EUROPEAN
COMMISSION

Brussels, 9.12.2020
SWD(2020) 543 final

PART 2/2

COMMISSION STAFF WORKING DOCUMENT

IMPACT ASSESSMENT REPORT

Accompanying the document

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation

{COM(2020) 796 final} - {SEC(2020) 545 final} - {SWD(2020) 544 final}

ANNEXES 1 – 11
to the Draft Europol Impact Assessment

Annex 1: Procedural information

1. LEAD DG, DECIDE PLANNING

The lead DG is the Directorate-General for Migration and Home Affairs (DG HOME). The agenda planning reference is PLAN/2020/6621.

2. ORGANISATION AND TIMING

The Commission Work Programme for 2020 announced a legislative initiative to "*strengthen the Europol mandate in order to reinforce operational police cooperation*".[1]

The inception impact assessment was published on 20 May 2020.[2] Within this framework, the impact assessment was subsequently prepared.

The Inter-service Group on the Security Union discussed a draft text of the impact assessment on 31 August 2020.

3. CONSULTATION OF THE RSB

On 7 September 2020, the Directorate-General for Migration and Home Affairs submitted the draft impact assessment to the Regulatory Scrutiny Board, which examined the draft impact assessment on 30 September 2020. The overall opinion of the Regulatory Scrutiny Board was negative. In response, the Directorate-General for Migration and Home Affairs submitted a revised version of the draft impact assessment to the Regulatory Scrutiny Board on 4 November 2020 that addressed all comments made by the Regulatory Scrutiny Board in the following way:

Findings of the Regulatory Scrutiny Board	**How the impact assessment has been modified in response**
(1) The report does not sufficiently explain the **context** and the current mandate of Europol.	The revised impact assessment includes a **detailed chapter setting out the context of the initiative**, based on input that was previously in the annex to the impact assessment. **Chapter 1** of the revised impact assessment sets out the: • the political context of the initiative; • the mandate and role of Europol as EU agency for law enforcement cooperation; • the legal context set by the Europol Regulation (EU) 2016/794; • the steps taken in the impact assessment to ensure full compliance with Fundamental Rights (see also below under point 2); • the link to other relevant EU initiatives that are taken into account in the impact assessment.

[1] COM(2020) 37 final (29.1.2020).
[2] The Inception Impact Assessment consultation is available here.

(2) The report does not clearly describe the **problems at stake** and does not provide sufficient evidence to support the analysis. It does not sufficiently assess the core problem, i.e. the trade-off between **personal data protection** and combatting crime.	The revised impact assessment provides a **detailed description of the key problems and their drivers** (**Chapter 2**), with supporting evidence and practical examples, based on input that we previously in the annex to the impact assessment. Given the space limitations in Commission impact assessments, the revised impact assessment therefore **focuses on the three major problems** that raise the **most important policy choices**: • lack of effective cooperation between private parties and law enforcement authorities to counter the abuse of cross-border services by criminals; • big data challenge for law enforcement authorities; • gaps in innovation and research relevant for law enforcement. Three additional aspects are considered politically relevant as they respond to calls by the co-legislators, even though they raise less of a policy choice notably due to legal constraints. They are addressed in **annexes 6, 7 and 8**: • Europol's ability to provide frontline officers with the result of the analysis of third-countries sourced information on suspects and criminals; • Europol's cooperation with third countries; • Europol's capacity to request the initiation of criminal investigations. In terms of the impact on Fundamental Rights and notably on the right to **protection of personal data**, the revised impact assessment provides for **thorough consideration of Fundamental Rights**. This is based on a detailed assessment of policy options in terms of their limitations on the exercise of Fundamental Rights (**annex 5**) that: • describes the policy options discarded at an early stage due to their serious adverse impact on Fundamental Rights; • sets out a step-by-step assessment of necessity and proportionality; • outlines the rejected policy options if a less intrusive but equally effective option is available; and • provides for a complete list of detailed safeguards for those policy options where a limitation on the exercise of Fundamental Rights is necessary, also due to the absence of a less intrusive but equally effective option. As a result, the preferred policy options are **strictly limited to what is necessary and proportionate** and include the **necessary safeguards**.

(3) The report fails to present the **policy options** clearly, how they link to the problems and what fundamental **political choices** they entail.	The revised impact assessment provides for a **detailed presentation of the policy options** (**Chapter 5**), setting out how they link to the problems identified, what fundamental policy choices they raise, and how they would have an impact on Fundamental Rights, based on input that was previously in the annex to the impact assessment. Given the space limitations in Commission impact assessments, the revised impact assessment **focuses on the policy options that address the three main problems raising the <u>most important policy choices</u>**, namely: 1) lack of effective cooperation between private parties and law enforcement authorities; 2) big data challenge for law enforcement authorities; 3) gaps in innovation and research relevant for law enforcement.
(4) The report assesses the **subsidiarity** issues insufficiently. It does not explain why the problems identified cannot be solved by co-operation at the national level.	The revised impact assessment takes **full account of subsidiarity**, based on input that was previously in the annex to the impact assessment: • the description of the **problems and their drivers** (**Chapter 2**) explains why action at national level or intergovernmental cooperation between Member States would not sufficiently address the problems, and why there is a **need for action at EU level**; • the description of the **necessity of EU action** and of the **added value of EU action** has been expanded for each of the problems identified (**Chapter 3**).

4. EVIDENCE, SOURCE AND QUALITY

The impact assessment is notably based on the stakeholder consultation (see annex 2). The Commission applied a variety of methods and forms of consultation, ranging from consultation on the Inception Impact Assessment, which sought views from all interested parties, to targeted stakeholders' consultation by way of a questionnaire, experts' interviews and targeted thematic stakeholder workshops, which focused on subject matter experts, including practitioners at national level. Taking into account the technicalities and specificities of the subject, the Commission emphasised in targeted consultations, addressing a broad range of stakeholders, at national and EU level.

In this context, the Commission also took into account the findings of the '*Study on the practice of direct exchanges of personal data between Europol and private parties'*, which was commissioned by DG HOME and developed by the contractor based on desk research and the following stakeholder consultation methods: scoping interviews, questionnaire and online survey, semi-structured interviews and an online workshop.

Annex 2: Stakeholder consultation

This annex provides a synopsis report of all stakeholder consultation activities undertaken in the context of this impact assessment.

1. CONSULTATION STRATEGY

In order to ensure that the general public interest of the EU is properly considered in the Commission's approach to strengthening Europol's mandate, the Commission regards it as a duty to conduct stakeholder consultations, and wishes to consult as widely as possible.

The aim of the consultation was for the Commission to receive relevant input from stakeholders to enable an evidence-based preparation of the future Commission initiative on a strengthened mandate for Europol and had four main objectives:

- to identify the problems the stakeholders consider should be addressed in the initiative;
- to identify the effectiveness, efficiency, relevance, coherence and EU added value of available solutions to these issues outlined above;
- to identify the roles of different actors in the actions to be taken and the level of action needed, taking into consideration the principle of subsidiarity;
- to identify the possible options to tackle the problems and the impact thereof.

To do this, the Commission services identified relevant stakeholders and consulted them throughout the development of its draft proposal. The Commission services sought views from a wide range of subject matter experts, national authorities, civil society organisations, and from members of the public on their expectations and concerns relating to enhancing Europol's capabilities in supporting Member States to effectively prevent and investigate crime.

During the consultation process, the Commission services applied a variety of methods and forms of consultation.[3] They included:

During the consultation process, the Commission services applied a variety of methods and forms of consultation.[4] They included:

- the consultation on the Inception Impact Assessment, which sought views from all interested parties;
- targeted stakeholder consultation by way of a questionnaire;
- expert interviews; and
- targeted thematic stakeholder workshops that focused on subject matter experts, including practitioners at national level. Taking into account the technicalities and

[3] It should be noted that consultation activities used served to collect information and arguments. They are not surveys, as they refer to non-representative samples of the stakeholders or the general population and thus do not allow for conclusions.

[4] It should be noted that consultation activities used served to collect information and arguments. They are not surveys, as they refer to non-representative samples of the stakeholders or the general population and thus do not allow for conclusions.

specificities of the subject, the Commission services focused on targeted consultations, addressing a broad range of stakeholders at national and EU level.

In this context, the Commission also took into account the findings of the '*Study on the practice of direct exchanges of personal data between Europol and private parties'*, which was commissioned by Commission's Directorate-General for Migration and Home Affairs and prepared by the contractor based on desk research and the following stakeholder consultation methods: scoping interviews, questionnaire and online survey, semi-structured interviews and an online workshop.

The aforementioned diversity of perspectives proved valuable in supporting the Commission to ensure that its proposal address the needs, and took account of the concerns, of a wide range of stakeholders. Moreover, it allowed the Commission to gather necessary and indispensable data, facts and views on the relevance, effectiveness, efficiency, coherence and EU added value of the proposal.

Taking into consideration the Covid-19 pandemic and the related restrictions and inability to interact with relevant stakeholders in physical settings, the consultation activities focused on applicable alternatives such as online surveys, semi-structured phone interviews, as well as meetings via video conference.

An open public consultation as part of the consultation strategy for the new legislative proposal was not carried out due to the technicalities and specificities of the initiative. Strengthening Europol's mandate is of a pure technical nature, thus broad open public consultation would not provide added value to the analysis. In this context, the Commission services focused on targeted consultations, addressing a broad range of stakeholders at national and EU level, through a variety of methods and forms of consultation, which include a questionnaire, expert interviews, targeted thematic stakeholder workshops and a study on the exchange of personal data between Europol and private parties. Nevertheless, it should be noted that despite the technical nature of the initiative and in order to achieve transparency and accountability and give any stakeholder the possibility to contribute, the Commission sought public's views through an open call (web-based) for feedback, on the basis of the Inception Impact Assessment.

An open public consultation as part of our consultation strategy for the new legislative proposal was not carried out due to the technicalities and specificities of the initiative. Strengthening Europol's mandate has a pure technical nature, thus broad open public consultation would not provide added value to the analysis. In this context, the Commission services focused on targeted consultations, addressing a broad range of stakeholders at national and EU level, through a variety of methods and forms of consultation, which include a questionnaire, expert interviews, targeted thematic stakeholder workshops and a study on the exchange of personal data between Europol and private parties. Nevertheless, it should be noted that, despite the technical nature if the initiative and in order to achieve transparency and accountability and give any stakeholder the possibility to contribute, the Commission sought public's views through an open call (web-based) for feedback, on the basis of the Inception Impact Assessment.

2. CONSULTATION ACTIVITIES

2.1. Feedback on the Inception Impact Assessment[5]

A call for feedback, seeking views from any interested stakeholders, on the basis of the Inception Impact Assessment. The consultation, sought feedback from public authorities, businesses, civil society organisations and the public, was open for response from 4 May 2020 to 09 July 2020. Participants of the consultation were able to provide online comments and submit short position papers, if they wished, to provide more background on their views.

2.2. Targeted consultation by way of a questionnaire

An online survey in the form of a questionnaire[6] made accessible to targeted stakeholders via the EUSurvey[7] tool was also held until 17 July 2020. The objective of this consultation was to receive feedback, comments and observations on the challenges that the Commission had identified for the revision of Europol's mandate. The questionnaire addressed different topics, where the respondent was able to further elaborate. The questionnaire also gave the possibility to upload documents, relevant for the consultation. Each section contained a short description of the background to the question. A 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 questionnaire consisted of 16 general and targeted questions aimed at receiving feedback on the following thematic areas:

- direct exchange of personal data between Europol and private parties;
- initiation of criminal investigations;
- High Value Targets;
- processing of data for prevention purposes;
- Europol's cooperation with partners;
- legal regime applicable to Europol operational data;
- Europol's access to the Schengen Information System and Prüm framework;
- research and innovation.

2.3. Stakeholder events

In the course of the consultation, the Commission organised three workshops that were held on 1 July, 1 September and 2 September 2020, respectively, to which representatives of the Member States were invited.

Workshop on the revision of the Europol Regulation

On 1 July 2020, the Commission organised a technical meeting on the revision of the Europol Regulation. The objective was to have an exchange of views on key elements of the planned revision, as part of a wider stakeholders' consultation. The topics of the discussion were based

[5] The Inception Impact Assessment consultation is available here. All contributions received are publically available.

[6] See annex 10 of the impact assessment.

[7] https://ec.europa.eu/eusurvey/home/welcome.

on the inception impact assessment and specifically on the identified problems, objectives and policy options. The 27 Member States, 2 Schengen associated third countries, Europol, the European Anti-Fraud Office (OLAF) and Commission Directorate-Generals participated in the workshop.

Workshop on Schengen Information System

On 1 September 2020, an online workshop on Europol and the Schengen Information System, in the context of the revision of the Europol Regulation, was organised jointly by the Units responsible for Police cooperation and information exchange, for information systems for borders, migration and security, and for counter-terrorism in the Commission's Directorate-General for Migration and Home Affairs. The objective of this technical workshop was to bring together experts from the Europol and the SIS/SIRENE communities to have an exchange of views on the operational needs for Europol to issue alerts in the Schengen Information System, as well as on possible options to enable Europol to issue such alerts.

Workshop on Europol and the European Public Prosecutors Office

On 2 September 2020, an online technical workshop on the cooperation between Europol and the European Public Prosecutors Office (EPPO), in the context of the revision of the Europol regulation, was co-organised by the Commission's Directorate-General for Migration and Home Affairs and by the Commission's Directorate-General for Justice and Consumers. The aim of the workshop was to bring together experts from the Europol community and the EPPO community to have an exchange of views on the cooperation between the EPPO and Europol, and on options to strengthen this cooperation in the context of the revision of the Europol Regulation. In this context, the workshop also involved Eurojust and the European Anti-Fraud Office (OLAF) to provide a complete picture of the relevant actors at EU level.

Law Enforcement Working Party

The Commission also made use of the Law Enforcement Working Party (LEWP)[8] meetings on 10-09-2020 and 14-10-2020 to brief Member States on its preparatory work and relevant technical deliberations, in the context of strengthening Europol's mandate, and explore Member States' views on the problems and potential solutions. Although not events dedicated to the consultation in the context of strengthening Europol's mandate, these meetings included topics in their agendas that corresponded to the problems addressed by this initiative.

2.4. Semi-structured interviews

The consultation included targeted – mainly follow-up – bilateral and multilateral semi-structured interviews with stakeholders on the basis of formalised and open-ended questions allowing for open and in depth discussions. These interviews were conducted from June to September 2020 via teleconferencing. They included in particular Europol staff, law enforcement representatives and private parties. The interviews are aimed at:

[8] Law Enforcement Working Party (LEWP) is a Council preparatory body, which handles work relating to legislative activities as well as cross-border policing and related operational issues. This includes activities related to Europol.

- gathering information related to the implementation of the current EU framework by pointing at loopholes and specific issues deserving further attention;
- deepening the understanding of the current practice;
- gathering recommendations and suggestions in order to improve Europol's capacity to support Member States in the prevention and fight against serious crime, terrorism and other forms of crime affecting an interest of the Union.

In terms of research and innovation, the structured interviews included:

- the chairperson of ECTEG - European Cybercrime Training and Education Group;
- the chairperson of ENLETS - European Network for Law Enforcement Technology Services;
- the two chairpersons of EACTDA - European Anti-Cybercrime Technology Development Association;
- the Head of the Border Security Research Observatory of Frontex;
- the (informal) lead of the Community of Users' Fight against Crime and Terrorism (CoU FCT) scoping group;
- the chairman of the Research & Development Standing Committee of ENFSI - European Network of Forensic Science Institutes.

2.5. Study on the practice of direct exchanges of personal data between Europol and private parties

The Commission also contracted an external consultant to conduct a study into the practice of direct exchanges of personal data between Europol and private parties. The work on the study took place between September 2019 and August 2020, and involved desk research, and stakeholder consultations by way of scoping interviews, targeted questionnaires, a survey, semi-structured interviews, and a workshop.

3. STAKEHOLDER PARTICIPATION

Stakeholders consulted included:

- EU institutions and agencies;
- law enforcement authorities in the Member States (e.g. police, customs);
- judicial authorities in the Member States;
- data protection authorities;
- non-governmental organisation, civil society;
- private entities.

The feedback on the Inception Impact Assessment included responses from members of the public, Member States non-governmental organisations and associations with an interest in this field.

This diversity of responses and perspectives has been valuable in assisting the Commission in drawing up its proposal and we are grateful to all who have participated in this consultation process.

