Contribution ID: 2a724c0e-f8f6-40b4-a8ac-9979cd6b186f
Date: 17/07/2020 15:22:18

Strengthened Mandate for Europol Questionnaire

Fields marked with * are mandatory.

Strengthened Mandate for Europol Questionnaire

Introduction

The Commission has included in its Work Programme 2020 a legislative proposal to “strengthen the Europol mandate in order to reinforce operational police cooperation” among Member States. The need for such initiative lies on the need to ensure that the Agency is equipped to face the current and future challenges posed by criminality and terrorism.

The objective of this consultation is to receive feedback, comments and observations on the challenges that the Commission has identified for the revision of Europol’s mandate.

The questionnaire addresses different topics, where the respondent will be able, in case (s)he wishes, to further elaborate. The questionnaire also gives the possibility to upload documents which are considered relevant for this consultation.

The questionnaire aims at receiving feedback on the following areas:

1. Direct exchange of personal data between Europol and private parties.
2. Initiation of criminal investigations
3. High Value Targets
4. Processing of data for prevention purposes
5. Europol’s cooperation with partners
6. Legal regime applicable to Europol operational data
7. Europol’s access to SIS and Prüm framework
8. Research and Innovation

Each section contains a short description of the background to the question. More detailed description of the topics can be found in the Inception Impact Assessment, published on 14 May 2020 in the Better Regulation Portal of the European Commission.

The Commission is not going to publish individual responses. The Commission may publish statistics gathered from this questionnaire.

Information

* First name

Chloé

* Surname

Berthélémy

* Name of organisation

European Digital Rights

* Email

chloe.berthelemy@edri.org

Type of organisation

- ○ Law enforcement authority
- ○ Judicial authority
- ○ Data protection authority
- ○ Private entity
- ○ EU Institution and bodies
- ○ Academic instutiton / research
- ○ International Organisation
- ◉ Non-Governemntal Organisation
- ○ Other

If other, please specify

Type of organisation

- ○ Local
- ○ Regional
- ○ National
- ◉ International

Country of organisation

- ○ Austria
- ◉ Belgium
- ○ Bulgaria
- ○ Croatia
- ○ Cyprus
- ○ Czechia

- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Ireland
- Italy
- Latvia
- Lithuania
- Luxembourg
- Malta
- Netherlands
- Poland
- Portugal
- Romania
- Slovak Republic
- Slovenia
- Spain
- Sweden

☑ I agree with the personal data protection provisions

Privacy_statement_targeted_consultations_HOME_June_2020.docx

* Do you agree that the Commission may use the information provided to contact you?

- (●) Yes
- ( ) No

* **Q1.** Do you think that there is a need to strengthen Europol's legal mandate (Regulation (EU) 2016/794) to support Member States in preventing and combating serious crime, terrorism and other forms of crime which affect a common interest of the European Union?

- ( ) Yes
- (●) No
- ( ) Other

Please explain.

4000 character(s) maximum

EDRi believes that the revision of the Europol Regulation (2016/794) is premature and deserves first an evaluation of its added value in the field of police cooperation and its impact on fundamental rights, especially how the safeguards are being respected (or not) in practice.

It is highly surprising that the EU Commission proposes a revision of Europol's rules before even the first implementation and review cycle of five years (Article 68) is complete. The first fully fledged evaluation of the Regulation is planned for 2022 to assess the effectiveness and efficiency of Europol and of its working practices. In its Roadmap, the European Commission states that it does not intends to carry out an evaluation of Europol's current mandate because "the amount of evidence that can be collected for the purpose of a fully fledged evaluation is limited and non-representative".

However, the Commission and the Council already foresee the revision of the mandate, before there is any evidence that the current practices are unfit for purpose. It seems to be at odds with the Better Regulation agenda promoted by the Commission itself, which requires EU legislation to be based on solid evidence.

EDRi recommends to first carry out a full and public evaluation of the 2016 Europol Regulation before considering reforms of the Agency's mandate.

