022, https://www.edps.europa.eu/press-publications/press-news/press-releases/2022/edps-orders-europol-erase-data-concerning_en

that **there is an urgent need to increase legal certainty about Europol's processing of personal data**, because the 2022 amendment allows Europol to process large data sets under conditions that **lack basic requirements of clarity and foreseeability for the persons concerned**.

Data-mining processing for the purpose of identifying unknown persons of interest in large data sets containing indiscriminately collected personal data constitutes a particularly serious interference with fundamental rights. There is a high risk of circumventing critical safeguards in criminal procedural laws and the presumption of innocence. Personal data about the entire population is processed under the assumption that everyone in the dataset is a potential suspect.

Under the case law of the Court of Justice, EU law which restricts the right to protection of personal data must lay down clear and precise rules governing the scope and application of the measure and imposing minimum safeguards, so that the persons concerned have sufficient guarantees to protect effectively their personal data against the risk of abuse.¹⁴

We seriously doubt that the current Europol Regulation complies with these requirements for the processing of large data sets. For example, the Regulation contains no objective criteria for the large data sets that can be collected by Europol from Member States' competent authorities or other sources, and the Regulations contains no restrictions on the algorithms that can be used for analysing large data sets.

We recommend that the 2022 amendments allowing almost unrestricted data-driven policing are repealed. The data collection and processing by Europol must be limited to what is necessary for supporting targeted investigations by Member States' law enforcement authorities.

6. Data exchanges with third countries must respect EU primary and secondary law

Under EU law, personal data can only be transferred to third countries when controllers can ensure an essentially equivalent level of protection to that guaranteed within the EU. The main instruments for ensuring that in Article 25 of the Europol Regulation are (1) adequacy decisions under the Law Enforcement Directive 2016/680, (2) international agreements between the EU and the third country, (3) certain cooperation agreements concluded before May 2017, and (4) when appropriate safeguards for the transfer are provided for by either a legally binding instrument with the recipient competent authority or an assessment by Europol of all the circumstances surrounding the transfer.

In addition, Europol may transfer personal data to a third country based on derogations in Article 25(5). This can only be done on a case-by-case basis, and derogations cannot lead to systematic, massive or structural transfers of personal data.

EDRI has noted an increased political interest in transferring personal data from Europol to countries with systemic rule of law problems and frequent fundamental rights violations, typically in the context of EU cooperation with these countries to limit migration to the EU or

¹⁴ See e.g. C-817/19, *Ligue des droits humains*, para. 117.



support the security agenda of the EU.¹⁵ Since these countries cannot offer an essentially equivalent level of protection for personal data, derogations may be relied upon for the transfer.

In the 2023 proposal on combatting human smuggling, recital 8 envisages an increased use of derogations in order to transfer personal data to third countries not covered by Article 25(1). In combination with the overall intention of increased information sharing with third countries, the proposal creates a risk that derogations will be used on a *de facto* systematic basis (even though is not permitted by the Europol Regulation) with detrimental impact on the fundamental rights of people in these countries.

For EDRi, it is imperative that transfer of personal data to third countries does not lead to human rights violations. The best way to uphold that principle is to only transfer personal data to countries where an essentially equivalent level of protection can be guaranteed. If the EU wishes to cooperate with countries where this cannot be guaranteed, the modalities of the cooperation cannot include transfer of personal data from the EU.

In this connection, EDRi wishes to emphasise that whilst recent initiatives have focused transfers of personal data from the EU to third countries, **we are highly critical of Europol's practices regarding receiving information, including personal data, from countries with disastrous human rights records.** There is a high risk that Europol will be engaging in data laundering of personal data and other information that may have been obtained under torture or other serious human rights violations. These human rights violations could also affect the accuracy of the personal data (e.g. if obtained under torture), something that may not be recognised when the received personal data is further processed by Europol or Member States' competent authorities. Recital 39 of the Europol Regulation specifically requires Europol to not process any information which has clearly been obtained in obvious violation of human rights. Regrettably, this wording ("obvious violation") gives Europol an incentive to not ascertain all relevant facts about how the information was collected by the third country source.

Furthermore, some of Europol's cooperation agreements that allow for exchange of personal data [Article 25(1)(c)] date from the early 2000s. They are likely to contain elements that do not meet current EU data protection standards in the Law Enforcement Directive 2016/680 and the Data Protection Regulation for EU institutions 2018/1727, as well as the updated case law from the Court of Justice. Article 25(4) of the Europol Regulation requires the Commission to assess these agreements by 14 June 2021. The Commission launched a dedicated call for evidence for this task in April 2022, but the initiative does not seem to have been brought to completion.¹⁶

We strongly oppose any initiative which will lead to increased data sharing with third countries that do not have adequate data protection standards. In addition, we recommend that the Commission completes the evaluation of the cooperation agreements from before May 2017 and initiate the necessary processes to update these instruments to be compatible with modern EU data protection standards.

15 EDRi, Civil society raises concerns over Europol-Egypt cooperation agreements, 16 January 2025, <https://edri.org/our-work/civil-society-raises-concerns-over-europol-egypt-cooperation-agreements/>

16 Proposal for a Regulation on police cooperation to counter migrant smuggling and human trafficking: Targeted substitute impact assessment, European Parliamentary Research Service, 5 February 2025 [https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU\(2025\)765777](https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2025)765777)

7. There is an urgent need to improve the oversight, transparency and accountability of Europol

First, Europol greatly **suffers from a lack of accountability**. Yet the Commission's call for evidence does not even acknowledge this issue in the "problems this initiative aims to tackle" section.