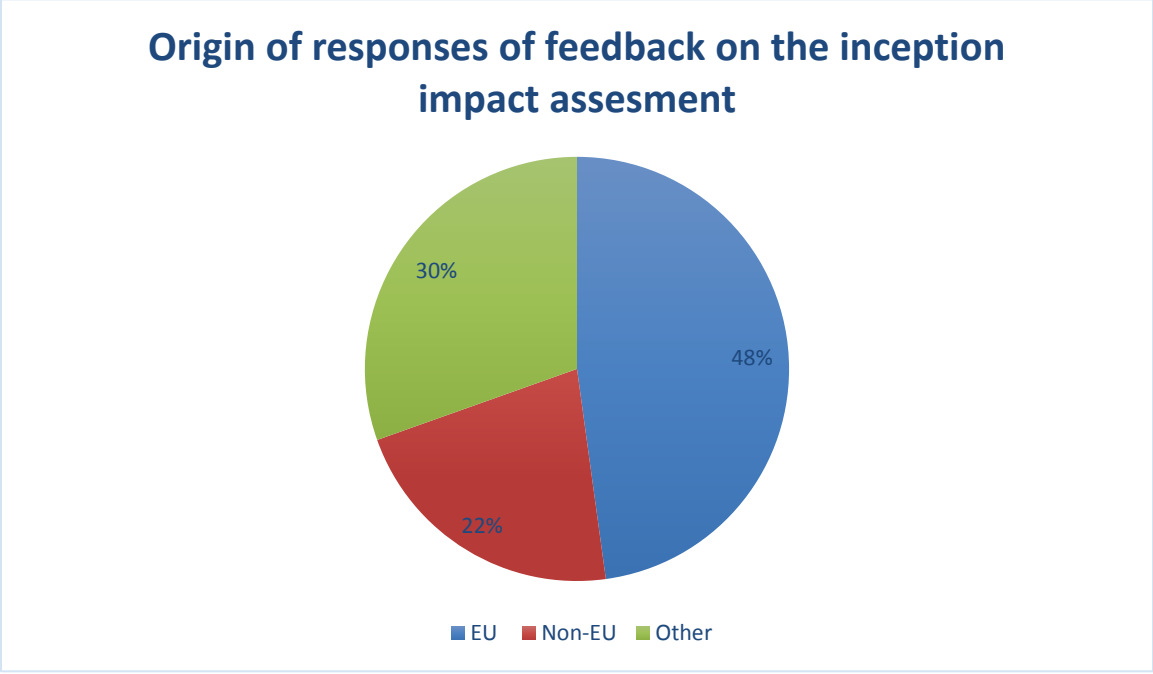
4. METHODOLOGY AND TOOLS

Given the small number of results and the high number of open questions in the survey, designed to seek detailed views from respondents, the feedback from the consultation – as with the feedback received from stakeholder events – has been processed manually. This involved reading the consultation responses in full, noting support and any issues and concerns that were raised, and feeding back on these internally as appropriate.

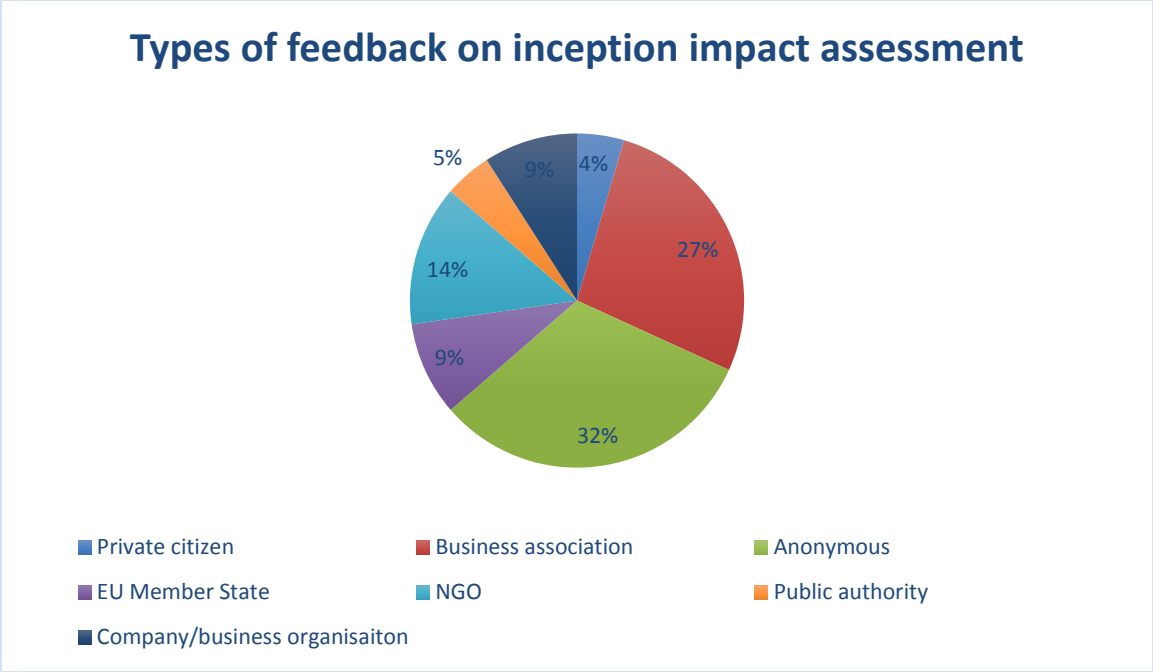
5. RESULTS

5.1. Consultation on the Inception Impact Assessment

This public consultation received 22 replies from a variety of stakeholders, ranging from members of the public and public authorities of the Member States, to business associations, private parties and non-governmental organisations. All the responses have been published in full online[9]. Of these responses, 10 came from EU states, 5 from non-EU states, 4 responses were anonymous thus could not be attributed and 3 responses did not address the subject matter.



[9] The responses are available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12387-Strengthening-of-Europol-s-mandate.



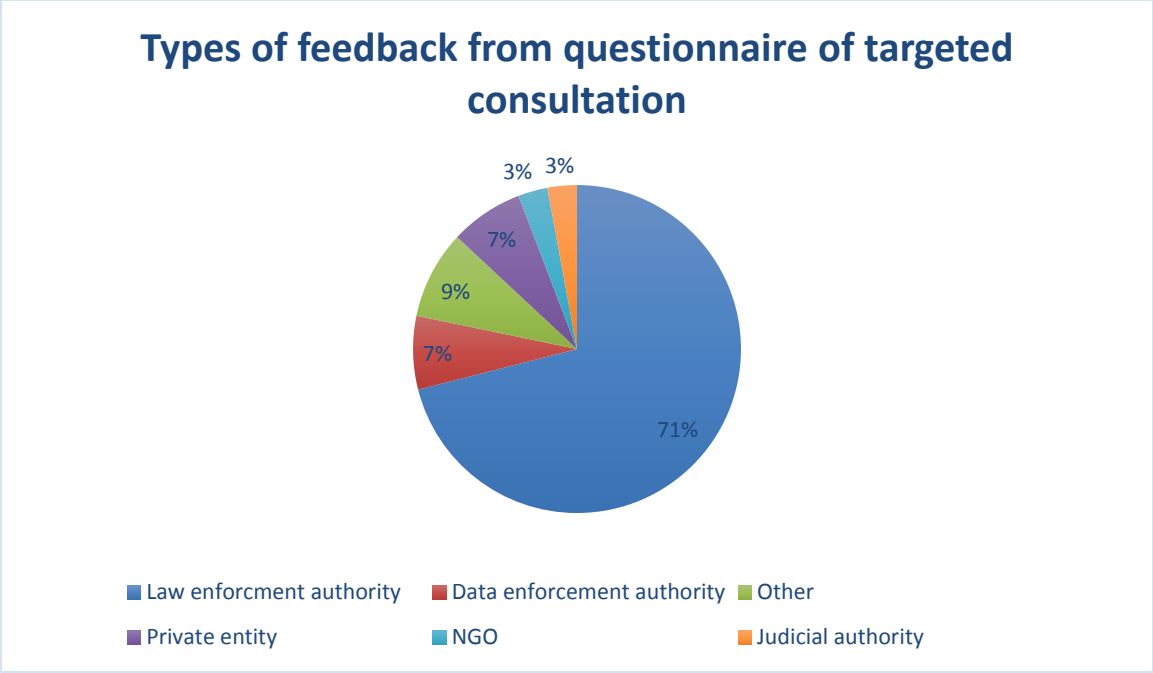
The responding NGOs said there should be increased transparency of Europol's activities and operations. Sufficient protection of fundamental rights was raised as a concern referring to cooperation with third countries. Businesses associations favour voluntary versus mandatory data disclosure under exchange of data with private parties. Safeguarding the protection of fundamental rights was also highlighted as important among business associations. Overall, the contributions recognised the importance of the work that Europol undertakes. The majority of the respondents support strengthening Europol's mandate in general and in particularly to be able to receive data from private parties. Most of the contributions from the business associations, non-governmental organisations and private parties illustrated that any transfer of data from private parties to Europol must be voluntary. Several parties referred to the continued upholding of data protection safeguards. Concerns were raised on the need to equip Europol with adequate resources and on the need to further clarify the applicable legal basis.

The responding NGOs said there should be increased transparency of Europol's activities and operations. Sufficient protection of fundamental rights was raised a concern referring to cooperation with third countries. Businesses associations favour voluntary versus mandatory data disclosure under exchange of data with private parties. Safeguarding the protection of fundamental rights was also highlighted as important among business associations. Overall, the contributions recognised the importance of the work that Europol undertakes. The majority of the respondents support strengthening Europol's mandate in general and in particularly to be able to receive data from private parties. Most of the contributions from the business associations, non-governmental organisations and private parties illustrated that any transfer of data from private parties to Europol must be voluntary. Several parties referred to the continued upholding of data protection safeguards. Concerns were raised on the need to equip Europol with adequate resources and on the need to further clarify the applicable legal basis.

5.2. Targeted consultation by way of a questionnaire

In the course of this consultation, the Commission received 71 responses. Of these, 22 Member States participated, some with more than one reply from different departments/authorities. 66 responses originated from European Union countries with 3 responses (private parties) not specifying. 70.42 % of the responses came from law enforcement authorities and 83,10% from national organisations.

In the course of this consultation, the Commission received 71 responses. of these, 21 Member States participated, some with more than one reply from different departments/authorities. 66 responses originated from European Union countries with 3 responses (private parties) not specifying. 70.42 % of the responses came from law enforcement authorities and 83.10% form national organisations.



73.24 % of the responses indicated that there is a need to strengthen Europol's legal mandate 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. Respondents said that centralised research and innovation is beneficial particularly in the identification of gaps and in coordination of technological solutions for EU law enforcement cooperation. Cyber, decryption, machine learning and IA were flagged as areas, which need to be developed, as they may be decisive for investigations.

73.24 % of the responses indicated that there is a need to strengthen Europol's legal mandate 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. Respondents said that centralised research and innovation is beneficial particularly in the identification of gaps and in coordination of technological solution for EU law enforcement cooperation. Cyber, decryption, machine learning and IA were flagged as areas, which need to be developed, as they may be decisive for investigations.

In regards to research and innovation, the consultation indicated a vast support (74, 65%) on the need for Europol to step up such support to the Member States. Participants of the survey highlighted that it is necessary to enhance Europol' s role in the identification of gaps and in coordination of the technological solutions for EU law enforcement cooperation, with regard to research and innovation. Further strengthening the legal framework of Europol to support the competent authorities of the Member States in the field of research and innovation will enable the Agency to develop innovative programs.

As regards to enabling Europol to cooperate effectively with private parties, 77.46 % of the respondents replied 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. The majority (64.79 %) of the respondents 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. The limitations under the current regime identified are: the risk of delays (e.g. where the identification of the Member State concerned is difficult and time-consuming) in 54.93 % of the responses, followed by the inability of Europol to support Member States law enforcement authorities in obtaining personal data from a private party outside their jurisdiction (52.11 % of the responses) and the risk of loss of information (e.g. where Europol does not have enough information to identify the Member State concerned), in 50.70 % of the replies. Responses also stated that Europol should be able to request and obtain data directly from private parties with the involvement of national authorities, however some Member States confronted this by taking the position that this power should remain with national authorities, as there are procedural safeguards and accountability mechanisms in place under the national jurisdiction. The survey revealed that there is a wide agreement that, in the possible future regime, it would be important the sharing of information by the private parties concerned to Europol to be in a voluntary basis (i.e. no obligation to share personal data with Europol), to be in full compliance with fundamental rights (including a fair trial) and applicable European legislation on data protection and based on a procedure of consent from the Member States (e.g. from Europol's Management Board).

Concerning the strengthening of Europol's capacity to request the initiation of cross-border investigations, respondents largely believe that Europol is able to effectively support Member States in complex high profile investigations. In addition, the replies very much supported regulating the relationship with European Public Prosecutors Office. On initiating criminal investigations, the majority of the replies illustrated that Europol is effective in supporting Member States to prevent and combat crime with its capacity under the current mandate to request the competent authorities of the Member States to initiate, conduct or coordinate criminal investigations. Some respondents referred to the benefit of a strengthened role of Europol in high value/risk cases due to its intelligence and expertise. Some respondents also queried the status of HVT at Europol and differing definition at MS level. The finite resource of Europol was also mentioned in regards to HVTs.

As to streamlining Europol's cooperation with third countries, responses to the questionnaire referred to the balance between data protection and operational cooperation and the need to assess the level of democracy of a country. Member States largely support cooperation with third countries and adequate data protection safeguards were outlined in many responses as well as having a solid legal basis for the cooperation. More specifically, on the question of if Europol should be able to establish operational cooperation with third country partners in a more flexible way, 40.85% of respondents stated yes whilst 36.62% respondent negatively. Further, 39.44% of respondents think the current rules allow Europol to efficiently establish cooperative relations with third countries whilst 18.31% disagreed. Some respondents referred to the challenges Europol faces in having cooperation with third counties with a large majority noting the need to safeguard and uphold fundamental rights. Member States recognised the need to receive data from third countries in order to deal with the evolving nature of internet-based and cross-border crime. However, respondents said that 'more flexible' way cannot be interpreted as undermining fundamental rights. Furthermore, a striking majority of responses agree that Europol's data protection safeguards relating to operational data should be aligned with Chapter IX of Regulation (EU) 2018/1725.

As to streamlining Europol's cooperation with third countries, responses to the questionnaire referred to the balance between data protection and operational cooperation and the need to assess the level of democracy of a country. Member States largely support cooperation with third countries and adequate data protection safeguards were outlined in many responses as well as having a solid legal basis for the cooperation. More specifically, on the question of if Europol should be able to establish operational cooperation with third country partners in a more flexible way, 40.85.5% of respondents stated yes whilst 36.62% respondent negatively. 39.44% of respondents think the current rules allow Europol to efficiently establish cooperative relations with third countries whilst 18.31% disagreed. Some respondents referred to the challenges Europol faces in having cooperation with third counties. A large majority referred to the need to safeguard and uphold fundamental rights. Member States recognised the need to receive data from third countries in order to deal with the evolving nature of internet-based and cross-border crime. However, respondents said that 'more flexible' way cannot be interpreted as undermining fundamental rights. Furthermore, a striking majority of responses agree that Europol's data protection safeguards relating to operational data should be aligned with Chapter IX of Regulation (EU) 2018/1725.

5.3. Workshop on the revision of the Europol Regulation

In the workshop, participants highlighted the importance of Europol being able to effectively cooperate with private parties, but also noted the importance of the data protection aspects, as also highlighted in the related Council Conclusions on this issue. In particular, any proposal for a revised mandate should take into account the necessary safeguards for different types of data, and ensure that applicable national rules for collecting such data are respected. Participants highlighted that Europol should not duplicate the investigative measures of national law enforcement and should not request data that can be easily accessed by national agencies. In addition, a distinction should be made between private parties based in the EU and provided parties based outside the EU. At least for private parties based in the EU, any request from Europol to those private parties should go through the national channels.

As regards strengthening Europol's tasks to address emerging threats, participants expressed their overall support of the innovation hub, which is of particular importance in the digital age. In addition, participants supported codifying and clarifying existing tasks to solve interpretation issues with regard to the current wording, in particular on the notion of suspects. Several concerns were expressed with regard to Europol's role in contributing to the Schengen Information System by way of the use of an existing alert category, and questions were raised mainly with regard to the role of national agencies and the need for coordination with them. Some Member States expressed their support to enabling Europol to contribute to the Schengen information System as this could solve part of the problems related to terrorist fighters, in particular to provide a solution for dealing effectively information provided by third countries in that regard.

As regards streamlining Europol's cooperation with third countries, participants recognised the operational need to exchange information with these countries, notably on specific cases, and the limitations of the current legal framework in that regard. Participants noted that data protection must be taken into account, calling for the European Data Protection Supervisor to provide its views.

As regards strengthening Europol's capacity to request the initiation of cross-border investigations, participants highlighted that there are no gaps in coordination on High Value Targets and no need to strengthen the mechanism by which Europol can request the initiation of cross border investigations. Member States were supportive to regulating the role of Europol in supporting the European Public Prosecutor Office.

5.4. Workshop on Schengen Information System

During this technical workshop, the Commission presented possible policy options and a case study. Europol also provided the Agency's view, which focused on the problem description, the potential solution, its benefits and relevant safeguards, backed by case studies illustrating the operational needs of Europol inserting alerts in the Schengen Information System. Participants highlighted the importance of the availability of information from third countries and focused on the importance of providing frontline officers with relevant, accurate and reliable data received from third countries on suspects and criminals. Participants acknowledged an existing gap in that respect. Participants raised questions in regards to legal (e.g. under whose authority would Europol issue alerts) and operational aspects (e.g. risk of overlap with Interpol alerts) related to Europol issuing alerts in the Schengen Information System, as well as the required resources and the increased workload in the Member States. Some participants were not convinced of the feasibility of Europol issuing alerts, while others considered it as an interesting option requiring further discussion. While participants opposed the idea of Europol issuing existing 'discreet check' alerts in the Schengen Information System, there was some openness to the idea of introducing a dedicated alert category exclusively for Europol.

5.5. Workshop on Europol and the European Public Prosecutors Office

During this technical workshop, the Commission's Directorate-General for Migration and Home Affairs presented possible policy options and issues for consideration. The participants provided overall positive feedback on aligning Europol's mandate with the European Public Prosecutors Office (EPPO), and clarifying and detailing their cooperation. Discussions on technical aspects

of such an intervention focused on the 'double reporting' issue (Europol and Member States are both obliged to report cases of crimes against the EU budget, so-called 'PIF crimes', to the EPPO), the handling of information provided by Europol ('data ownership principle'), the possibility of an indirect access by the EPPO to Europol's information on the basis of a hit/no hit system (similarly to Eurojust and European Anti-Fraud Office OLAF), and the administrative and logistical costs to Europol, which would derive from the enhancement of the Agency's cooperation with the EPPO.