Direct exchange of personal data between Europol and private parties

Article 26 of the Europol Regulation significantly limits Europol's ability to exchange personal data with private parties (such as online service providers, financial institutions, or non-governmental organisations). There are a few exceptions to this rule (notably in the area of referrals of illicit content that is publicly available online). However, in most investigations, the Europol Regulation prohibits the Agency from requesting information from private parties. In addition, Europol is not allowed to receive personal data from private parties. While private parties may submit personal data on criminal activities to the Agency, Europol is not allowed to keep this data for longer than necessary to identify the Member States concerned, unless a Member States resubmits this personal data as a 'national' contribution to Europol's databases. If Europol is not able to identify the Member State concerned, the Agency has to delete the personal data regardless of its content and potential significance in combating and preventing crime.

Q2. There is evidence of an increase in serious criminal offences committed online, on the dark web or with the help of such information technologies (cyber-enabled crimes). Do you agree that the role of private parties in preventing and countering cyber-enabled crimes is growing as they are often in possession of significant amounts of personal data relevant for law enforcement operations?

- ○ Yes
- ○ No
- ◉ Other

Please explain.

4000 character(s) maximum

The digital environment also offers both opportunities to commit new offences and to impose new restrictions on people's online rights. According to a 2017 study (see S. Rubinstein, T. Nojeim and D. Lee, Systematic Government Access to Private-Sector Data. A Comparative Analysis. In: H. Cate and X. Dempsey, Bulk Collection: Systematic Government Access to Private-Sector Data. Oxford Scholarship Online, 2017), there has been an increase worldwide in government demands for data held by the private sector. The study concludes that “in all countries studied [including France, Germany, the UK and Italy], the law provides an inadequate foundation for systematic access to data, both from a human rights perspective and at a practical level. Transparency about systematic access remains weak.” What they mean by “systematic access” is access by the government to private-sector databases or networks whether direct or mediated by the company that maintains the database or network, to large volumes of data.

If companies sometimes hold valuable information for criminal investigations, it remains that current legal frameworks to access it are “vague and ambiguous, and government interpretations of them are often hidden or even classified; that practices are often opaque; and that oversight and reporting mechanisms are either absent or limited in scope when they exist”.

As recently stated by the Advocate General (AG) Campos Sánchez-Bordona of the Court of Justice of the European Union (CJEU) in his opinions on four cases regarding data retention regimes in France, Belgium and the UK, national security can neither serve as a blank cheque to justify indiscriminate mass surveillance and cannot be used as an escape route from relevant data protection laws. Instead, access to data for law enforcement must be part of the Rule of Law and must respect fundamental rights.

Q3. Do you consider that the current restrictions on Europol’s ability to exchange personal data with private parties limits Europol’s capacity to effectively support Member States’ investigations?

- ○ Yes
- ○ No
- ◉ Other

If yes, what type of limitations do you envisage? (multiple answers possible)

- ☐ Risk of loss of information (e.g. where Europol does not have enough information to identify the Member State concerned).
- ☐ Risk of delays (e.g. where the identification of the Member State concerned is difficult and time-consuming).
- ☑ Lack of legal certainty for private parties, when they submit personal data to Europol.
- ☐ Inability of Europol to support Member States law enforcement authorities in obtaining personal data from a private party outside their jurisdiction.
- ☑ Other

Please explain.

4000 character(s) maximum

Several initiatives at European Union (EU) level, like the proposed regulation on European Production and Preservation Orders for electronic evidence in criminal matters (so called “e-evidence” Regulation), seek to “facilitate” access to personal data held by private companies by law enforcement authorities.

Many critics, including EDRi, bar associations, academics, the European Data Protection Board (EDPB), and other civil society organisations oppose the very idea behind the “e-evidence” proposal because it weakens judicial cooperation and risks to heavily infringing fundamental rights without introducing the necessary safeguards. Eight EU Member States in the Council also expressed doubts about the very constitutionality of this kind of proposal and criticised the “far reaching consequences (…) of the proposed regulation” as well as the lack of “checks and balances” and “guarantees for the protection of fundamental rights of citizens, freedom of press and freedom of expression and of public, national interests (...)”. Finally, the previous European Parliament Committee responsible (Committee on Civil Liberties, Justice and Home Affairs, LIBE) expressed serious criticism in a series of Working Documents.