Europol was caught on several occasions breaching its own rules and violating fundamental rights. A major problem is that it is barely held to account after violations are discovered. After being admonished by the data protection oversight body, the European Data Protection Supervisor, for unlawfully processing data of (potentially hundreds if not thousands) individuals with no links to criminal activities, **Europol faced absolutely no consequence**. Instead, the European Commission and the EU legislators lifted the data protection limitations and retroactively legalised Europol's illegal data processing practices in the 2022 reform – leaving the agency to continue its activities with impunity. More recently, Europol refused to confirm that it will delete data unlawfully received from Frontex, and even suggested that it would keep this information, arguing that Frontex's unlawful transfer "does not mean that Europol's data processing of the information received from Frontex was non-compliant".¹⁷ If Europol continues to process (analyse, use, etc.) data which it should not have received, data protection rules are rendered void and useless. Once again, it demonstrates how the agency pays absolutely no heed to the law, in particular to fundamental rights protections.

Yet, rules are absolutely necessary in the field of law enforcement to prevent abuses, limit interferences with, and sanction violations of fundamental rights. It is particularly worrying that, in the context of Europol's mission, they are portrayed as obstacles to the realisation of operational objectives. **The way in which Europol always escapes responsibility undermines justice and people's trust in EU institutions**. That is why it should be a priority for the Commission to remedy Europol's current lack of accountability.

Second, **Europol is a highly opaque agency**. Investigative journalists have pointed out the agency's aversion to transparency and public oversight.¹⁸ Attempts to access meaningful information on Europol's activities are systematically obstructed "through procedural delays, heavy redactions, or blanket rejections on 'public security' grounds".¹⁹ **Civil society organisations and independent journalistic investigations constitute a vital element of Europol's oversight ecosystem**. However, their ability to contribute effectively is significantly hindered by limited or non-existent access to information regarding the agency's operations²⁰, thereby restricting transparency and accountability.

Third, Europol's current oversight mechanisms are largely insufficient and ineffective. The impact of Europol's activities on peoples' lives continues to grow, accompanied by increased risks of

17 Ludek Stavinoha, Apostolis Fotiadis and Lola Hierro, Frontex unlawfully shared thousands of people's personal data with Europol, Solomon, 7 July 2025 <https://wearesolomon.com/mag/format/investigation/frontex-unlawfully-shared-thousands-of-peoples-personal-data-with-europol/>

18 Ludek Stavinoha, Giacomo Zandonini and Apostolis Fotiadis, Europol's deepening aversion to transparency, EUobserver, 19 May 2025, <https://euobserver.com/migration/ara76e008c>

19 Ibid

20 Ibid

abuse and errors, particularly as powers continue to grow in the successive reforms of the past years whereas safeguards become less effective or clearly defined and oversight mechanisms are not enhanced – if not squarely undermined.²¹

The oversight ecosystem must comprise multiple, complementary layers of scrutiny to ensure effective checks and balances that extend beyond any single institution. Internal controls, such as those conducted by the Fundamental Rights Officer (FRO), currently lack independence from the agency to guarantee objective oversight. External administrative supervision by the European Data Protection Supervisor (EDPS) remains limited in scope to personal data processing and generally suffer from a lack of resources. Furthermore, the political oversight function provided by the Joint Parliamentary Scrutiny Group (JPSG) is constrained by its operational framework and its restricted access to meaningful information, which impedes its capacity to exercise robust political scrutiny.

Given the expanding mandate of the agency—augmented by increased data collection and the deployment of advanced technologies such as artificial intelligence—**the establishment of a comprehensive EU-wide oversight system is essential**. This system must acknowledge the multilayered nature of scrutiny and accommodate the distinct operational modalities of each oversight mechanism. It should function in close coordination with national oversight bodies and incorporate judicial involvement to ensure full accountability.

A criminal justice framework founded on the rule of law requires **clearly articulated legal provisions, enforceable individual rights, and coordinated oversight mechanisms**. The present disparity between the growth of policing powers and the adequacy of corresponding scrutiny poses a threat to the integrity of the entire oversight ecosystem; the weakening of any single component risks systemic failure.

Sources and further reading:

Recommendations on the revision of Europol's mandate, EDRi position paper, 10 June 2021
<https://edri.org/wp-content/uploads/2021/06/Recommendations-on-the-revision-of-Europol-s-mandate.pdf>

Fair Trials raises serious concerns about increasing mandates of Europol and Frontex, Fair Trials, 24 November 2022 <https://www.fairtrials.org/articles/news/fair-trials-raises-serious-concerns-about-increasing-mandates-of-europol-and-frontex/>

Stopping the Unfettered Expansion of Europol's Digital Surveillance Powers against Migrants, position paper on the European Commission's proposal for a Regulation to enhance Europol's support in 'preventing and fighting migrant smuggling', Protect Not Surveil coalition, 20 February 2025 <https://edri.org/our-work/protect-not-surveil-position-paper-stop-europol-s-expanding-digital-surveillance-against-migrants/>

21 EDPS, [Amended Europol Regulation weakens data protection supervision](https://www.edps.europa.eu/press-publications/press-news/press-releases/2022/amended-europol-regulation-weakens-data_en), 27 June 2022, https://www.edps.europa.eu/press-publications/press-news/press-releases/2022/amended-europol-regulation-weakens-data_en



Sarah Tas and Flavia Patanè, Proposal for a regulation on police cooperation to counter migrant smuggling and human trafficking. Targeted substitute impact assessment, EPRS, February 2025, [https://www.europarl.europa.eu/RegData/etudes/STUD/2025/765777/EPRS_STU\(2025\)765777_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2025/765777/EPRS_STU(2025)765777_EN.pdf)