5.6. Law Enforcement Working Party Meetings

The Commission also made use of the Law Enforcement Working Party (LEWP)[10] meetings on 10-09-2020 and 14-10-2020 to brief Member States on its preparatory work and relevant technical deliberations, in the context of strengthening Europol's mandate, and explore Member States' views on the problems and potential solutions. More specifically, Member States called to amend Europol Regulation as far as necessary to mirror the EPPO legal basis, avoiding an imbalance between the two Regulations. At the same time, they stressed that it is important to keep core principles of Europol applicable (i.e. *data ownership principle*).

In regards to Europol's cooperation with private parties, several Member States described the system of referrals as only partially suitable due to the limitations of the current system that discourages private parties from sharing data with Europol in particular on non-publicly available content and saw a benefit in Europol serving as a channel for Member States to send requests to private parties. Several delegations stressed once more the importance of a voluntary system and of involving/informing Member States as soon as possible and emphasised the importance of avoiding circumvention of national procedures. Participants also stressed that Europol should also enrich the data, when identifying the Member State concerned and underlined the importance of data protection and fundamental rights.

Concerning the possibility of a tailored-made dedicated alert category for Europol in the Schengen Information System (SIS), delegations stressed that only Member States should decide on action to be taken as a follow up and warned about the risk of changing the character of SIS by introducing a non-actionable alert category.

In regards to the big data challenge, Member States highlighted that the EDPS admonishment touches upon Europol's core business, that there is a clear need for Europol to analyse large datasets and any possible action should be taken to minimise the impact of the EDPS decision. In this context, Member States highlighted that the nature of police investigation requires large data to be stored and analysed before it can be established whether personal data falls into the categories of data subjects set out in annex II of the Europol Regulation and that they might not always have the capacity to do the analysis themselves. The importance of storage of data for court proceedings was also highlighted. Furthermore, delegations stressed that Europol must be and remain operational in digital world and be able to process large datasets. At the same time, a high level of data protection must be guaranteed.

[10] Law Enforcement Working Party (LEWP) is a Council preparatory body, which handles work relating to legislative activities as well as cross-border policing and related operational issues. This includes activities related to Europol.

In regards to the big data challenge, Member States highlighted that the EDPS admonishment touches upon Europol's core business, that there is a clear need for Europol to analyse large datasets and any possible action should be taken to minimise the impact of the EDPS decision. In this context, Member States highlighted that the nature of police investigation requires large data to be stored an analysed before it can be established whether personal data falls into the categories of data subjects set out in annex II of the Europol Regulation and that they might not always have the capacity to do the analysis themselves. The importance of storage of data for court proceedings was also highlighted. Furthermore, delegations stressed that Europol must be and remain operational in digital world and be able to process large datasets. At the same time, a high level of data protection must be guaranteed.

5.7. Semi-structured interviews

The participating representatives of the innovation and research communities expressed strong support for enhancing the role of Europol on fostering innovation and supporting the management of research relevant for law enforcement. Participants highlighted the importance of involving all Member States in this, referring to the risk that close cooperation between Europol and more advanced Member States could otherwise lead to even bigger gaps between forerunners and less advanced Member States when it comes to innovation and research relevant for law enforcement.

5.8. Study on the practice of direct exchanges of personal data between Europol and private parties

The Study[11] suggests that many stakeholders consider that the current legal framework limits Europol's ability to support Member States in effectively countering crimes prepared or committed with the help of cross-border services offered by private parties.

While the system of referrals is functioning well, the current system of proactive sharing, as regulated by the European Regulation, is not suitable to address these operational needs. Therefore, many stakeholders would see benefits in enabling Europol to exchange personal data directly with private parties, outside the context of referrals.

In addition, a number of stakeholders have recommended the channeling of the requests and the responses through a dedicated platform, and many stakeholders suggested Europol in that regard. However, some others were doubtful about the intermediary role Europol might play between the private parties and the law enforcement agencies. As an alternative solution to the issue, some stakeholders recommended the establishment of platforms for the exchanges of good practices between the law enforcement agencies.

6. HOW THE RESULTS HAVE BEEN TAKEN INTO ACCOUNT

The results of the consultation activities have been incorporated throughout the impact assessment in each of the sections in which feedback was received. The consultation activities were designed to follow the same logical sequence as the impact assessment, starting with the

[11] Study on the practice of direct exchanges of personal data between Europol and private parties. Final Report. HOME/2018/ISFP/FW/EVAL/0077.

problem definition and then moving on to possible options and their impacts. Using the same logical sequence in the consultation activities as in the impact assessment itself, facilitated the incorporation of the stakeholders' feedback – where relevant – into the different sections of the impact assessment.

Annex 3: Who is affected and how?

1. PRACTICAL IMPLICATIONS OF THE INITIATIVE

The initiative covers a range of policy options, which vary in their impact on the various stakeholders concerned. However, all policy options have the following characteristics in common:

- The initiative primarily **benefits individuals and society at large**, by improving Europol's ability to support Member States in countering crime and protecting EU citizens.
- The initiative **creates economies of scale** for administrations as it shifts the resource implications of the targeted activities from the national level to the EU level.
- The initiative **does not contain regulatory obligations for citizens/ consumers**, thus, does not create additional costs related thereto.

The different economic impacts of the preferred option on stakeholders are listed in more detail below.

Policy Option 2: allowing Europol to receive and request personal data held by private parties to establish jurisdiction, as well as to serve as a channel to transmit Member States' requests containing personal data to private parties outside their jurisdiction (regulatory intervention)

- Consumer/Citizens: Consumers will profit from improved security of the cross-border services they use and citizens as well as society at large will profit from a reduction in crime.
- National authorities: National authorities will spend additional resources on dealing with Europol own-initiative request for personal data from private parties. However this will be offset by significant savings, as national authorities will spend less resources on identifying large data sets for information relevant to their jurisdiction, because Europol will be able to perform this task for them. In addition, Member States will spend less resources on transferring requests containing personal data to private parties outside their jurisdiction, as they can use Europol as a channel to transmit such requests.
- EU bodies: Europol will spend additional resources on processing and analysing non-attributable and multi-jurisdictional data sets to establish the jurisdiction of the Member States concerned, and will invest in IT structures that will allow the Agency to act as a channel for Member States' requests to provide parties. This will lead to a reduction of costs at national level in all Member States.
- Businesses: Businesses will spend additional resources on dealing with requests from Europol, but this will be offset by significant savings. Businesses will spend less resources on identifying the relevant national jurisdictions themselves, and will be less exposed to liability risks when sharing data with Europol. Also, business will suffer less reputational damages from criminals abusing their cross-border services.

Policy option 4: clarifying the provisions on the purposes of information processing activities (regulatory intervention)

- Citizens: Direct positive impact to the security of the European citizens and societies. Europol will continue to support Member States' competent authorities as a service provider under Article 8(4) by handling data related to crimes, Europol will continue facilitating the prevention and detection of crime, by processing of data related to crime and falling into the categories of annex II. Information will be analysed with a view to establishing whether criminal acts have been committed or may be committed in the future, as well as establishing and identifying facts, suspects and circumstances regarding criminal acts.
- National authorities: Positive impact to national authorities in their daily operation. It will enhance their capabilities in preventing and investigating crime, especially taking into account that law enforcement authorities worldwide rely on information to perform their tasks, which needs to be analysed and transformed to actionable criminal intelligence that would provide direction in investigations, in the course of the 'intelligence cycle process' (direction - planning, collection, evaluation, collation, analysis, dissemination). It will facilitate identifying links between suspects and criminal activities and thus enhancing investigations. Europol will be able to continue performing existing critical activities to support national competent authorities (e.g. large data processing) and implement foreseen ones (e.g. PIU.net). It will drive to adequately interpreting the criminal environment at tactical, operational and strategic levels and achieving informed decision-making. It will positively affect resource allocation by the national competent authorities in the Member States.
- EU bodies: It entails significant benefits to Europol, as it will safeguard the status quo of Europol's daily work in supporting Member States crime preventive and investigative actions. The Agency will be in the position to effectively perform its tasks and process personal data related to crime, acting either as a service provider or as a data controller, in order to support Member States preventive activities and to assist them in developing criminal intelligence. In this context, uncertainty and challenges with regard inter alia to the processing of large data will be cleared and Europol will continue to be able to support relevant operational activities, such as digital forensics.
- Businesses: It has an indirect positive impact on businesses. The option will enhance security in the EU. Maintaining a secure environment is an important prerequisite for conducting business.

Policy option 7: enabling Europol to process personal data, including large amounts of personal data, as part of fostering innovation; Europol will participate in the management of research in areas relevant for law enforcement (regulatory intervention)

- Citizens: Europol's support to Member States in terms of fostering innovation and participating in the management of research related to law enforcement will enhance their ability to use modern technologies to counter serious crime and terrorism, including with the use of new digital tools that require the processing of personal data. This will enhance EU internal security and therefore have a positive impact on citizens. It would increase the public trust in the digital tools used by law enforcement, as the development of these tools would take place with trusted, high quality EU datasets in a controlled environment. It would reduce the dependency on third country products.
- National authorities: National authorities would benefit from Europol's support in terms of coordination and fostering of innovation processes and in the management of security research, bringing the operational needs of end-users closer to the innovation and research cycles and hence helping to ensure that new products and tools respond to the needs of law enforcement. There would be synergies and economies of scale in innovation and research relevant for law enforcement. Moreover, thanks to the training, testing and validation of algorithms, the sub-option will provide national authorities with digital tools including AI-based systems for law enforcement that they could use on the basis of national legislation, thus enhancing their capabilities to use modern technologies for fighting serious crime and terrorism.
- EU bodies: Europol would be able to support Member States in fostering innovation and participate in the management of security research. The sub-option would also enable Europol to train, test and validate algorithms for the development of digital tools including AI-based systems for law enforcement with specific requirements and safeguards. Other EU agencies in area of justice and home affairs text as well as the Commission's Joint Research Centre will benefit from the secretarial support that Europol will provide to the EU innovation hub for internal security.
- Businesses: Businesses active in the market of security products would benefit from closer links and interaction between the operational needs of law enforcement and security research, bringing the development of new products closer to the needs of end-users and hence supporting the uptake of new products.

Policy option 9: introducing a new alert category in the Schengen Information System to be used exclusively by Europol (regulatory intervention)

- Citizens: It provides frontline officers with the result of Europol's analysis of data received from third countries on suspects and criminals, when they need it and where they need it. This will enhance EU internal security and therefore have a positive impact on citizens.
- National authorities: National authorities, namely the frontline officers at the EU external border and police officers within the Schengen territory, will receive a 'hit' in the Schengen Information System when they check a person on which Europol issued an alert using a new and dedicated alert category ('information alert'). In that way,

frontline officers are made aware that Europol holds information indicating that this person intends to commit or is committing one of the offences falling under Europol's competence, or that an overall assessment of the information available to Europol gives reason to believe that the person may commit such offence in future.

- EU bodies: Europol will be able to issue a new and dedicated alert category ('information alert') in the Schengen Information System, hence providing Member States' frontline officers with the result of its analysis of data received from third countries on suspects and criminals. In case of a 'hit' in a Member State with an alert issued by Europol, the national authorities concerned inform Europol of the 'hit' and its circumstances. They might exchange supplementary information with Europol. This will increase Europol's analytical capability (e.g. to establish a picture of travel movements of the person under alert), thus enabling Europol to provide a more complete information product to Member States.
- Businesses: There will be no impact on businesses.

Policy option 11: targeted revision aligning the provision on the transfer of personal in specific situations with the Police Directive (regulatory intervention)

- Citizens: As the policy option facilitates the transfer of personal data to a third country in specific situations where this is necessary for a specific investigation of a case of serious crime or terrorism, it enhances EU internal security and therefore can have a positive impact on citizens outweighing, at least in part, the limitations on privacy.
- National authorities: As the policy option facilitates the transfer of personal data from Europol to a third country in specific situations where this is necessary for a specific investigation of a case of serious crime or terrorism, national authorities will benefit from this enhanced possibility for cooperation between Europol and third countries.
- EU bodies: The policy option facilitates the transfer of personal data from Europol to a third country in specific situations where this is necessary for a specific investigation of a case of serious crime or terrorism, thus enhancing the possibilities for Europol to cooperate with third countries.
- Businesses: There is no impact on businesses.

Policy option 12: seeking best practice and guidance (non-regulatory intervention)

- Citizens: Best practices and guidance on the application of the Europol Regulation for the cooperation with third countries might enhance that cooperation and therefore EU internal security, which would have a positive impact on citizens.
- National authorities: Best practices and guidance on the application of the Europol Regulation for the cooperation with third countries might enhance that cooperation and therefore enable Europol to better support Member States with the result of its cooperation with third countries.

- EU bodies: Best practices and guidance on the application of the Europol Regulation for the cooperation with third countries might enhance that cooperation and therefore enable Europol to better support Member States with the result of its cooperation with third countries.
- Businesses: There is no impact on businesses.

Policy option 14: enabling Europol to request the initiation of criminal investigations in cases affecting only one Member State that concern forms of crime which affect a common interest covered by a Union policy (regulatory intervention)

- Citizens: The security of the citizens will be enhanced, as the protection of common interests (e.g. the rule of law) will be enhanced and Member Sates' efforts to investigate serious organised crime and its key enablers (e.g. corruption) will be facilitated. Citizens will also built trust to the criminal justice systems of the Member States, as any doubts about the independence and quality of investigations, will be cleared up.
- National authorities: National law enforcement and judicial authorities investigating serious organised cross-border crime will benefit from Europol's enhanced capabilities and resources to provide specialised operational support and expertise. The competent authorities will also save valuable and indispensable resources.
- EU bodies: Europol enhances its role as the EU criminal information hub and a provider of agile operational support to the Member States. Europol's administrative and logistical costs will rise, as one of its tasks will practically expand in scope.
- Businesses: Business will be conducted in a secure environment. The improved fight against serious and organised crime will also help to protect the legal economy against infiltration by organised crime.

Enabling Europol to invite the EPPO to consider initiating an investigation (regulatory intervention)[12]

- Citizens: European citizens will be positively affected, as the protection of the financial interests of the Union -which reflect the financial interests of the European taxpayers- will be enhanced. The limited financial resources of the Union will be used in the best interests of EU citizens, which is not only indispensable for the legitimacy of its expenditure but as well for ensuring public trust in the Union. The European societies will also benefit from the enhancement of the protection of Union's financial interests, especially when it comes to cases concerning structural funds and the cohesion fund.

[12] This is not a policy option, but a regulatory alignment following from Council Regulation (EU) 2017/1939 (12.10.2017), which will have cost impacts on Europol (see Impact Assessment, Main Report, Section 2 Problem Definition).

- National authorities: National competent authorities in the participating Member States will benefit, as the EPPO, strongly supported by Europol, will be better equipped to fulfil its mandate, undertaking relevant investigations and to fill the enforcement gap in the participating Member States to tackle crimes against the EU budget. Without prejudice to the support provided by Eurojust, the medium to long-term relations among the EPPO and third countries and non-participating Member States can be regulated through working arrangements. In the context of Europol's support to the EPPO, the Agency could facilitate the coordination of investigations with non-participating Member States. In order to avoid action by Europol that would create a 'double reporting' situation that would result to unnecessary duplication and confusion, Europol's reporting under this option should focus on information and cases generated by its own analysis

- EU bodies: Europol and the EPPO will directly benefit, as well as –indirectly- OLAF and Eurojust. This option will provide legal certainty and clarity in Europol's role vis-à-vis the EPPO and detail the framework of their cooperation. Europol will enhance its proactive role in flagging cases of crimes against the EU budget ("PIF crimes"). Taking into consideration EPPO's prosecutorial tasks and the fact that information held by Europol are not necessarily evidence, special attention should be drawn to the appropriate handling of information submitted to the EPPO. Europol's obligation to provide information to the EPPO could include the indirect access of the EPPO to information held by Europol. Europol's administrative and logistical costs will rise. Europol, Eurojust, OLAF and the EPPO will have to coordinate their actions, avoid duplication and thus achieve economies of scale by properly allocating their resources. A comprehensive system of coordination including Eurojust and OLAF, where EU bodies and agencies will act side by side at a coordinated manner, based on their tasks and supporting each other in implementing the overarching Union objective to protect Union's financial interests will be established.

- Businesses: Private entities conducting business with the Union will benefit from the secure and trustworthy environment, as the policy will enhance EU's internal security, strengthen the protection of the Union's financial interests and enhance the trust of EU businesses in the Union's institutions, thus maintaining a secure environment. Reduced fraud, corruption and obstruction of public procurement will help to ensure a level playing field for legitimate business and will strengthen the internal market.

2. SUMMARY OF THE COSTS AND BENEFITS

The tables below summarises the costs and benefits for the **preferred options** as well as other elements of this initiative mentioned above. For some positions, the lack of available data limits the level of detail of the analysis of the costs and benefits. In order to mitigate this limitation, the tables have been filled to the maximum extent possible predominately by making use of approximation of costs and benefits calculated in other similar policies, as well as by taking advantage of assumptions and estimations drawn from experience and logic and by taking into account Europol's previous Europol programming.