The “e-evidence” Regulation as well as the foreseen extension of Europol’s powers in the field of data exchanges with private parties almost turn companies into judicial authorities. Indeed, they must decide whether the demand or request is lawful, proportionate and necessary. If companies feel coerced into handing over citizens’ data, there is a big risk for human rights. The work of the Europol Internet Referral Unit (IRU) at Europol shows how the Agency can put pressure on companies to restrict fundamental rights (in this case by deleting content) without any responsibility or accountability (in this case for potential over-removal of legitimate content). This mechanism hardly complies with the EU Charter’s requirement that restrictions of fundamental rights must be “provided for by law” and not based on opaque “cooperation” between law enforcement authorities and private companies.

Furthermore, rules governing the disclosure of people’s data rarely include a notification to the affected individuals or introduce exceptions to this notification requirement, making it very difficult for the user to defend her/his rights and contest access to his/her personal data.

Q4. Do you consider that, in order to fulfil its role as an information hub, Europol should be able to request and obtain data directly from private parties?

- ○ Yes
- ◉ No
- ○ Other

Please explain.

4000 character(s) maximum

Europol should not be able to avoid procedural safeguards and accountability mechanisms provided for in EU and national laws, including data protection safeguards.

As per its mission, Europol's main task is to "collect, store, process, analyse and exchange information" that it gathers from Member States, EU bodies and "from publicly available sources, including the internet and public data".

Since Europol is not a competent authority with executive powers, the proposal for effective cooperation with private parties would institutionalise a system of voluntary disclosure of personal data by online service providers and other private companies. EDRi has consistently opposed voluntary disclosures of personal data since this represents further processing of that data by the private controller for a purpose inconsistent with the original purpose. Disclosure of personal data to law enforcement bodies should always be regarded as a restriction of fundamental rights that must be provided for by law and satisfy requirements of necessity and proportionality in accordance with Article 52(1) of the Charter of Fundamental Rights. There is an inherent logical contradiction between disclosures that would be both "voluntary" for private companies and "necessary" for objectives of general interest.

The current rules are intended to prevent Europol from breaching procedural rules governing the collection and processing of evidence in Member States. Direct "cooperation" with service providers, whereby Europol directly requests data from the providers, affects the territorial sovereignty of Member States in which the order is executed (executing State). As a result, the executing State cannot effectively fulfill its responsibility to protect the fundamental rights of its citizens since it has no knowledge of the data transfers taking place. Procedural rules for the collection and processing of personal data in criminal matters also guarantee that collected evidence will not be declared inadmissible by the courts later. EDRi believes that access to personal data by Europol must be validated by the competent authority in the executing State in order to ensure the verification of immunities or other specific protections granted by national laws that restrict the access to certain categories of personal data.

In addition, judicial review and validation by a competent authority are always required when fundamental rights interference are at stake, because it ensures that the data request meets the necessity and proportionality tests. Judicial review and validation of data access request should only be carried out by a court or an independent administrative authority in accordance with CJEU jurisprudence. Europol does not fall within the definition of a court or an independent administrative authority to access personal data as required by the CJEU. If Europol was able to request and obtain data directly from private parties, the system completely falls short of the rights-protective procedural requirements and of strong judicial oversight required under the rule of law.

Furthermore, the possibility for Europol to directly receive information by private parties is limited by its own legal basis. Indeed, Article 88(2) states 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.". This can hardly encompass Europol receiving and actively requesting data from private companies on a larger scale.

Q5. Do you see merits in enabling Europol to request and receive personal data directly from private parties on behalf of Member States' law enforcement in order to facilitate exchanges of personal data between Member States' law enforcement and private parties?

- ○ Yes
- ◉ No

- Other

Please explain.

4000 character(s) maximum

There is a risk that this system encourages Member States to bypass existing procedural safeguards that apply to Member States' law enforcement authorities when seeking access to personal data in accordance with national or Union law, e.g. prior review by a court or an independent administrative body. The voluntary disclosure of data by companies incentivises a structural shift in data collection practices from Member States' authorities to Europol in order to avoid what may be perceived as "red tape" obstacles, which would have a detrimental effect on fundamental rights. The Commission's Impact Assessment mentions a "reduction of the administrative burden for national law enforcement authorities" as a likely impact of Europol "cooperating in a direct and more efficient way with private entities", without considering the potential adverse implications for fundamental rights.