As regards the **benefits in terms of savings in administrative costs** (approximately EUR 200 million over 10 years), these have been estimated in a conservative manner as a direct function of envisaged costs of the current initiative for Europol. These costs are estimated to be at least EUR 120 million over six years, resulting in an average of EUR 20 million per year. On this basis the administrative savings for national administrations were estimated at EUR 20 million per year and EUR 200 million over 10 years.[13]

As regards the **benefits for society at large in terms of a reduction in crime** (approximately 1 000 million over 10 years), it is widely acknowledged that societal benefits of fighting and preventing crime are inherently difficult to estimate.[14] These benefits are a function of the direct and indirect costs of crime for society and are influenced by a variety of tangible and intangible costs for the victims (such as medical costs, pain, lost quality of life), offenders (such as lost productivity), or tax payers (such as costs of criminal justice system).[15] Against this background, the estimated impact of the benefits of the initiative to strengthen the Europol mandate was based on several resources, including:

- available reports on the costs of specific types of crime, such as terrorism and corruption (e.g. the costs of corruption alone are estimated to be at least EUR 200 billion per year),[16]

- studies on the total criminal proceeds in the EU, which are estimated to be at least EUR 110 billion annually,[17] and

- previous Commission impact assessments from the area of law enforcement, in particular on the e-evidence proposal, which estimated the benefits of this proposal at EUR 3 000 billion over 10 years.[18]

The chosen estimate therefore reflects – in a conservative manner - the magnitude of the effects of serious crime on society, and the potential benefits of high-impact EU level solutions on combatting and preventing crimes on a European scale.

As regards the **cost estimates**, these have been calculated in cooperation with Europol. They took into consideration the increase in workload as stakeholders make more use of Europol's services over time, as well as the time needed for Europol to absorb resources in order to avoid a situation where the agency would not be able to fully implement its EU contribution and commit appropriations in due time. Staff costs, which represent an important share of the overall costs estimates, have been estimated based on Commission average unit costs, to which was applied the correction coefficient for the Netherlands (111,5%). Where the proposed

[13] An alternative way of calculating the savings in administrative costs would be as a direct function of the costs of 27 national solutions corrected for the costs of the envisaged proposal (EUR 120-150 million over 6 years). On this basis the savings in administrative costs over 10 years would amount to more than EUR 5 billion. However, such an approach would not control for a number of important factors including the unwillingness or inability of some Member States to undertake such investments.

[14] Organised Crime and Corruption, Cost of Non-Europe Report, Wouter van Ballegooij, Thomas Zandstra, European Parliamentary Research Service, 2016.

[15] Cost of Crime: A systematic review, Nyantara Wicramasekera, Helen Elsey, Judy M. Wright, and Jenni Murray, Journal of Criminal Justice, 2018.

[16] Organised Crime and Corruption, Cost of Non-Europe Report, Wouter van Ballegooij, Thomas Zandstra, European Parliamentary Research Service, 2016.

[17] Final Report of Project OCP – Organised Crime Portfolio: From illegal markets to legitimate businesses: the portfolio of organised crime in Europe, Savona Ernesto, Michele Riccardi (Eds.), 2015.

[18] COM SWD(2018) 118 final.

measures do not entail additional costs, it is estimated that these measures can be covered by the financial and human resources already allocated to Europol in the existing MFF proposal.

The preferred options would require financial and human reinforcements compared to the resources earmarked in the Commission proposal of May 2020 for the Multiannual Financial Framework 2021-2027, which plan for a 2% yearly increase of the EU contribution to Europol. It is estimated that an additional budget of around EUR 120 to 150 million and around 150 additional posts would be needed for the overall MFF period to ensure that Europol has the necessary resources to enforce its revised mandate.

I. Overview of benefits (total of all provisions) – Preferred options (EUR million over a 10 year period)		
Description	*Amount*	*Comments*
Direct benefits		
Saving in administrative costs	200 (Total)	Main beneficiaries are public authorities in Member States and businesses. Savings are based on the following factors: *Policy Option 2: Europol to process data received directly from private parties, to request personal data held by private parties to establish jurisdiction, as well as to tasks serve as a channel to transmit Member States' requests containing personal data to private parties outside their jurisdiction (regulatory intervention)* - Reduced costs for cross-border service providers to identify the jurisdiction of the relevant law enforcement authorities concerned, in cases in which these are difficult to establish; - Reduced liability risks for service providers when sharing personal data with Europol; - Reduced costs for national law enforcement authorities, who will have to spend less resources on analysing multi-jurisdictional data sets for information relevant for their jurisdiction, because Europol is doing this for them; - Reduced cost for national law enforcement authorities to transfer requests containing personal data to private parties outside their jurisdiction by using channels set up by Europol for this purpose. *Policy option 4: clarifying the provisions on the purposes of information processing activities (regulatory intervention)* - Reduced costs for national law enforcement authorities as Europol will provide more operational support, especially in complex, large-scale

		and resource demanding investigations in the Member States, upon their request. The reduced costs cannot be established in advance. *Policy option 7: enabling Europol to process personal data, including large amounts of personal data, as part of fostering innovation; Europol will participate in the management of research in areas relevant for law enforcement (regulatory intervention)* - Reduced costs for national authorities, notably national innovation labs working on security, as they will benefit from synergies and economies of scale created by the Europol innovation lab. The reduced costs cannot be established in advance. This is mainly because the innovation and research needs in relation to internal security will depend on the development of crime and the use of technology by criminals, both of which is the result of various factors and cannot be predicted in advance. *Policy option 9: introducing a new alert category in the Schengen Information System to be used exclusively by Europol (regulatory intervention)* - There are no direct cost benefit for national authorities. Indirectly, the society as a whole will benefit from enhanced internal security (see below). *Policy option 11: targeted revision aligning the provision on the transfer of personal in specific situations with the Police Directive (regulatory intervention)* - Reduced costs for national authorities as they will benefit from Europol's cooperation with third countries. The reduced costs cannot be established in advance. This is mainly because the crime rate, and hence the workload of public authorities investing and countering those crimes that require cooperation with third countries, is the result of various factors and cannot be predicted in advance.

		Policy option 12: seeking best practice and guidance (non-regulatory intervention) - Reduced costs for national authorities as they will benefit from Europol's cooperation with third countries. The reduced costs cannot be established in advance. This is mainly because the crime rate, and hence the workload of public authorities investing and countering those crimes that require cooperation with third countries, is the result of various factors and cannot be predicted in advance. *Policy option 14: enabling Europol to request the initiation of criminal investigations in cases affecting only one Member State that concern forms of crime which affect a common interest covered by a Union policy (regulatory intervention)* - Reduced costs for national competent authorities in the Member States in investigating cases falling under this option, as they will have to spend fewer resources in activities that will be supported by Europol (e.g. criminal and forensic analysis). The reduced costs cannot be established in advance. This is mainly because the crime rate, and hence the workload of public authorities investing and countering these crimes, is the result of various factors and cannot be predicted in advance. *EPPO:*[19] *enabling Europol to invite the EPPO to consider initiating an investigation (regulatory intervention)* - Reduced costs for national authorities in the participating Member States as the EPPO, strongly supported by Europol, will undertake relevant investigations. The reduced costs cannot be established in advance. This is mainly because the crime rate, and hence the workload

[19] This is not a policy option, but a regulatory alignment following from Council Regulation (EU) 2017/1939 (12.10.2017), which will have cost impacts on Europol (see Impact Assessment, Main Report, Section 2 Problem Definition).

		of public authorities investing and countering these crimes, is the result of various factors and cannot be predicted in advance.
Indirect benefits		
Reduction of crime	1 000	Main beneficiary of reduction of crime for society at large.

II. Overview of costs – Preferred options[20]							
Policy Option	*Measures*	*Citizens/ Consumers*		*Businesses*		*Administrations*[21]	
		One-off	*Recurrent*	*One-off*	*Recurrent*	*One-off*	*Recurrent*
Policy option 2	Private parties sharing personal data proactively with Europol, Europol engaging in follow-up exchanges with private parties about missing information, Europol issuing own-initiative request to Member State of Establishment, and Europol serving as a channel for Member State's request containing personal data to a private party outside its jurisdiction	None	None	Small one-off costs for adapting internal procedures for direct exchanges with Europol	Costs of identifying the relevant personal data for Europol. However, these costs should be offset by savings, as national law enforcement authorities issue less individual requests for the data already shared with Europol.	One-off costs for Europol to modify IT systems to allow for exchanges with private parties and the subsequent processing of personal data, including an increase in bandwidth and storage capacity (~EUR 1 million).	Additional costs for Europol to maintain IT systems and increase support for operations including meetings and missions (~EUR 6 million). ~60-70 FTE for Europol to analyse additional data coming from private parties. However, these costs should be offset at the level of Member States, as national law enforcement authorities will not have to analyse this data to identify information relevant for their jurisdiction. FTEs to be scaled up in the first years of implementation, to follow expected demand growth.
Policy Option 4	clarifying the provisions on the purposes of information processing	None	None	None	None	None	Additional costs for Europol to increase support for operations including meetings and missions

[20] Figures are total estimates over the period of the next MFF 2021-2027. The number of FTEs will be scaled up in the first years of implementation, to follow expected demand growth. Staff figures are based on Europol's resource needs at the end of this period. The ranges for staff figures are based on Europol's estimates with a margin of 1-5 staff for smaller staff needs, and a margin of 1-10 staff for higher staff. The indications of FTEs correspond mostly to temporary agents, due to the specificities of the tasks (handling of personal data). A limited number of contract agents (~1-5) is included as well in the FTE estimates, for tasks related to the establishment and maintenance of IT capabilities.

[21] The costs related to Europol have been estimated on the basis of the considerations outlined in the Impact Assessment, of estimates shared by the agency, and of the agency's annual reporting on operational indicators related to their levels of activities.

	activities						(~EUR 0.1 million). ~5-15 FTE for Europol for Europol to manage, process and analyse data and maintain IT systems.
Policy Option 7	enabling Europol to process personal data, including large amounts of personal data, as part of fostering innovation; Europol will participate in the management of research in areas relevant for law enforcement	None	None	None	None	One-off costs for Europol to set up relevant IT systems including a secured data space, a repository of tools and an EU technology observatory (~EUR 2 million).	Additional costs for Europol to support Member States in implementing innovation projects including the management of the Innovation hub and the testing of innovative IT solutions in a secured environment (~EUR 13 million). ~25-35 FTE for Europol to run its innovation lab, support the EU innovation hub for internal security, and to support the management of security research.
Policy Option 9	introducing a new alert category in the Schengen Information System to be used exclusively by Europol	None	None	None	None	There will be marginal costs for Member States to update their national systems allowing their end-users to see the alerts issued by Europol, as well as to update their SIRENE workflows.[22] One-off costs for Europol to establish and adapt relevant connections with SIRENE community to be able to send	Additional costs for Europol to renew, maintain, and expand IT systems (including bandwidth and storage) in line with demand (~EUR 7 million). ~10-20 FTE for Europol to create alerts in the Schengen Information System and to provide 24/7 follow up to Member States in case of a

[22] SIRENE stands for "Supplementary Information Request at the National Entries". Each Member State operating the Schengen Information System has set up a national SIRENE Bureau, operational 24/7, that is responsible for any supplementary information exchange and coordination of activities connected to alerts.

						data in a structured way to the central component of the Schengen Information System when they issue an alert (~EUR 1 million). Costs for eu-LISA,[23] the EU agency responsible for the operational management of the Schengen Information, as it would need to update the central system to enable Europol as a new user to create alerts, as well as some elements of the SIRENE mail exchange. These costs would be below EUR 2 million.	hit. FTEs to be scaled up in the first years of implementation, to follow expansion of the new system's users. The need of 24/7 support implies necessary human resources (shift work).
Policy option 11	targeted revision aligning the provision on the transfer of personal in specific situations with the Police Directive	None	None	None	None	One-off costs for Europol to adapt IT systems to provide for secured connections with third countries (~EUR 0.4 million).	Additional costs for Europol to increase support for operations including meetings and missions (EUR 3 million). ~1-5 FTE for Europol to make use of its mechanism to exchange personal data with third countries where necessary
Policy option 12	seeking best practice and guidance	None	None	None	None	None	Additional costs for Europol to exchange best practices, organise meetings and trainings (~EUR 0.3 million).
Policy option	Europol requesting the initiation of criminal	None	None	None	None	One-off costs for Europol to modify IT systems and tools,	Additional costs for Europol to increase support for

[23] EU Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice.

14	investigations in cases affecting only one Member State that concern forms of crime which affect a common interest covered by a Union policy					including an increase in bandwidth and storage capacity (~EUR 0.5 million).	operations in individual Member States including meetings, missions and operational infrastructure (EUR 6 million). ~15-25 FTE for Europol to coordinate with the Member States and to support Member States in their investigation (incl. on-the-spot-support, access to criminal databases and analytical tools, operational analysis, forensic and technical expertise)
EPPO[24]	Europol requesting the EPPO to consider initiating an investigation in line with its mandate, in full respect of the independence of the EPPO, and Europol actively supporting the investigations and prosecutions of the EPPO (e.g. report suspected PIF cases, provide any relevant information requested by the EPPO, provide on-the-spot-support, access to criminal databases and	None	None	None	None	None	Additional costs for Europol to increase support for investigations of the EPPO including meetings, missions and operational infrastructure (EUR 1 million). ~5-15 FTE Europol to coordinate with EPPO and to actively support EPPO in its investigations and prosecutions. This includes reporting suspected PIF cases, providing relevant information requested by the EPPO, providing on-the-spot-support, access to criminal databases and analytical tools, operational

[24] This is not a policy option, but a regulatory alignment following from Council Regulation (EU) 2017/1939 (12.10.2017), which will have cost impacts on Europol (see Impact Assessment, Main Report, Section 2 Problem Definition).

	analytical tools, operational analysis, forensic and technical expertise, specialised training)						analysis, forensic and technical expertise and specialised training). FTEs to be scaled up in the first years of implementation, as the volume of EPPO investigations and prosecutions increases.

Annex 4: Past performance of Regulation (EU) 2016/794

1. INTRODUCTION

Europol, the European Union Agency for Law Enforcement Cooperation, operates on the basis of Regulation (EU) 2016/794.[25] Europol's mission is 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, fulfilling its Treaty-based objective set out in Article 88(1) TFEU. Regulation (EU) 2016/794 entered into force on 13 June 2016 and took effect in all EU Member States 1 May 2017. On 31 December 2019, the total number of staff employed by Europol was 756: 549 staff in Establishment Plan (TA posts) and 207 Contract Agents. The number of non-Europol staff (Seconded Experts, Liaison Officers and staff of Liaison Bureaus, Trainees and Contractors) was 543. Europol's budget in 2019 was EUR 138.3 million.

This technical annex provides an assessment of the application of Regulation (EU) 2016/794, highlighting its achievements and identifying areas that require improvement.

Europol was set up by Council Decision 2009/371/JHA[26] as an entity of the Union funded from the general budget of the Union. Decision 2009/371/JHA replaced the Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention).

Regulation (EU) 2016/794 amended and expanded the provisions of Decision 2009/371/JHA and of Council Decisions 2009/934/JHA,[27] 2009/935/JHA,[28] 2009/936/JHA[29] and 2009/968/JHA[30] implementing Decision 2009/371/JHA. Since the amendments were of a substantial number and nature, those Decisions in the interests of clarity, were replaced in their entirety in relation to the Member States bound by Regulation (EU) 2016/794. Europol as established by Regulation (EU) 2016/794 replaced and assumed the functions of Europol as established by Decision 2009/371/JHA, which, as a consequence, was repealed.

---

25 Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA.

26 Council Decision of 6 April 2009 establishing the European Police Office (Europol) (2009/371/JHA).

27 Council Decision 2009/934/JHA of 30 November 2009 adopting the implementing rules governing Europol's relations with partners, including the exchange of personal data and classified information.

28 Council Decision 2009/935/JHA of 30 November 2009 determining the list of third States and organisations with which Europol shall conclude agreements.

29 Council Decision 2009/936/JHA of 30 November 2009 adopting the implementing rules for Europol analysis work files.

30 Council Decision 2009/968/JHA of 30 November 2009 adopting the rules on the confidentiality of Europol information.

2. PURPOSE OF REGULATION (EU) 2016/794

The Commission's 2013 legislative initiative,[31] leading to the adoption of Regulation (EU) 2016/794, had the following **general objectives**:

- making Europol a **hub for information exchange** between the law enforcement authorities of the Member States;
- granting Europol **new responsibilities**, including a possibility for Europol to develop the EU **centres of specialised expertise** for combating certain types of crime falling under Europol's objectives.

Europol was entrusted with new responsibilities following the European Council's '**Stockholm programme** — An open and secure Europe serving and protecting citizens'[32], which called for Europol to evolve and become a hub for information exchange between the law enforcement authorities of the Member States, a service provider and a platform for law enforcement services. On the basis of an assessment of Europol's functioning, further enhancement of its operational effectiveness was needed to meet that objective. Furthermore, available threat assessments showed that criminal groups were becoming increasingly poly-criminal and cross-border in their activities. National law enforcement authorities therefore needed to cooperate more closely with their counterparts in other Member States. In this context, it was necessary to equip Europol to better support Member States in Union-wide crime prevention, analyses and investigations. This was also confirmed in an evaluation of Decision 2009/371/JHA.