Q6. Which aspects would be important to include in a possible regime to allow Europol to exchange personal data directly with private parties? (multiple answers possible)

- [ ] Any such regime should be voluntary for the private parties concerned (i.e. no obligation to share personal data with Europol).
- [ ] Any such regime should be in full compliance with fundamental rights (including a fair trial) and applicable European legislation on data protection.
- [ ] Any such regime should clarify that private parties should not expect to receive information related to operational activities, because they are not state actors.
- [ ] Any such regime should ensure that such direct exchanges are based on a procedure of consent from the Member States (e.g. from Europol's Management Board).
- [ ] Any such regime should ensure that Europol must notify the relevant national competent authorities of the Member States concerned by the personal data transmitted to Europol by a private party as soon as this Member State is identified.
- [x] Other

If other, please explain.

4000 character(s) maximum

EDRi opposes the Commission's proposal to expand Europol's powers in the field of data exchange with private parties for several reasons: (1) The lack of evidence and evaluation of the effectiveness of the existing framework for exchange of data between Europol, Member States authorities and private parties, (2) the original nature and mission of Europol as a European agency for law enforcement cooperation (among Member States), and (3) the poor level of meaningful human rights safeguards that would protect affected people from unwarranted data access. Specifically, the proposal to enable effective cooperation between Europol and private parities will favour voluntary disclosure of personal data by private companies over compelled disclosure to Member States' law enforcement authorities in accordance with national or Union law, which circumvents appropriate safeguards for fundamental rights (e.g. prior review by a court or an independent administrative authority).

Q7. Please elaborate on the necessary procedural and institutional safeguards that you consider would need to accompany such extension of Europol's mandate to exchange personal data with private parties.

4000 character(s) maximum

See answer to question 4 above

Initiation of criminal investigations and cooperation with the European Public Prosecutor Office (EPPO)

According to the current Europol Regulation (EU) 2016/794, the Agency shall support and strengthen action by the competent authorities of the Member States and their mutual cooperation in preventing and combating serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy and related crimes (Article 3). Europol's tasks include the coordination, organisation and implementation of investigative and operational actions to support and strengthen actions by the competent authorities of the Member States, which are carried out jointly with their competent authorities and the support to Member States' cross-border operations and investigations [Article 4(1)(v), (h)].

In this context, Article 6 provides for the possibility for Europol to request Member States to initiate, conduct or coordinate criminal investigations in specific cases, where cross-border cooperation would add value. The national units of the Member States shall inform Europol of their competent authorities' decision concerning such requests and, if they decide not to accede to them, they shall inform Europol of the reasons for their decision. However, the reasons may be withheld if providing them would: (a) be contrary to the essential interests of the security of the Member State concerned; or (b) jeopardise the success of an ongoing investigation or the safety of an individual.

Recent experience suggests that there are benefits to Europol supporting individual Member States' investigations in high profile cases. Europol may also have a pivotal role in triggering the initiation of criminal investigations in the context of transnational cases requiring particularly urgent and coordinated cross-border action. However, the current Europol mandate only foresees a rather light form of engagement between Europol and the Member States concerned in both such cases of Regulation (EU) 2017/1939.

Q8. Do you believe Europol is able to effectively support Member States in preventing and combating crime with its capacity under the current mandate to request the competent authorities of the Member States to initiate, conduct or coordinate a criminal investigation?

- Yes
- No
- Other

Please explain.

4000 character(s) maximum

The European Public Prosecutor Office (EPPO) Regulation (EU) 2017/1939 foresees that Europol should actively support the investigations and prosecutions of the EPPO, as well as cooperate with it, from the moment a suspected offence is reported to the EPPO until the moment it determines whether to prosecute

or otherwise dispose of the case. In addition, the Regulation recognises that the cooperation with Europol is of particular importance to avoid duplication and enable the EPPO to obtain the relevant information, as well as to draw on its analysis in specific investigations. In this context, Article 102 provides for the possibility of the EPPO to obtain, at its request, any relevant information held by Europol, concerning any offence within its competence, and to ask Europol to provide analytical support to a specific investigation conducted by the EPPO. However, Europol's current mandate does not provide for any specific role to support the investigations conducted by the EPPO in line with Regulation (EU) 2017/1939.