Regulation (EU) 2016/794 pursues the following **specific objectives** that will be assessed in this technical annex:

- Europol should be a **hub for information exchange** in the Union. Information collected, stored, processed, analysed and exchanged by Europol includes **criminal intelligence** which relates to information about crime or criminal activities falling within the scope of Europol's objectives, obtained with a view to establishing whether concrete criminal acts have been committed or may be committed in the future.[33]
- Europol should **increase the level of its support** to Member States, so as to enhance mutual cooperation and the sharing of information.[34]
- To improve Europol's effectiveness in **providing accurate crime analyses** to the competent authorities of the Member States, it should use new technologies to process data. Europol should be able to **swiftly detect links between investigations** and common *modi operandi* across different criminal groups, to **check cross-matches of data** and to have a clear overview of trends, while guaranteeing a high level of protection of personal data for individuals. Therefore, Europol databases should be structured in such a way as to allow Europol to choose the most efficient IT structure. [35]
- Europol should also be able to **act as a service provider**, in particular by providing a

31 COM(2013) 173 final (27.3.2013).
32 Official Journal of the European Union, 2010/C 115/01.
33 Recital 12 of Regulation (EU) 2016/794.
34 Recital 13 of Regulation (EU) 2016/794.
35 Recital 24 of Regulation (EU) 2016/794.

secure network for the exchange of data, such as the secure information exchange network application (SIENA), aimed at facilitating the exchange of information between Member States, Europol, other Union bodies, third countries and international organisations. In order to ensure a high level of data protection, the purpose of processing operations and access rights as well as specific additional safeguards should be laid down. In particular, the principles of necessity and proportionality should be observed with regard to the processing of personal data.[36]

- Serious crime and terrorism often have links beyond the territory of the Union. Europol should therefore be able to **exchange personal data with authorities of third countries** and with international organisations such as the International Criminal Police Organisation – Interpol to the extent necessary for the accomplishment of its tasks.[37]

3. OVERALL ASSESSMENT AND ACHIEVEMENTS IDENTIFIED

Overall, the application of Regulation (EU) 2016/794 can be considered a success, at it allowed the agency to support Member States' law enforcement authorities in countering serious crime and terrorism. Indeed, the Management Board of Europol, bringing together representatives of the Member States and the Commission to effectively supervise the work of the agency, notes that "*'users' satisfaction with Europol's products and services and with how Europol's work contributed to achieve operational outcomes, is very high (…), thereby confirming the continued trust of Member States in Europol's ability to support their action in preventing and combating serious organised crime and terrorism*".[38]

The stakeholder consultation[39] carried out in the preparation of the impact assessment also showed a very high level of satisfaction with the services provided by Europol. This success manifests itself in the quantitative data set out below on the operational activities of Europol in support of national law enforcement authorities.

---

36 Recital 24 of Regulation (EU) 2016/794.

37 Recital 32 of Regulation (EU) 2016/794.

38 Europol: 2019 Consolidated Annual Activity Report (9.6.2020). The Consolidated Annual Activity Report (CAAR) 2019 covers the period from 1 January to 31 December 2019 and presents the progress made to achieve the objectives deriving from the Europol's 2020+ Strategy and the 2019 Annual Work Programme. The CAAR 2019 was submitted on behalf of the Executive Director of Europol to the Management Board for adoption, in accordance with article 16 (5)(g) of Regulation (EU) 2016/794 and Article 48 of the Financial Regulation applicable to Europol. According to Article 11 (1)(c) of Regulation (EU) 2016/794, this report was adopted by the Management Board on 9 June 2020 and submitted to the European Parliament, the Council, the Commission, the Court of Auditors and the national parliaments by 1 July 2020.

39 See Annex 11 on the stakeholder consultation. The Commission sought views from a wide range of subject matter experts, national authorities, civil society organisations, and from members of the public on their expectations and concerns relating to the objective of enhancing Europol's capabilities in supporting Member States to effectively prevent and investigate crime. The Commission applied a variety of methods and forms of consultations, ranging from: (1) consultations on the Inception Impact Assessment, which sought views from all interested parties, to (2) targeted stakeholders' consultations by way of a questionnaire, (4) expert interviews and (4) targeted thematic stakeholder workshops, which focused on subject matter experts, including practitioners at national level. Taking into account the technicalities and specificities of the subject, the Commission focused on targeted consultations, addressing a broad range of stakeholders at national and EU level.

However, 73.24 % of the responses in the targeted consultation questionnaire (see annex 11 of the impact assessment) indicated that there is a need to strengthen Europol's legal mandate 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. Moreover, in two areas set out below in this technical annex, Regulation (EU) 2016/794 did not meet its objectives, and these shortcomings call for improvement (see section 4 below for more details). First, Regulation (EU) 2016/794 does not provide the necessary legal clarity on the processing of personal data by Europol to enable the agency to meet its objectives and fulfil its tasks in relation to three specific problems identified in section 4.1 below. Second, Regulation (EU) 2016/794 has led to uncertainties around the use of mechanisms to exchange personal data with third countries, as set out in detail in section 4.2 below.

In the context of assessing the application of Regulation (EU) 2016/794, it should be noted that the Commission acknowledged the need that the Europol Regulation should be revised before the evaluation of the impact, effectiveness and efficiency of the Agency and its working practices due for May 2022 (as foreseen in Europol Regulation). This was deemed necessary to provide Europol with the means to face the evolving nature crimes committed on or by means of the internet and financial crimes; to align the procedures establishing cooperation with third countries with other Agencies and to align the data protection provisions with Regulation 2018/1725. It was also taken into account that a number of stakeholders (Member States and Europol) acknowledged the need to revise key elements of the current legal base, without awaiting the outcomes of the envisaged evaluation. Besides, aligning the Europol Regulation to the law enforcement most recent needs and challenges, in order to allow the Agency to fully implement its mandate, has an inherent EU added value.

3.1. Europol as hub for information exchange

Regulation (EU) 2016/794 enabled Europol to become a hub for information exchange in the Union. Since the Regulation took effect, and as a result of the new capabilities that the Regulation gave to the agency, Europol saw a significant increase both in:

- the information exchanged between Member States using the agency's Secure Information Exchange Network Application (SIENA);
- the data provided to the Europol Information System, the agency's central criminal information and intelligence database, and the number of searches.

	2016[40]	**2019**[41]
number of SIENA messages exchanged	869.858	1.242.403
number of SIENA cases initiated	46.437	84.697
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

[40] All 2016 statistics can be found in: Europol: 2016 Consolidated Annual Activity Report (1.5.2017).
[41] All 2019 statistics can be found in: Europol: 2019 Consolidated Annual Activity Report (9.6.2020).

number of person objects in the Europol Information System	103.796	241.795
number of searched performed in the Europol Information System	1.436.838	5.356.135

3.2. Increased level of operational support by Europol

Regulation (EU) 2016/794 enabled Europol to step up its operational support to Member States' law enforcement authorities. This increased support, resulting from the new capabilities that the Regulation gave to the agency, manifests itself in the number of operational reports produced by Europol as well as in the number of operational cases in the Member States to which Europol provides support. This applies to all forms of crime that fall into the scope of Europol's mandate, including the work of Europol's specialised centres.

The improved service that Europol is able to provide is also reflected in the speed of the first-line response to requests by Member States' law enforcement authorities. Moreover, there is also a notable increase in the number of mobile offices deployed in Member States to provide operational support on the ground to specific investigations.

	2016[42]	**2019**[43]
number of operational reports produced by the Operational Centre	5.222	more than 9.600
number of operational cases supported by the European Counter Terrorism Centre[44]	127	632
number of operational reports produced by the European Counter Terrorism Centre	268	1.883
number of operational cases support by the European Cybercrime Centre[45]	175	397
number of operational reports produced by the European Cybercrime Centre	2.200	1.084
number of operations supported related to serious organised crime	664	726
number of operational reports produced related to serious organised crime	1.388	4.636
number of operations supported by financial intelligence	45	205
speed of first-line response to Member States request	27.5	6.6

42 All 2016 statistics can be found in: Europol: 2016 Consolidated Annual Activity Report (1.5.2017).

43 All 2019 statistics can be found in: Europol: 2019 Consolidated Annual Activity Report (9.6.2020).

44 In January 2016 Europol created the European Counter Terrorism Centre (ECTC), an operations centre and hub of expertise that reflects the growing need for the EU to strengthen its response to terrorism.

45 Europol set up the European Cybercrime Centre (EC3) in 2013 to strengthen the law enforcement response to cybercrime in the EU

number of mobile offices deployed in Member States	221	353

4. SHORTCOMINGS IDENTIFIED THAT REQUIRE IMPROVEMENT

In two areas, Regulation (EU) 2016/794 did not meet its objectives, and these shortcomings call for improvement:

First, Regulation (EU) 2016/794 does not provide the necessary legal clarity on the processing of personal data by Europol to enable the agency to meet its objectives and fulfil its tasks in relation to three specific problems identified in section 4.1 below.

Second, Regulation (EU) 2016/794 has led to uncertainties around the use of mechanisms to exchange personal data with third countries that, in turn, seem to affect the agency's ability to support national law enforcement authorities through its cooperation with these third countries.

Moreover, due to external factors that have changed since the adoption of Regulation (EU) 2016/794, certain aspects of that Regulation no longer allow Europol to fulfil its mandate and support Member States in an effective way. This is notably due to evolving and increasingly complex security threats linked to the way in which criminals exploit the advantages brought about by the digital transformation, new technologies, globalisation and mobility.

For example, this concerns Europol's ability to cooperate with private parties (see problem I of the impact assessment)[46], or the need to foster innovation and support the management of research relevant for law enforcement (see problem II of the impact assessment).[47] However, these problems are due to the effects of external factors that were, as such, not foreseeable at the time of adoption of Regulation (EU) 2016/794.

In fact, it was not an objective of the Regulation to address these problems. For example, while the lack of cooperation between Europol and private parties raises a number of concerns[48] today, the Commission's legislative initiative leading to Regulation (EU) 2016/794 explicitly prohibited any contact from Europol towards private parties.[49] Likewise, Regulation (EU) 2016/794 stipulates that "*Europol shall not contact private parties to retrieve personal data*".[50] Consequently, the lack of sufficient cooperation between Europol and private parties cannot be attributed to Regulation (EU) 2016/794 failing to meet its objectives.

---

46 Chapter 2 of the impact assessment.

47 Chapter 2 of the impact assessment.

48 Study on the practice of direct exchanges of personal data between Europol and private parties. Final Report. HOME/2018/ISFP/FW/EVAL/0077. The Study revealed that many stakeholders consider that the current legal framework limits Europol's ability to support Member States in effectively countering crimes prepared or committed with the help of cross-border services offered by private parties. While the system of referrals is functioning well, the current system of proactive sharing, as regulated by Regulation (EU) 2016/794, is not suitable to address these operational needs. Therefore, many stakeholders would see a need to enable Europol to exchange personal data directly with private parties, outside the context of referrals.

49 COM(2013) 173 final (27.3.2013). Article 32(3) of the Commission proposal states that "*Europol shall not contact private parties directly to retrieve personal data*."

50 Article 26(9) of Regulation (EU) 2016/794.

As regards the cooperation between Europol and private parties, the Commission has commissioned a study[51] that provides an overview of the current practice of direct and indirect exchanges of personal data between Europol and private parties.

The study's main findings are the following:

- As regards the system of referrals and responses to referrals, the system functions well and it is well-documented. However, online service providers and Europol would both see benefits in exchanging personal data directly, outside the context of referrals.
- As regards Europol receiving personal data from private parties via an intermediary, typically national law enforcement authorities, the study finds that this system is commonly used. However, only a fraction of personal data from the private parties reaches Europol. Therefore, it is recommended to reinforce Europol's capacity to exchange personal data directly with private parties.
- As regards private parties sharing personal data directly with Europol outside the context of referrals, the study concludes that the system of resubmission via national authorities is rarely used, as it is perceived to be complex, complicated and slow. Its rare use results in missed opportunities. Therefore, it is recommended to reconsider the provisions of the Europol Regulation to allow for direct exchanges of personal data with private parties, and to empower Europol with a more extensive data processing mandate.
- As regards national law enforcement authorities sharing personal data with private parties via Europol, the study proved that national law enforcement authorities often require access to personal data held by private parties during their investigations, but might face obstacles when trying to obtain personal data from private parties. Channeling requests from law enforcement authorities to private parties through a dedicated platform such as Europol was one of the solutions recommended by the stakeholders.

4.1. Lack of clarity on Europol's information processing activities

Europol's legal basis needs to provide legal certainty for the agency to perform its tasks in support of Member States. However, there is a **lack of clarity** in Regulation (EU) 2016/794 when it comes to the agency's **information processing activities**. Europol's legal basis limits the processing of personal data by Europol to data related to **specific categories of data subjects** listed in annex II of the Regulation (i.e. persons related to a crime for which Europol is competent).[52] However, the Regulation does not set out how Europol can comply with this requirement when processing personal data to meet its objectives and fulfil its tasks in relation to three aspects set out below.

The supervision of Europol's data processing activities by the European Data Protection

[51] Milieu, Study on the practice of direct exchanges of personal data between Europol and private parties, Final Report, HOME/2018/ISFP/FW/EVAL/0077, September 2020 (not yet published).

[52] Article 18(5) of Regulation (EU) 2016/794 (11.5.2016) limits the processing of personal data by Europol to the categories of data subjects listed in annex II of that Regulation. The categories of data subjects cover: (1) suspects, (2) convicted persons, (3) persons regarding whom there are factual indications or reasonable grounds to believe that they will commit, (4) persons who might be called on to testify in investigations or in subsequent criminal proceedings, (5) victims, (6) contacts and associates of a criminal, and (7) persons who can provide information on a crime.

Supervisor has shed light on the lack of clarity in Europol's legal basis as regards the agency's information processing activities. In December 2019, the European Data Protection Supervisor found that the embedment of FIU.net[53] into Europol's systems breached the provisions governing the processing of personal data, inter alia due to the restrictions of Regulation (EU) 2016/794 on the categories of individuals about whom Europol can process personal data.[54] In that respect, the EDPS decision revealed an inconsistency between the safeguards on categories on data subjects set out in Regulation (EU) 2016/794 on the one hand, and situations where Europol acts as a service provider to Member States regarding their bilateral exchanges of data on crimes on the other.[55] In the latter case, Europol does not have access to the personal data exchange, and therefore cannot ensure that the processing of personal data is limited to data related to specific categories of data subjects. Beyond that, the lack of clarity that the EDPS decision highlights as regards the requirement related to the specific categories of data subjects in annex II of Regulation (EU) 2016/794 may also apply to other – and more essential – aspects of data processing by Europol.

Indeed, the Regulation (EU) 2016/794 does not set out how the agency can comply with the requirement related to the specific categories of data subjects when processing personal data to meet its objectives and fulfil its tasks with regard to:

1) Europol's ability to act **as a service provider** for crime-related bilateral exchanges between Member States using Europol's infrastructure:[56] In these cases, Europol does not have access to the personal data exchanged between Member States through Europol's infrastructure and can therefore not ensure compliance with the requirement related to the specific categories of data subjects.
2) Europol's ability to **process personal data it received from Member States** for the purposes of cross-checking[57] or operational analysis[58] in the context of preventing and combating crimes that fall under Europol's mandate: When Member States submit personal data to Europol for cross-checking or operational analysis, they usually do not indicate the categories of data subjects under which the data falls. Moreover, it is not always clear from the outset if a person (to whom the data transmitted by a Member State relate) is related to a crime for which Europol is competent. Consequently, Europol cannot verify if the data submitted by Member States for further processing by the agency falls within the categories of data it is allowed to process, including for prevention and criminal intelligence.

---

53 FIU.net is a decentralised and sophisticated computer network supporting the Financial Intelligence Units (FIUs) in the European Union in their fight against money laundering and the financing of terrorism

54 EDPS Opinion 5/2020 on the European Commission's action plan for a comprehensive Union policy on preventing money laundering and terrorism financing (23.7.2020). In its related decision, the EDPS addressed the question whether Europol could act as the technical administrator of this network, considering the restrictions outlined in Regulation (EU) 2016/794 on the categories of individuals about whom Europol can process personal data (see EDPS Annual Report 2019).

55 According to Article 8(4) of Regulation (EU) 2016/794 (11.5.2016), Member States may use Europol's infrastructure for exchanges also covering crimes falling outside the scope of the objectives of Europol. In these cases, Europol acts as data processor rather than as data controller, i.e. it does not have access to the personal data exchanged between Member States through Europol's infrastructure.

56 Article 8(4) of Regulation (EU) 2016/794.

57 Article 18(2)(a) of Regulation (EU) 2016/794 (11.5.2016).

58 Article 18(2)(c) of Regulation (EU) 2016/794 (11.5.2016).

3) The aforementioned problem affects in particular Europol's ability to support Member States with operational analysis for criminal investigations that require the **processing of high volumes of data**. [59]

This **lack of clarity on Europol's information processing activities** risks limiting Europol's ability to provide sufficient support to Member States. The **regulatory failures** in Regulation (EU) 2016/794 are twofold:

1) The mandate given to Europol to support Member States as service provider[60] is not fully reflected in the provisions on the purposes of information processing activities. This applies in particular to the obligation imposed on Europol to limit its data processing to personal data that relate to specific categories of data subjects listed in annex II of Regulation (EU) 2016/794, which refer to the crimes that fall under Europol's mandate.
2) Regulation (EU) 2016/794 remains ambiguous as to how Europol can ensure its processing of personal data is limited to personal data that falls into one of the categories of data subjects listed in annex II of that Regulation. Compliance with this safeguard would require Europol to undertake an initial processing of personal data submitted by Member States with the sole purpose of determining whether such data falls into the specific categories of data subjects listed in annex II. Such verification would require cross-checking with data already held by Europol. When it comes to high volumes of personal data received by Europol in specific investigations[61], such initial data processing for the sole purpose of verification may be time-consuming and may require the use of technology. However, Regulation (EU) 2016/794 does not provide for such initial data processing. In fact, Regulation (EU) 2016/794 does not set out any specific procedure which would enable Europol to verify if personal data submitted by Member States falls under the specific categories of data subjects in annex II.

Consequently, Regulation (EU) 2016/794 has not met its objectives in that respect.

4.2. Uncertainties around the use of mechanisms to exchange personal data with third countries

Since the entry into application of Regulation (EU) 2016/794 in 2017, and hence of the legal grounds it provides for Europol to enter into an structural cooperation with third countries and transfer personal data, related efforts have not progressed at the desired pace[62] and have not yet

---

59 For example, Europol received an unprecedented volume of data in the context of the Task Force *Fraternité* that was set up to support French and Belgian authorities in the investigation of the November 2015 Paris attacks and the March 2016 Brussels attacks. The aim was to investigate further international connections of the terrorists involved in those attacks by analysing communication, financial, internet and forensic records. Task Force *Fraternité* analysed 19 terabyte of information. Europol's processing of this high volume of data resulted in 799 intelligence leads.

60 Article 8(4) of Regulation (EU) 2016/794.

61 Data collected in serious and organised crime and terrorist investigations increase in size and become more complex. They require the processing of high volumes of data involving sometimes terabytes of data, including audio, video and machine-generated data that is increasingly complex to process.

62 See the Seventeenth Progress Report towards an effective and genuine Security Union (COM(2018) 845 final (11.12.2018).

led to tangible results in terms of establishing such cooperation:[63]

1) The Commission has not adopted yet any **adequacy decision** in accordance with the Data Protection Law Enforcement Directive that would allow for the free transfer of personal data to a third country.
2) Due to various reasons, following the adoption by the Council of eight mandates[64] in June 2018 for the Commission to negotiate **international agreements** with priority third countries on strengthening the cooperation with Europol, the subsequent efforts by the Commission have not yet led to conclusion of such agreements. While negotiations have led to considerable progress with one key foreign partner, political reasons in one country (repeated elections) have prevented such progress in another case. For the remaining cases, the third countries have not shown an interest in entering into such negotiations. So although the Council and the Commission consider it necessary to establish a structural cooperation between Europol and these eight priority countries, it has not yet been possible to achieve this. On the other hand, as regards the mandate the Commission received in 2020 to open negotiations with New Zealand, informal discussions have started with good prospects.
3) The possibility to transfer personal data based on a **self-assessment of the adequate level of safeguards** and an authorisation by the Europol Management Board, in agreement with the EDPS, has not been applied in practice. In one case, preparatory steps have been taken for such an authorisation. This case seems to indicate that there are uncertainties around the conditions under which such transfer mechanism can be used.

As regards the possibility[65] to transfer personal data in specific situations on a case-by-case basis, the Europol Executive Director made use of this **derogation** in two case, including in the cooperation with New Zealand in the follow up to the March 2019 Christchurch attack.

Consequently, and besides the cooperation that takes place on the basis of cooperation agreements[66] concluded before the entry into application of Regulation (EU) 2016/794, uncertainties around the use of mechanisms to exchange personal data with third countries seem to affect the agency's ability to support national law enforcement authorities through its cooperation with these third countries. In that respect, Regulation (EU) 2016/794 has not met its objectives.

---

63 Regulation (EU) 2016/794 sets outs three ways to establish a structural cooperation with a third countries that would provide legal grounds based on which Europol could lawfully transfer personal data to authorities of that third countries: (1) a Commission adequacy decision adopted in accordance with Article 36 of Directive (EU) 2016/680; (2) an international agreement concluded by the Union pursuant to Article 218 TFEU; (3) an authorisation by the Europol Management Board, in agreement with the EDPS, based on a self-assessment that adequate safeguards for the protection of privacy and fundamental rights exist. Moreover, in specific situations on a case-by-case basis, the Europol Executive Director may authorise the transfer of personal data.

64 The negotiating mandates allow the Commission to enter into negotiations with eight priority countries on behalf of the EU: Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia and Turkey.

65 Article 25(5) of Regulation (EU) 2016/794.

66 Europol has cooperation agreements in place with 17 countries: Albania, Australia, Bosnia and Herzegovina, Canada, Columbia, Georgia, Iceland, Liechtenstein, Moldova, Monaco, Montenegro, North Macedonia, Norway, Serbia, Switzerland, Ukraine, United States of America.

Annex 5: Detailed assessment of the policy options in terms of their limitations on the exercise of Fundamental Rights

Fundamental Rights, enshrined in the Charter of Fundamental Rights of the European Union (hereinafter, 'the Charter'), constitute the core values of the EU. These rights must be respected whenever EU institutions design new policies or adopt new legislative measures. EU institutions and Member States are obliged to respect the rights, observe the principles and promote the application of the Charter in accordance with their respective powers and respecting the limits of the powers of the Union as conferred on it by the Treaties. It is therefore the responsibility of the EU legislator to assess the necessity and proportionality of a proposed measure.

Building on the detailed description of the problems,[67] drivers,[68] objectives[69] and policy options[70] set out in the impact assessment and in annex 6,[71] this annex provides a more detailed assessment of the policy options in terms of their limitations on the exercise of the Fundamental Rights protected by the Charter. Chapters 6 and 7 of the impact assessment, setting out the overall impact of the policy options and their comparison, incorporate the result of the detailed Fundamental Rights impact assessment provided by this annex.

1. METHODOLOGY

To be lawful, any limitation on the exercise of the Fundamental Rights protected by the Charter must comply with the following criteria, laid down in Article 52(1) of the Charter:

- it must be provided for by law;
- it must respect the essence of the rights;
- it must genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others;
- it must be necessary;[72] and
- it must be proportional.

67 See chapter 2 of the impact assessment.

68 See chapter 2 of the impact assessment.

69 See chapter 4 of the impact assessment.

70 See chapter 5 of the impact assessment.

71 In addition to the problems, drivers, objectives and policy options set out in the impact assessment, this annex also provides a more detailed assessment of the policy options set out in annex 6 ('Europol and the Schengen Information System') in terms of their limitations on the exercise of the Fundamental Rights, given that these policy options would foresee a structural processing of personal data. As regards the policy options set out in annex 7 ('Europol's cooperation with third countries'), their impact on Fundamental Rights is limited and is therefore assessed directly in that annex. The policy options set out in annex 8 ('Europol's capacity to request the initiation of criminal investigations') do not limit any Fundamental Right and are therefore not addressed in this annex.

72 For any limitations on the exercise of the Fundamental Rights to the protection of personal data (Article 8 of the Charter) and to respect for private life (Article 7 of the Charter) with regard to the processing of personal data, the case law of the CJEU applies a *strict necessity* test. The requirement of "strict necessity" flows from the important role the processing of personal data entails for a series of fundamental rights, including freedom of expression.

In assessing the policy options against these criteria, this annex applies the Commission's Operational guidance on taking account of Fundamental Rights in Commission impact assessments,[73] the handbook by the Fundamental Rights Agency on Applying the Charter of Fundamental Rights[74], and the toolkits provided by the European Data Protection Supervisor (EDPS) on assessing necessity and proportionality.[75] Given the importance of the processing of personal data for the work of law enforcement in general, and for the support provided by Europol in particular, this annex puts a particular focus on the Fundamental Rights to the protection of personal data (Article 8 of the Charter) and to respect for private life (Article 7 of the Charter).

For those policy options that limit Fundamental Rights, the assessment follows the checklists for assessing necessity of new legislative measures and the checklist for assessing proportionality of new legislative measures as set out in the toolkits provided by the European Data Protection Supervisor:

I. Checklist for assessing **necessity** of new legislative measures
   - step 1: factual description of the measure
   - step 2: identification of Fundamental Rights limited by the measure
   - step 3: definition of objectives of the measure
   - step 4: choice of option that is effective and least intrusive

II. Checklist for assessing **proportionality** of new legislative measures
   - step 1: assessment of the importance of the objective and whether the measure meets the objective
   - step 2: assessment of the scope, the extent and the intensity of the interference
   - step 3: 'fair balance' evaluation of the measure
   - step 4: identification and introduction of safeguards

In line with the Commission's Operational guidance on taking account of Fundamental Rights in Commission impact assessments, and notably its guidance on discarding policy options at an early stage of the process if they have a serious adverse impact on Fundamental Rights, the impact assessment discarded one policy option at an early stage.[76] As regards the specific objective of clarifying the provisions on information processing activities in the Europol Regulation, the impact assessment does not address the policy option of removing the requirement[77] related to specific categories of data subjects in annex II of the Europol Regulation. This policy option would undermine the existing level of data protection at Europol and have a serious adverse impact on Fundamental Rights.

This document assesses the policy options in terms of their limitations on the exercise of Fundamental Rights against the existing level of data protection at Europol, as provided

73 SEC(2011) 567 final (6.5.2011).

74 European Union Agency for Fundamental Rights: Applying the Charter of Fundamental Rights of the European Union in law and policymaking at national level (2018).

75 European Data Protection Supervisor: Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A toolkit (11.4.2017); European Data Protection Supervisor: EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data (19.12.2019).

76 See Annex 9 on policy options discarded at an early stage.

77 Article 18(6) of Regulation (EU) 2016/794 (11.5.2016). The categories of data subjects are listed in annex II of that Regulation.

for in the Europol Regulation. As stated in the impact assessment, the legislative initiate to strengthen Europol's legal mandate is expected to include aligning Europol's data protection regime with the Regulation[78] on the processing of personal data by EU institutions, bodies, offices and agencies, also taking inspiration from the Data Protection Law Enforcement Directive.[79] Such an alignment will further strengthen the data protection regime applicable to Europol, including its supervision by the EDPS, thus ensuring that the agency's legal regime continues to provide for the highest level of data protection. Albeit not explicitly addressed in the assessment of each policy option, the alignment will overall have a positive impact and help mitigating the limitations on the exercise of Fundamental Rights.

This document assesses each policy option individually in terms of its limitations on the exercise of Fundamental Rights. Building on that, it is also important to assess the accumulated impact of the preferred options on Fundamental Rights, as provided for in section 8.3 of the impact assessment.

2. ASSESSMENT OF POLICY OPTIONS IN TERMS OF THEIR LIMITATIONS ON THE EXERCISE OF FUNDAMENTAL RIGHTS

2.1. Objective 1: Enabling Europol to cooperate effectively with private parties

Policy option 1: allowing Europol to process data received directly from private parties

1. Checklist for assessing necessity of new legislative measures

Step 1: Factual description of the measure

The policy option is described in detail in chapter 5 of the impact assessment. It entails the processing of personal data as it will enable Europol to receive personal data from private parties on their own initiative and process it in fulfilment of its tasks. The overall objective is to enable Europol to cooperate effectively with private parties in order to effectively support Member States in countering crimes prepared or committed using cross-border services offered by private parties. In line with this objective, the purpose of this data processing is to provide private parties with the possibility to share multi-jurisdictional or non-attributable data sets with Europol, so that the Agency can analyse the data and share it with the Member States concerned. The policy option provides for the processing of all personal data, which private parties share with Europol. The personal data would be processed by Europol in line with its existing legal framework. The Agency would – in a first step – process the data in order to determine whether such data are relevant to its tasks and, if so, for which purposes. In a second step, the Agency would analyse the data and share it with the Member States concerned.

Step 2: Identification of Fundamental Rights limited by the measure

The policy options limits the Fundamental Right to the protection of personal data as guaranteed by Article 8 of the Charter. As the policy option entails the processing by a public authority of data relating to the private life of an individual, it also limits the Fundamental Right to respect for private life (Article 7 of the Charter). Consequently, the

[78] Regulation (EU) 2018/1725.
[79] Directive (EU) 2016/680.

policy option needs to comply with the conditions laid down in Article 52(1) of the Charter. This policy option does not adversely affect the essence of the Fundamental Rights to the protection of personal data and to respect for private life, as transfers would be limited to situations where they are in the legitimate interest of the private party sharing the data. Subsequent processing would be limited to legitimate purposes under Europol's mandate and subject to adequate safeguards set out in the Europol Regulation.

Step 3: Definition of objectives of the measure

The policy option addresses the problem that Member States cannot effectively counter crimes prepared or committed using cross-border services offered by private parties, in particular the problems private parties face when they want to share multi-jurisdictional or non-attributable data sets on criminals using their cross-border services. This problem is clearly identified and described in detail in chapter 2 of the impact assessment. The policy option aims to achieve the specific objective to enable Europol to cooperate effectively with private parties as precisely defined in chapter 4 of the impact assessment, in particular to enable Europol to receive personal data directly from private parties. The policy option therefore falls within the scope of the fight against serious crime and terrorism which are recognised as objectives of general interest in EU law.

Step 4: Choice of option that is effective and least intrusive

The policy option is **genuinely effective** as it is essential to achieve the specific objective of improving Europol's ability to support Member States in identifying cases and information with relevance for their respective jurisdictions. In particular, where the cases rely on the analysis of multi-jurisdictional data sets, or data sets where the jurisdiction of the data subjects is difficult to establish, and therefore also essential to the fight against serious crime and terrorism as objectives of general interest in EU law.

Enabling Europol to receive personal data directly from private parties **effectively contributes to achieving these objectives**, as it provides private parties with a central point of contact, when they see the need to share personal data with unclear or multiple jurisdictions.

This policy option addresses the problems that private parties and national law enforcement face in identifying the jurisdiction that is responsible for the investigation of a crime committed with the use of cross-border services. It does so **more effectively** than non-legislative options such as best practices. Indeed, **best practices would be less intrusive but insufficient** to address the problem.[80] Also, national authorities cannot effectively investigate such crimes through national solutions, or by way of intergovernmental cooperation.[81] Likewise, existing rules on the exchange of personal data between Europol and private parties, even if their application is reinforced, are insufficient to address the problem.[82] In particular, private parties cannot effectively share multi-jurisdictional or non-attributable data sets indirectly with Europol via national law enforcement authorities, as they focus on identifying data relevant for their respective jurisdictions, and are not well placed to identify personal data relevant to other jurisdictions. Such an indirect way of sharing personal data entails risks of delays and

[80] See annex 9 on policy options discarded at an early stage.

[81] See Chapter 2.1 of the impact assessment on the problem description.

[82] See chapter 2 of the impact assessment on the problem description, the problem drivers, and how the problem will evolve.

even data loss.

As there are no other effective but less intrusive options, the policy option is **essential and limited to what is absolutely necessary** to achieve the specific objective of enabling Europol to cooperate effectively with private parties, and hence the fight against serious crime and terrorism as objectives of general interest in EU law.

2. Checklist for assessing proportionality of new legislative measures

Step 1: Importance of the objective and whether the measure meets the objective

The policy option addressed the **problems private parties face when they want to report criminals using their cross-border services**, but have difficulties identifying the appropriate jurisdiction. The problem and its drivers are described in detail in chapter 2 of the impact assessment. As set out in chapter 2 of the impact assessment, there is indeed an urgent need to address the problem as it will otherwise increase. There is indeed a pressing social need to protect EU citizens from crimes prepared or committed using cross-border services offered by private parties.

The policy option and its purpose, namely to enable Europol to effectively cooperate with private parties **corresponds to the identified need and partially solves the problem** of Europol's inability to support Member States in countering crimes prepared or committed using cross-border services offered by private parties. The policy option is effective and efficient to fulfil the objective.

Step 2: Assessment of the scope, the extent and the intensity of the interference

The policy option affects data subjects, who are associated with a serious crime falling within Europol's mandate, such as criminals, suspects, witnesses and victims, and whose personal data private parties share with Europol. The policy option raises **collateral intrusions** as private parties may share data on data subjects, who are not associated with a crime, for which Europol is competent, and hence of persons other than the targeted individuals of the measure. This risk will be mitigated with the introduction of necessary safeguards in step 4.

The policy option does **not impose a disproportionate and excessive burden** on the persons affected by the limitation, in relation to the specific objective of enabling Europol to cooperate effectively with private parties and hence the fight against serious crime and terrorism as objectives of general interest in EU law, as Europol's data protection regime will provide for adequate safeguards (see step 4) .

No potential harmful effect of the policy option on other Fundamental Rights has been identified, as the impact of this policy option is limited to impacts on the right to the protection of personal data and the respect for private life.

Step 3: 'Fair balance' evaluation of the measure

Weighing up the intensity of the interference with the Fundamental Rights to the protection of personal data and to respect for private life as described under step 2 with the legitimacy of the objectives to fight against serious crime and terrorism as objectives of general interest in EU law, the policy option constitutes a **proportionate response** to the need to solve the problem resulting from limits in Europol's ability to effectively support Member States in countering crimes prepared or committed using cross-border services offered by private parties.

However, in order to establish a balance between the extent and nature of the interference and the reasons for interfering as translated into the objective of enabling Europol to effectively cooperate with private parties, a **number of safeguards are required** (see step 4).

Step 4: Identification and introduction of safeguards

A **number of safeguards would be necessary** to establish a balance between the extent and nature of the interference and the reasons for interfering as translated into the objective of enabling Europol to effectively cooperate with private parties:

- All the safeguards set out in the rules applicable to personal data, which Europol receives from competent authorities, would also to apply to personal data, which Europol receives directly from private parties.[83]
- In particular, upon receiving the data, Europol would process the personal data only temporarily for as long is necessary to determine whether the data is relevant to its tasks. If the data is not relevant for its tasks, Europol would delete the data after six months. Only if the data is relevant to its tasks, would Europol process the data further (Article 18 (6) Europol Regulation). In practice, this would mean that Europol would delete personal data on data subjects, which are not associated with a serious crime falling within Europol's mandate. There should be a high threshold with clear criteria and strict conditions for Europol to determine whether data received from private parties is relevant for Europol's objectives and should become part of Europol's operational data.
- Furthermore, Europol would be limited in the way it can process special categories of data (e.g. on ethnicity or religious beliefs) and different categories of data subjects (e.g. victims and witnesses) (Article 30 Europol Regulation).
- Moreover, Europol would not be allowed to process the data for longer than necessary and proportionate, and within the time-limits set by the Europol Regulation (Article 31).
- Also, the Europol Regulation would ensure the necessary data subject rights, in particular a right of access (Article 36), and a right to rectification, erasure and restriction (Article 37).
- In addition, the Europol Regulation would ensure the possibility for an individual to pursue legal remedies (Article 47 and 48 Europol Regulation).