Q9. Do you believe that Europol's cooperation with the EPPO should be regulated in more detail, in order for the two organisations to work well together in the future?

- ○ Yes
- ◉ No
- ○ Other

Please explain.

4000 character(s) maximum

The EPPO Regulation does not foresee any role for Europol in initiating criminal investigations. It contains a mandate for cooperation with Europol that concerns the provision of information and analytical support, while the initiation of criminal investigations is to be undertaken by European Delegated Prosecutors. Proposing such a role for Europol appears to be excessive and unnecessary.

High Value Targets

According to the current Europol Regulation (EU) 2016/794, the Agency shall support and strengthen action by the competent authorities of the Member States and their mutual cooperation in preventing and combating serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy and related crimes (Article 3). In this context, Europol coordinates and actively supports EU-wide complex high profile investigations targeting individuals and organisations constituting the highest security risk to more than one Member State (so called 'High Value Targets').

Q10. Do you believe Europol is able, under the current mandate, to effectively support Member States in complex high profile investigations against individuals and organisations constituting the highest security risk to more than one Member States?

- ○ Yes
- ○ No
- ○ Other

Please explain.

4000 character(s) maximum

Preventive nature of Europol's mandate

According to Article 88 of the Treaty on the functioning of the EU, Europol's mission is to support the Member States' cooperation *in preventing and combating serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy.*

For the purpose of fulfilling its objectives, under its current mandate Europol can process personal data in order to develop an understanding of criminal phenomena and trends, to gather information about criminal networks, and to detect links between different criminal offences.

Q11. Do you see merit in Europol being able to process personal data also for the purpose of identifying /confirming the identity of the suspects, by analysing the data that clearly belong to suspects or have been obtained in the course of criminal procedures?

- Yes
- No
- Other

Please explain.

4000 character(s) maximum

International cooperation and exchange of personal data

According to the existing rules, Europol can exchange personal data with third countries and international organisations, when such exchanges are needed to perform its tasks.

As per general rules, these exchanges can take place only if (1) the Commission has adopted a decision, finding that the third country ensures an adequate level of protection of personal data ('adequacy decision'); (2) an international agreement has been concluded between the Union and that third country, adducing adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals; (3) a cooperation agreement allowing for the exchange of personal data was concluded between Europol and that third country before 1 May 2017, based on Europol's old legal framework (Article 23 of Decision 2009/371/JHA).

Q12. Do you consider it important that Europol is able to establish operational cooperation with partners like third countries in a more flexible way, without prejudice to the need to ensure data protection safeguards?

- Yes
- No
- Other

Please explain.

4000 character(s) maximum

After the entry into force of the General Data Protection Regulation and the Police Directive, it is crucial that transfers to third countries and international organisations can only take place on the basis of adequacy or a binding agreement providing adequate safeguards. A binding agreement will ensure legal certainty as well as full accountability of Europol for the transfer and should always be a requirement for structural and repetitive transfer of personal data. In any event of a data transfer, appropriate safeguards should exist to ensure that individuals' rights are enforceable and effective legal remedies are available following the transfer.

According to Europol's programming document 2020-2022, priority agreements on the transfer of personal data between Europol and Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia and Turkey are currently negotiated. All these countries have very poor records in terms of democratic standards, the rule of law and the respect of human rights, especially human rights abuses committed by law enforcement authorities and national security services. Up to now, some of them do not have any legally binding data protection instrument in place or have only moderate data protection regimes (source: https://www.dlapiperdataprotection.com/). In addition to loosening Europol's conditions for transferring data to third countries, these agreements risk undermining the quality of the protection of the personal data of European data subjects.

Q13. In your experience, do you think that the rules currently in place allow Europol to efficiently establish cooperative relations with third countries?

- Yes
- No
- Other

Please explain.

4000 character(s) maximum

Q14. Please elaborate on necessary procedural and institutional safeguards that you consider would need to accompany the flexibility referred above.

4000 character(s) maximum

A binding agreement is always preferrable for structural and repetitive transfer of personal data. In any event of a data transfer, appropriate safeguards should exist to ensure that individuals' rights are enforceable and effective legal remedies are available following the transfer.

Q15. Directive (EU) 2016/680 ('Police Directive') includes the possibility for National Authorities to perform an assessment of the data protection conditions existing in the third country before personal data are transferred, in the context of an ongoing investigation (Article 37). The provision is reflected in Article 58 of Eurojust legal basis, Regulation (EU) 1727/2018. According to this provision, in the absence of any other appropriate instrument, Eurojust can transfer personal data to a third country if, after having assessed all the circumstances surrounding the transfer of operational personal data, the Agency concludes that appropriate safeguards exist with regard to the protection of operational personal data.

Do you think that Europol should be given this possibility?

- ○ Yes
- ◉ No
- ○ Other

Please explain.

4000 character(s) maximum

The idea that Europol would be competent to assess by itself that the level of protection of personal data in a third country is adequate in order to permit transfers is incompatible with current law. This task should remain within the remit of the Commission's and the European Data Protection Supervisor's mandates.

Legal regime applicable to Europol operational data

With regard to data protection safeguards, Europol applies two different regimes. Regulation 2018/1725 applies to administrative personal data (such as staff personal data), while specific rules as reflected in the Europol regulation apply to operational data. With the entry into application of Regulation 2018/1725, the legislator aimed at ensuring consistency in data protection safeguards across the EU bodies, including Justice and Home Affairs agencies. Accordingly, Chapter IX of the abovementioned Regulation contains specific rules on the processing of operational personal data by Union bodies, when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V TFEU, such as prevention, detection, investigation, and prosecution of criminal offences. These rules apply to Frontex and to Eurojust, but do not apply yet to Europol. According to Article 98 of Regulation 2018/1725, this divergence should be addressed in the context of any amendment to Regulation (EU) 2016/794 following a report to be issued by 30 April 2022.

Q16. Do you think that Europol's data protection safeguards relating to operational data should be aligned with Chapter IX of Regulation (EU) 2018/1725?

- ◉ Yes
- ○ No
- ○ Other

Please explain.

4000 character(s) maximum

If the aim is to increase the level of data protection at Europol, in particular with regard to data subjects' rights, changes to the data protection regime would be welcome. Any such action should take special consideration of the processing of biometric data by Europol. This is not specifically mentioned in the current Regulation but, as a special category of personal data, requires particular consideration and a higher level of protection than other categories of personal data.

Contributing to the Schengen Information System

Europol can currently only access alerts in the Schengen Information System as the most widely used EU law enforcement database, without being able to feed the system with information Europol holds, in particular the information that the Agency receives from third countries. This limits the capacity of the Agency to promptly share with Member States the results of its analysis of data it has received from third

countries. This has an impact in areas such as terrorism or child sexual abuse, where crucial information is often received from third countries.

Q17. Do you think that Europol should be able to create alerts in the Schengen Information System?

- ○ Yes
- ◉ No
- ○ Other

Please explain.

4000 character(s) maximum

Giving the agency a role in entering data received from third countries into the SIS, may amount to 'data laundering' if that data is received from countries that cannot guarantee a sufficient level of rights protection.

Q18. Please elaborate on necessary procedural and institutional rules and safeguards that you consider would need to accompany the extension of Europol's mandate referred above.

4000 character(s) maximum

Data from states that do not ensure a high level of fundamental rights protection should not be entered in EU systems that enable Member States to take action on the basis of such data.

Link with the Prüm framework

The Prüm framework allows for the exchange of information between national authorities responsible for the prevention and investigation of criminal offences, with Member States granting one another, on a mutual basis, access rights to their automated DNA analysis files, automated dactyloscopic identification systems and vehicle registration data. Europol is currently not part of the Prüm framework.