<u>Policy option 2</u>: allowing Europol to exchange personal data directly with private parties

1. Checklist for assessing necessity of new legislative measures

Step 1: Factual description of the measure

The policy options entails the processing of personal data as it foresees that Europol will be able to exchange personal data directly with private parties to establish the jurisdiction of the Member States concerned, as well as to serve as a channel to transmit Member States' requests containing personal data to private parties in addition to the possibility to process personal data received from private parties under policy option 1.

[83] See pp. 45f of the Opinion of the European Union Agency for Fundamental Rights on Interoperability and fundamental rights implications (11.4.2018).

Under this option, Europol would be able to:

a) exchange information with a private party as part of a follow-up to that private party having shared personal data with the Agency in the first place in order to notify that private party about the information missing for the Agency to establish the jurisdiction of the Member State concerned; or
b) request personal data indirectly from private parties on its **own initiative**, by sending a reasoned request to the Member State of establishment (or the Member States in which the legal representative[84] is based)[85] to obtain this personal data under its national procedure, in order to identify the Member State concerned for a crime falling under Europol's mandate (e.g. when a data set received from a private party requires additional information from another private party in order to identify the Member State concerned); or
c) serve as a **channel** to transmit Member States' requests containing personal data to private parties in relation to crimes falling under Europol's mandate[86] (e.g. to ensure co-ordination with regards to removal orders and referrals as foreseen by Article 13 of the proposed Regulation on removing terrorist content online).[87]

The objective is to **improve Europol's ability to support Member States in identifying cases and information with relevance for their respective jurisdictions**, in particular where the cases rely on the analysis of multi-jurisdictional data sets, or data sets where the jurisdiction of the data subjects is difficult to establish. In line with this objective (and in addition to policy option 1), this policy option would address the challenges Europol is facing when the Agency needs additional information from private parties to analyse multi-jurisdictional or non-attributable data sets in order to establish the jurisdiction of the Member States concerned. It would also address the problems private parties face when receiving requests from law enforcement authorities of another country, including problems in verifying whether the requesting authority is a legitimate law enforcement agency.[88]

The policy option provides for the processing of personal data, as it foresees that Europol will transfers personal data to private parties for the purpose of notifying private parties and requesting further personal data. Moreover, Europol would process the personal data received from private parties, and serve as a channel for Member States requests to private parties. It concerns the personal data of persons that are relevant to Europol's

84 It should be noted that representatives appointed to comply with the such requests and those appointed in line with the General Data Protection Regulation may share some similarities as they would act as contact points of the service providers they represent. However, they would have very different tasks and responsibilities in nature and they would answer to different types of stakeholders. These two functions require different knowledge and competencies (see also p. 17 of the Opinion of the European Union Agency for Fundamental Rights on Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters (6.11.2019)).

85 Hereafter the notion of 'Member State of establishment' will refer to (i) the Member State in which the private party is established, and (ii) the Member State in which the private party has a legal representative (in case it is not established in the EU).

86 Such channels set up by Europol should not duplicate existing or future other channels, such as might be set up in the framework for e-evidence.

87 Article 13 of the Proposal for a Regulation on preventing the dissemination of terrorist content online, COM(2018) 640 final (12.9.2018).

88 On private parties' ability to verify the authenticity of requests from competent authority, see also p. 6 of the of the Formal comments of the EDPS on the Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (13.2.2019).

tasks, such as criminals, suspects, witnesses, and victims. Europol would process the personal data for the purpose of issuing the request, and by the private parties for the purpose of replying to the request.

Step 2: Identification of Fundamental Rights limited by the measure

The policy options limits the Fundamental Right to the **protection of personal data** as guaranteed by Article 8 of the Charter. As the policy option entails the processing by a public authority of data relating to the private life of an individual, it also limits the Fundamental Right to **respect for private life** (Article 7 of the Charter). The policy option also limits the fundamental rights of private parties to **conduct business** (Article 16 of the Charter). Consequently, the policy option needs to comply with the conditions laid down in Article 52(1) of the Charter.

The policy option does **not adversely affect the essence** of the Fundamental Right to protection of personal data, respect for private life and the right to conduct business, as exchanges would be limited to situations, in which Europol requires additional information in order to process data it has previously received, or upon a request from a Member State, for legitimate purposes under Europol's mandate and subject to adequate safeguards enshrined in the Europol Regulation.

Step 3: Definition of objectives of the measure

The policy option addresses the **problems Europol is facing when the Agency needs additional information from private parties to analyse multi-jurisdictional or non-attributable data sets** in order to establish the jurisdiction of the Member States concerned, and the problems private parties are facing when receiving requests from law enforcement authorities of another country. These problems are clearly identified and described in detail in chapter 2 of the impact assessment.

The policy option aims to achieve the specific objective to **improve Europol's ability to support Member States in identifying cases and information with relevance for their respective jurisdictions**, in particular where the cases rely on the analysis of multi-jurisdictional data sets, or data sets where the jurisdiction of the data subjects is difficult to establish, and to be able serve as a channel to transmit Member States' requests containing personal data to private parties, as precisely defined in chapter 4 of the impact assessment. The policy option therefore falls within the scope of the fight against serious crime and terrorism which are recognised as objectives of general interest in EU law.

Step 4: Choice of option that is effective and least intrusive

The policy option is **genuinely effective as it is essential to achieve the specific objective** of enabling Europol to improve Europol's ability to support Member States in identifying cases and information with relevance for their respective jurisdictions, in particular where the cases rely on the analysis of multi-jurisdictional data sets, or data sets where the jurisdiction of the data subjects is difficult to establish, and to be able serve as a channel to transmit Member States' requests containing personal data to private parties, and therefore also essential to fight against serious crime and terrorism as objectives of general interest in EU law

Enabling Europol to exchange personal data directly with private parties to establish the jurisdiction of the Member States concerned, as well as to serve as a channel to transmit Member States' requests containing personal data to private parties (in addition to the

possibility to process personal data received from private parties under policy option 1) **effectively contributes to achieving this objective**, as it enable Europol to obtain additional information necessary to establish the jurisdiction of the Member States concerned, and to serve as a channel or Member States' requests to private parties.

This policy option addresses the problems that Member States and private parties face in identifying the jurisdiction that is responsible for the investigation of a crime committed with the use of cross-border services, and when private parties receive request from law enforcement authorities of another country, **more effectively than non-legislative options** such as best practices. Indeed, **best practices would be less intrusive but insufficient to address the problem**.[89]

Likewise, **existing rules** on the exchange of personal data between Europol and private parties, even if their application is reinforced, are **insufficient** to address the problem. The current system does not allow for a point of contact for private parties in multi-jurisdictional cases or in cases where the jurisdiction is unclear, nor can it ensure that this type of data is shared with other Member States concerned.[90]

Notably, private parties cannot effectively share multi-jurisdictional or non-attributable data sets indirectly with Europol via national law enforcement authorities, as they focus on identifying data relevant for their respective jurisdictions, and are not well placed to identify personal data relevant to other jurisdictions. Such an indirect way of sharing personal data entails risks of delays and even data loss. Moreover, the current system does not allow for Europol to serve as a channel for Member States requests for private parties.

As there are no other effective but less intrusive options, the policy option is **essential and limited to what is absolutely necessary** to achieve the specific objective of enabling Europol to cooperate effectively with private parties, and hence the fight against serious crime and terrorism as objectives of general interest in EU law.

2. Checklist for assessing proportionality of new legislative measures

Step 1: Importance of the objective and whether the measure meets the objective

The policy option addressed the problem, that Member States and private parties face in **identifying the jurisdiction that is responsible for the investigation of a crime committed with the use of cross-border services**, and when private parties receive request from law enforcement authorities of another country. The problem and its drivers are described in detail in chapter 2 of the impact assessment.

As set out in chapter 2 of the impact assessment, there is indeed an **urgent need to address the problem** as it will otherwise increase. There is indeed a pressing social need to protect EU citizens from crimes prepared or committed using cross-border services offered by private parties.

The policy option and its purpose to enable Europol to effectively cooperate with private parties **corresponds to the identified need and partially solves the problem** of Europol's inability to support Member States in countering crimes prepared or committed

89 See annex 9 on policy options discarded at an early stage.

90 See chapter 2 of the impact assessment on the problem description, the problem drivers, and how the problem will evolve.

using cross-border services offered by private parties. The policy option is effective and efficient to fulfil the objective.

Step 2: Assessment of the scope, the extent and the intensity of the interference

This policy option affects data subjects who are associated with a serious crime falling within Europol's mandate (as discussed under policy option 1), as well as data subjects, which are subject to a criminal investigation at national level, but not necessarily associated with a crime falling within Europol's mandate.

In both cases, the policy option raises **collateral intrusions** as Europol may process personal data of data subjects, which are not associated with a serious crime falling within Europol's mandate. This risk will be mitigated with the introduction of necessary safeguards in step 4.

This policy option also affects private parties' right to conduct business, insofar as Europol would request personal data indirectly from private parties on its own initiative, by sending a reasoned request to the Member State of establishment (or the Member States in which the legal representative is based)[91] to obtain this personal data under its national procedure. This risk will also be mitigated with the introduction of necessary safeguards in step 4.

The policy option does **not impose a disproportionate nor an excessive burden** on the persons affected by the limitation, namely data subjects, who are not associated with a crime, for which Europol is competent, in relation to the specific objective of enabling Europol to cooperate effectively with private parties and hence the fight against serious crime and terrorism as objectives of general interest in EU law.

No potential harmful effect of the policy option on other Fundamental Rights has been identified, as the impact of this policy option is limited to impacts on the right to the protection of personal data, the respect for private life, and the right to conduct business.

Step 3: 'Fair balance' evaluation of the measure

Weighing up the intensity of the interference with the Fundamental Rights of data subjects regarding the protection of personal data and to respect for private life, as well as with the Fundamental Rights of private parties right to conduct business (both described under step 2) with the legitimacy of the objectives to fight against serious crime and terrorism as objectives of general interest in EU law, the policy option constitutes a **proportionate response to the need to solve the problem**, that Member States cannot effectively counter crimes prepared or committed using cross-border services offered by private parties.

However, in order to establish a balance between the extent and nature of the interference and the reasons for interfering translated into the objective of enabling Europol to effectively cooperate with private parties, a **number of safeguards are required**.

Step 4: Identification and introduction of safeguards

A **number of safeguards would be necessary** to establish a balance between the extent

[91] Hereafter the notion of 'Member State of establishment' will refer to (i) the Member State in which the private party is established, and (ii) the Member State in which the private party has a legal representative (in case it is not established in the EU).

and nature of the interference and the reasons for interfering as translated into the objective of enabling Europol to effectively cooperate with private parties.

- All the safeguards for data subjects set out in the current Europol Regulation, which are applicable to personal data received by Europol from competent authorities, would also apply to personal data received by Europol directly from private parties. These safeguards have been listed above (see policy option 1, proportionality assessment, step 4). In addition, an obligation to periodically publish in an aggregate from information on the number of exchanges with private parties could enhance transparency.[92]
- As regards follow-up exchanges, the policy option would introduce additional safeguards. Europol would issue such notifications solely for the purpose of gathering information to establish the jurisdiction of the Member State concerned over a form of crime falling within the Agency's mandate,[93] the personal data referred to in these notifications would have to have a clear link with and complement the information previously shared by the private party. Such notifications would have to be as targeted as possible,[94] and should refer to the least sensitive data that is strictly necessary for Europol to establish the jurisdiction of the Member State concerned. It should be clear that such notifications do not oblige the private party concerned to proactively share additional information.[95]
- As regards own-initiative requests, Europol would have to provide a reasoned request to the Member State of establishment, which should be as targeted as possible,[96] and should refer to the least sensitive data that is strictly necessary for Europol to establish the jurisdiction of the Member State concerned. The Member State of establishment would assess the request in the light of the European interest, but based on the standards of its applicable national law.[97] This would ensure that the request does not go beyond what the national law enforcement authorities of this Member State could request without judicial authorisation in terms of the type of information requested (e.g. subscriber data, access data, traffic data, or content data), as well as with regard to the procedural aspects of

92 See p.15 of the Opinion of the European Union Agency for Fundamental Rights on Proposal for a Regulation on preventing the dissemination of terrorist content online and its fundamental rights implications (12.2.2019).

93 It is noted that Europol's tasks should be clearly distinguished from those performed by financial intelligence units. Europol will remain limited to processing criminal intelligence with a clear link to forms of crime falling under Europol's mandate. Any cooperation with private parties will remain strictly within the limits of Europol's mandate and will neither duplicate nor interfere with the activities of the FIUs. Europol will continue to cooperate with FIUs via their national units in full respect of their competence and mandate as foreseen under Article 7 (8) of the Europol Regulation and under Articles 11 to 14 of the Directive (EU) 2019/1153.

94 See also p. 6 of the Formal comments of the EDPS on the Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (13.2.2019).

95 See p. 38f of the Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Regulation on preventing the dissemination of terrorist content online and its fundamental rights implications (12.2.2019)

96 See also p. 6 of the of the Formal comments of the EDPS on the Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online (13.2.2019).

97 On the involvement of the Member State of establishment, see also p. 12 of the opinion of the European Data Protection Supervisor: EDPS Opinion on Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters (6.11.2019).

the request (e.g. form, language requirements, delay in which the private party would have to reply to a similar request from national law enforcement authorities). This would also ensure that the applicable national thresholds for requesting more sensitive personal data (such as content data) also apply. The national requests would have to be subject to the appropriate judicial supervision[98] and provide access to an effective remedy.[99]

- As regards Europol serving as a channel for Member States requests to private parties, the Member State would follow the rules and procedures of the underlying legislation allowing for such requests (e.g. proposed Regulation on preventing the dissemination of terrorist content online[100]), and provide assurance that its request is in line with its applicable laws, which would have to provide sufficient safeguards to the affected fundamental rights, including access to an effective remedy.[101]

Policy option 3: allowing Europol to directly query databases managed by private parties

1. Checklist for assessing necessity of new legislative measures

Step 1: Factual description of the measure

The policy option is described in detail in chapter 5 of the impact assessment. The policy options entails the processing of personal data as it foresees that Europol will be able to directly query databases managed by private parties in specific investigations (in addition to enabling Europol to receive and requesting personal data from private parties as described under policy option 2 and 3).

The overall objective is to **enable Europol to analyse larger data volumes held by private parties** in a speedy manner in order to support a specific investigation of a Member State.

In line with that objective, the purpose of the data processing is to **enable Europol to directly query databases managed by private parties** in specific investigations. This would enable Europol to obtain and analyse such data much quicker than by way of an individual request.

The policy option provides for the processing of personal data contained in the data bases of private parties. It provides for the processing of personal data of persons, whose data Europol can process in the fulfilment of its tasks, in particular criminals, suspects, witnesses, and victims. The personal data would be processed by Europol.

Step 2: Identification of Fundamental Rights limited by the measure

98 See pp. 23f of the Opinion of the European Union Agency for Fundamental Rights on Proposal for a Regulation on preventing the dissemination of terrorist content online and its fundamental rights implications (12.2.2019).

99 See pp. 28f of the Opinion of the European Union Agency for Fundamental Rights on Proposal for a Regulation on preventing the dissemination of terrorist content online and its fundamental rights implications (12.2.2019).

100 COM(2018) 640 final (12.9.2018).

101 See p. 28f of the Opinion of the European Union Agency for Fundamental Rights on Proposal for a Regulation on preventing the dissemination of terrorist content online and its fundamental rights implications (12.2.2019).

The policy options limits the Fundamental Right to the **protection of personal data** as guaranteed by Article 8 of the Charter. As the policy option entails the processing by a public authority of data relating to the private life of an individual, it also limits the Fundamental Right to **respect for private life** (Article 7 of the Charter). The policy option also limits the fundamental rights of private parties to **conduct business** (Article 16 of the Charter). Consequently, the policy option needs to comply with the conditions laid down in Article 52(1) of the Charter.

The policy option **does not adversely affect the essence** of the Fundamental Rights to protection of personal data, respect for private life and the right to conduct business, as such queries would be limited to specific investigations, and subsequent processing would be limited to legitimate purposes under Europol's mandate and subject to adequate safeguards enshrined in the Europol Regulation.

Step 3: Definition of objectives of the measure

The policy option addresses the problem that Member States cannot effectively counter crimes prepared or committed using cross-border services offered by private parties. This problem is clearly identified and described in detail in chapter 2 of the impact assessment.

The policy option aims to achieve the specific objective to **enable Europol to cooperate effectively with private parties** as precisely defined in chapter 4 of the impact assessment, in order to better support Member States in specific investigations. The policy option therefore falls within the scope of the fight against serious crime and terrorism which are recognised as objectives of general interest in EU law.

Step 4: Choice of option that is effective and least intrusive

The policy option is **genuinely effective** as it is essential to achieve the specific objective of enabling Europol to cooperate effectively with private parties in order to effectively support Member States in countering crimes prepared or committed using cross-border services offered by private parties, and therefore the fight against serious crime and terrorism as objectives of general interest in EU law.

Enabling Europol to directly query data bases managed by private parties (in addition to enabling the Agency to receive, and request personal data in line with policy option 2 and option 3) **effectively contributes to achieve this objective**.

Existing possibilities to meet the objective, notably the promotion of best practices, are **insufficient** to address the problem. Likewise, existing rules on the exchange of personal data between Europol and private parties, even if their application is reinforced, are insufficient to address the problem.