Q19. Do you think that Europol should be connected to the Prüm framework for decentralised information exchange?

- ○ Yes
- ◉ No
- ○ Other

Please explain.

4000 character(s) maximum

Before any Europol integration with the Prüm framework is considered by the European Commission, Member States must address the serious data protection deficiencies in the implementation of the Prüm Decision pointed out in the study "Cross-Border Exchange and Comparison of Forensic DNA Data in the Context of the Prüm Decision", commissioned by the LIBE Committee: https://www.europarl.europa.eu /RegData/etudes/STUD/2018/604971/IPOL_STU(2018)604971_EN.pdf

Furthermore, giving the agency a role in cross-checking data received from third countries with the Prüm system, may amount to 'data laundering' if that data is received from countries that cannot guarantee a sufficient level of rights protection.

In this regard, it should be noted that Europol is already engaging in the exchange of data with operations and bodies with which it appears to have no working agreements. The 'Information Clearing House' that sits within the European Migrant Smuggling Centre "pools together military and law enforcement intelligence," and already receives data from EU naval operations and the European Gendarmerie Force (see https://www. europol.europa.eu/sites/default/files/documents/two_years_of_emsc_report.pdf, p.20), with whom Europol has neither strategic nor operational agreements; if it does, these should be made public immediately. As of December 2018, future cooperation was foreseen with the European Asylum Support Office, the European Maritime Safety Agency, the International Criminal Court, the EU Satellite Centre, the International Organization for Migration, the UN High Commissioner for Refugees and "possibly Eurojust" (see https://data. consilium.europa.eu/doc/document/ST-15250-2018-INIT/en/pdf). With the exception of Eurojust, Europol has no formal cooperation agreement with any of these bodies. This further underlines the need for a thorough, independent evaluation of Europol's current operations and activities.

Q20. Please elaborate on necessary procedural and institutional rules and safeguards that you consider would need to accompany the extension of Europol's mandate referred above.

4000 character(s) maximum

Data from states that do not ensure a high level of fundamental rights protection should not be entered in EU systems that enable Member States to take action on the basis of such data.

Research & innovation

Europol's current legal mandate does not foresee an explicit role in research and innovation. However, new technological developments offer opportunities – as well as challenges – to internal security. Innovation of cutting-edge products are therefore considered important to ensure a high level of security in future.

Q21. Do you think there is a need for Europol to step up its support to Member States on research and innovation?

- ○ Yes
- ○ No
- ◉ Other

Please explain.

4000 character(s) maximum

Allowing Europol to step up its support to Member States on research and innovation presumably refers to the “innovation lab” that is already in the works at Europol. It should be noted that the Regulation provides no legal basis for Europol to have a role in research and innovation activities. This proposal would therefore provide a legal footing for activities that have already begun. Again, a thorough, independent evaluation of those tasks is necessary in order to determine their necessity and proportionality and to permit a broad democratic debate.

In addition, predictive policing and police surveillance boosted by Big Data technologies are on the rise in Europe. We observe that the market for surveillance and social control technologies is booming and that public-private partnerships multiply in this field (e.g. Thales and the "Safe City" experimentation project in Nice, France). Common characteristics of these projects are the opacity, lack of accountability and public scrutiny and strong indicators of discrimination.

Before Europol becomes involved in research and development undertakings of new surveillance technologies, national competent authorities and governments should first bring transparency to the origin and structure of current and future research funding and to the close links between the security, governmental and research sectors. When governments enter into research and development agreements with other public or private sector entities, they must be based on law, and the existence of these agreements and information necessary to assess their impact on privacy and human rights must be publicly disclosed – in writing. Lastly, they should include strong accountability protections and safeguards, such as effective oversight by appropriate independent bodies, to prevent abuse.

This is the end of the questionnaire. Thank you for your contribution.

Please use the box below for any additional comments. Documents or position papers may also be uploaded in the section below.

4000 character(s) maximum

Please upload your file

The maximum file size is 1 MB

8b94278e-ee56-4cdf-abdf-189a8ed8dcae/EDRiResponseEuropolRegulation.pdf

Contact

HOME-POLICE@ec.europa.eu