However, **policy option 2 addresses the problem equally effective** as policy option 3 by enabling Europol to issue requests for personal data to private parties, while being **less intrusive** as it does not oblige private parties to accept a direct access by Europol to their data bases. Instead, policy option 2 would ensure that private parties maintain control over the data bases they manage. Moreover, under policy option 2, the Member State of establishment would have to assess Europol's request. Furthermore, policy option 2 would ensure the possibility of ex ante judicial remedy against individual own-initiative requests under applicable laws of the Member State concerned. In particular, the

safeguards under option 2 would ensure that Europol's request would not circumvent national safeguards, by ensuring that the applicable national thresholds for requesting more sensitive personal data (such as content data) also apply to Europol. Policy option 2 would therefore be less intrusive, both for data subjects and for private parties.

Consequently, as a less intrusive measure is available that is equally effective in meeting the objective, policy option 3 is not limited to what is strictly necessary to achieve the objective. **The policy option does therefore not pass the necessity test.** The policy option shall therefore **not be assessed in terms of its proportionality**.[102]

2. Checklist for assessing proportionality of new legislative measures

As the policy option did not pass the necessity test, and therefore is not limited to what is strictly necessary, the policy option shall **not be assessed in terms of its proportionality**.

2.2. *Objective II*: enabling law enforcement to analyse large and complex datasets to detect cross-border links, in full compliance with Fundamental Rights

Policy option 4: clarifying the provisions on the purposes of information processing activities and enabling Europol to analysis large and complex datasets

1. Checklist for assessing necessity of new legislative measures

Step 1: Factual description of the measure

This policy option consists of **clarifying the provisions on the purposes of information processing activities** of the Europol Regulation to enable Europol to effective fulfil its mandate in full compliance with Fundamental Rights including by way of **analysing large and complex datasets**. It would provide a clear legal basis and the necessary safeguards for such data processing, addressing the fact that criminals and terrorist use information and communications technology to communicate among themselves and to prepare and conduct their criminal activity. This would concern Europol's tasks when processing personal data it received in the context of the prevention and countering of crimes falling under Europol's mandate. This would include data processing for preventive purposes and criminal intelligence. It would also include the analysis of large and complex datasets upon request by a Member State in a specific investigation, including by way of digital forensics.

This policy option would address the **structural legal problems** identified by the EDPS in its decision on Europol's big data challenge.[103] This regulatory intervention would

---

[102] As set out in the toolkit provided by the EDPS on assessing necessity, "*only if existing or less intrusive measures are not available according to an evidence-based analysis, and only if such analysis shows that the envisaged measure is essential and limited to what is absolutely necessary to achieve the objective of general interest, this measure should proceed on to the proportionality test*". Likewise, the Commission's Operational guidance on taking account of Fundamental Rights in Commission impact assessments states that "*if it can be established that there are two policy options which are equally effective in achieving the objective but have different negative impacts on fundamental rights, then it is necessary to choose that option which is the least intrusive*".

[103] See the EDPS Decision on the own initiative inquiry on Europol's big data challenge: https://edps.europa.eu/sites/edp/files/publication/20-09-

maintain the obligation on Europol to limit its data processing to the specific categories of data subjects listed in annex II of the Europol Regulation (i.e. persons related to a crime for this Europol is competent), while clarifying that:

- when Europol receives personal data, it might carry out, in case of doubt and prior to any further data processing, an **initial processing of such data (e.g. by way of collation[104]), including a check against data held in its databases, for the sole purpose of verifying** if the data falls into the categories of data subjects set out in annex II of the Europol Regulation. This pre-analysis might involve the use of technology, and exceptionally require more time, for the verification of high volumes of personal data received in the context of a specific investigation. This would provide the **necessary legal clarity** for Europol to process personal data in compliance with the requirement related to the specific categories of data subjects listed in annex II of the Europol Regulation.
- when Europol **analyses large and complex data sets**, including by way of digital forensics, **to support a criminal investigation** in a Member State, it may **exceptionally process and store data of persons who are not related to a crime**. Such data processing would only be allowed where, due to the nature of the large dataset, it is necessary for the operational analysis to also process data of persons who are not related to a crime, and only for as long as it supports the criminal investigation for which the large dataset was provided. This **narrow and justified exception** would extend the grounds for data processing by Europol. Moreover, upon request of the Member State that provided the large and complex dataset to Europol in support of a criminal investigation, Europol may store that dataset and the outcome of its operational analysis beyond the criminal investigation. Such data storage would only be possible for the sole purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process, and only for as long as it is necessary for the judicial proceedings related to that criminal investigation. During that period, the data would be blocked for any other processing.

The policy option entails the processing of personal data as it would provide the possibility for Europol to process data it received in the context of the prevention and countering of crimes falling under Europol's mandate. For the **first aspect** identified above (i.e. the need for an initial data processing), and in line with the overall objective of clarifying Europol's mandate in a way that enables the agency to fulfil its mandate and support Member States effectively, the sole purpose of this data processing would be to verify, where necessary, if the data relates to the specific categories of data subjects set out in annex II of the Europol Regulation (i.e. persons related to a crime for which Europol is competent). This initial data processing (pre-analysis) would enable Europol to verify, in case of doubt, if it is authorised to analyse the personal data it received in the context of the prevention and countering of crimes falling under Europol's mandate.

18_edps_decision_on_the_own_initiative_inquiry_on_europols_big_data_challenge_en.pdf. The EDPS issued an admonishment pursuant to Article 43(3)(d) of the Europol Regulation to signal data processing activities that are not in line with the applicable data protection framework and to urge Europol to adjust its practices. The EDPS invited Europol to provide an action plan to address the admonishment within two months, and to inform of the measures taken within six months following the issuing of the decision.

[104] I.e. the pre-analysis phase where unstructured data received is being organised and structured into a format from which it can be analysed.

For the **second aspect** identified above (processing of large and complex datasets), again in line with the overall objective of clarifying Europol's mandate in a way that enables the agency to fulfil its mandate and support Member States effectively, the purpose of the data processing would be to enable Europol to analyse a large and complex dataset submitted by a Member State in a criminal investigation. The second aspect would only apply where it is not possible for Europol, due to the nature of the data set, to carry out its operational analysis of the dataset without processing personal data that does not comply with the requirements related to the specific categories of data subjects listed in annex II of the Europol Regulation. Moreover, upon request of the Member State that provided a large and complex dataset to Europol in support of a criminal investigation, Europol would be able to store that large dataset and the outcome of its operational analysis beyond the duration of the criminal investigation. Such storage, and the use of the data, would only be possible for the sole purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process, and only for as long as the judicial proceedings related to the criminal investigation are on-going in the Member State

As regards the first aspect on the need for an initial data processing (pre-analysis phase), the policy option would provide for the initial processing of personal data submitted to Europol. It therefore concerns personal data submitted by Member States, Union bodies, third countries, international organisations, private parties and private persons in the context of preventing and combating crimes falling under Europol's mandate[105], including data transmitted by Member States for preventive purposes and criminal intelligence. As regards the second aspect on large and complex datasets, the policy options provides for the processing of such large and complex datasets submitted by a Member State in support of a specific investigation. This may include the data of persons who are not linked to a crime and who therefore do not fall under any of the categories of data subjects listed in annex II of the Europol Regulation.

When **Member States** submit personal data to Europol, they **usually do not indicate the categories of data subjects** under which the data falls. Moreover, it is not always clear from the outset if a person (to whom the data transmitted by a Member State relate) is related to a crime for which Europol is competent. Notably at an early stage of an investigation, it is often not possible to establish from the outset if a person is involved or not in the crime under investigation. In such cases of doubt, the policy option would enable Europol to carry out an initial processing of the data (e.g. collation[106] of the data), including a check against data held in Europol's databases, for the sole purpose of verifying if the data relates to the specific categories of data subjects set out in annex II of the Europol Regulation.

Moreover, due to the **nature of large and complex datasets**, and the specific processing operations required to analyse such datasets by way of **digital forensics**[107], the analysis of such datasets inevitably involves **processing data that is not relevant for the**

---

105 Where it is not clear whether data received by Europol are relevant to its tasks, Article 18(6) of the Europol Regulation (EU) 2016/794 would apply, where Europol may temporarily process such data for the purpose of determining whether such data are relevant to its tasks.

106 I.e. the pre-analysis phase where unstructured data received is being organised and structured into a format from which it can be analysed.

107 Digital forensics are usually defined as the collection and analysis of data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law. See e.g. Suneeta Satpathy, Sachi Nandan Mohanty: Big Data Analytics and Computing for Digital Forensic Investigations (7.3.2020).

criminal investigation. Indeed, the very purpose of this analysis is to separate the necessary information from data which is not related to the criminal activity.[108] For Europol's operational support, including by way of digital forensics, this implies that it is not possible for the agency to analyse large and complex dataset without also processing personal data that may not comply with the requirements linked to the categories of data subjects listed in annex II of the Europol Regulation. Moreover, digital forensics requires the **storage of the entire dataset for the duration of the criminal investigation and, possibly, subsequent judicial proceedings** to ensure (1) data veracity, (2) the reliability of the analysis, and (3) the traceability of the decision-making process by the analysts.[109] For Europol's operational support by way of digital forensics, the EDPS decision indicates that "*large datasets are further stored [...] even after the analysts has completed the extraction process in order to ensure that they, potentially with the support of a forensic expert, can come back to the contribution in case of a new lead and to ensure the veracity, reliability and traceability of the criminal intelligence process*." Indeed, the analytical reports that Europol provides based on its operational analysis may be used by a Member State as part of judicial proceedings following the criminal investigation.

Step 2: Identification of Fundamental Rights limited by the measure

The policy limits the Fundamental Right to the **protection of personal data** as guaranteed by Article 8 of the Charter. As the policy option entails the processing by a public authority of data relating to the private life of an individual, it also limits the Fundamental Right to **respect for private life** (Article 7 of the Charter). Consequently, the policy option needs to comply with the conditions set out in Article 52(1) of the Charter. The policy option does **not adversely affect the essence** of the Fundamental Rights to the protection of personal data and to respect for private life.

Step 3: Definition of objectives of the measure

The policy option addresses the problem of the **big data challenge for law enforcement**, as clearly identified and described in detail in chapter 2 of the impact assessment. Europol's legal basis limits the processing of personal data by Europol to data related to specific categories of data subjects listed in annex II of the Regulation (i.e. persons related to a crime for which Europol is competent). However, the Regulation does not explicitly set out how to comply with this safeguard when Europol receives personal data and when there is doubt whether that data falls into the specific categories of data subjects listed in annex II. Moreover, the European Regulation does not take account of the specific requirements for the processing of large and complex datasets. It does not take into account that digital forensics requires the storage of the entire dataset for the duration of the criminal investigation and, possibly, subsequent judicial proceedings to ensure (1) data veracity, (2) the reliability of the analysis, and (3) the traceability of the decision-making process by the analysts.

The policy option aims to achieve the specific objective of **enabling Europol to fulfil its mandate and support Member States effectively** when they submit data in the context

[108] Through processes of minimising and aggregating information and data, forensic experts filter and reduce the information contained in large and complex datasets to what is relevant for the criminal investigation, while discarding information that is not relevant to the case. Depending on the size and complexity of the dataset, such data processing may take several months or even years.

[109] Point 3.11 of the EDPS Decision on the own initiative inquiry on Europol's big data challenge.

of preventing and combating crimes that fall under Europol's mandate, including the analysis of large and complex datasets in the context of a specific criminal investigation. Chapter 4 of the impact assessment precisely defines that objective. The policy option therefore falls within the scope of the fight against serious crime and terrorism, which are recognised as objectives of general interest in EU law.

Step 4: Choice of option that is effective and least intrusive

The policy option is **genuinely effective** as it is essential to achieve the specific objective of enabling Europol to fulfil its mandate and support Member States with the processing of personal data they submitted in the context of preventing and combating crimes that fall under Europol's mandate, and therefore the fight against serious crime and terrorism as objectives of general interest in EU law.

The initial processing of personal data by Europol, including by way of an initial check against data in Europol's databases, for the sole purpose of verifying if the data falls under the specific categories of data subjects set out in annex II of the Europol Regulation, **effectively contributes to enabling Europol to process data in full compliance with its data protection requirements and safeguards**. The policy option would provide legal clarity and foreseeability. It would enable Europol to comply with the requirement related to specific categories of data subjects when it processes personal data received in fulfilling its objectives and tasks.

It that respect, the policy option takes account of the specific situation where Europol receives high volumes of personal data from Member States in a specific investigation. This might require the use of technology, and exceptionally require more time, to verify whether all personal data included in such high volumes of data relate to the specific categories of data subjects set out in annex II.

The policy option is **less intrusive** than policy option 5, as it maintains the requirement and safeguard related to the specific categories of data subjects listed in annex II of the Europol Regulation. Policy option 5 introduces a new category of data subjects in annex II that does not have any connection to a crime. This option would introduce the possibility for Europol to process further the personal data of persons for whom no link to any crime could be established by the Member States or by Europol. This would soften – and basically undermine – the requirement related to specific categories of data subjects. Policy option 5 would therefore go beyond the need to clarify the legal regime and to take account of the nature of large and complex datasets. It would therefore raise important questions of necessity and proportionality. Policy option 4, instead, would **in principle maintain the obligation on Europol to limit its data processing to the specific categories of data subjects listed in annex II**, while taking into account the specific requirements of the processing of large and complex datasets. In doing so, policy option 4 would set out a procedure that would enable the Agency to meet this requirement when processing personal data as part of carrying out its tasks and fulfilling its mandate, including large and complex datasets.

The **existing rules** on this requirement and safeguard, even if their application is reinforced, are insufficient to address the problem of a lack of clarity on Europol's information processing activities, as they do not enable Europol to meet this requirement in practice when processing personal data it received, notably large and complex datasets. In case of doubt, the current rules do not provide for any possibility for Europol to verify if personal data received fall into the specific categories of data subjects listed in

annex II of the Europol Regulation. Moreover, the current rules does not take account of the specific requirement of the processing of large and complex datasets, including by way of digital forensics. Policy option 4, instead, would provide the **necessary legal clarity and foreseeability**, as it would enable Europol to apply in principle the requirement related to specific categories of data subjects in its data processing, thus ensuring that the processing of personal data is limited to personal data that falls into the categories of data subjects listed in annex II. In that respect, the policy option would provide for an initial data processing would constitute a pre-analysis, prior to Europol's data processing for cross-checking, strategic analysis, operational analysis or exchange of information. It would also take account of the operational reality that Member States might submit large and complex datasets where necessary for specific investigation, and enable Europol to process such large and complex datasets. In that respect, the policy option would provide a **new legal ground for data processing by Europol**, which would limit the exercise of Fundamental Rights. Notably, it would provide for the exceptionally processing of data of persons who are not linked to a crime and who therefore do not fall under any of the categories of data subjects listed in annex II of the Europol Regulation. Such data processing would constitute a **narrow and justified exception**, only applicable where such data processing is necessary for the analysis of a large and complex dataset in the context of Europol's support to a specific criminal investigation in a Member State.

Consequently, policy option 4 is **essential and limited to what is strictly necessary** to achieve the specific objective of clarifying Europol's mandate in a way that enables the agency to fulfil its mandate and support Member States effectively, and hence to fight serious crime and terrorism as objectives of general interest in EU law.

2. Checklist for assessing proportionality of new legislative measures

Step 1: Importance of the objective and whether the measure meets the objective

The policy option addresses the problem of the big **data challenge for law enforcement**, which is due to a lack of clarity on Europol's information processing activities in the agency's legal mandate. The problem and its drivers are described in detail in chapter 2 of the impact assessment. As set out in that chapter, there is indeed a need to address the problem, as it otherwise risks affecting Europol's ability to fulfil core tasks of its mandate. If interpreted narrowly, the requirement related to specific categories of data subjects might limit Europol's ability to support Member States with the analysis of personal data they submitted in the context of the prevention and combating of crimes falling under Europol's mandate.

Without any intervention, Europol will not be able to verify if the personal data it received from Member States fall within the specific categories of personal data it is allowed to process under its legal mandate, and hence it might not be able to provide the analytical support requested by the Member State. Moreover, without any intervention, Europol may not be able to address the structural legal concerns related to the analysis of large and complex datasets, as identified by the EDPS in its decision on Europol's big data challenge. This would have an impact on Europol's core working methods and hence on its operational capabilities, affecting Europol's ability to support Member States in the analysis of large and complex datasets to detect cross-border links.

The policy option and its purpose of clarifying the rules on Europol's information processing activities **correspond to the identified need**. They solve the problem, the big

data challenge, as far as Europol is concerned. The policy option is effective and efficient to fulfil the objective.

Step 2: Assessment of the scope, the extent and the intensity of the interference

The policy option affects persons whose personal data was transmitted to Europol in the context of preventing and combating crimes that fall under Europol's mandate, and where there is doubt whether they fall into the categories of data subjects listed in annex II of the Europol Regulation. The policy option notably affects persons whose personal data was transmitted by Member States to Europol as part of a large dataset related to a specific criminal investigation, and how are not related to the crime under investigation.

The policy option limits the Fundamental Right to the protection of personal data as guaranteed by Article 8 of the Charter. As the policy option entails the processing by a public authority of data relating to the private life of an individual, it also limits the Fundamental Right to respect for private life (Article 7 of the Charter). No potential harmful effect of the policy option on other Fundamental Rights has been identified.

The policy option limits the Fundamental Rights to the protection of personal data and to respect for private life. It provides, in case of doubt and prior to any further data processing, an initial processing of such data for the **sole purpose** of verifying if the data received relates to the specific categories of data subjects set out in annex II of the Europol Regulation. Moreover, the policy options exceptionally enables Europol to process the data of persons who are not related to a crime, if such data processing is necessary to enable Europol to analyse a large and complex dataset received by a Member State in the context of a specific criminal investigation. The measure does not amount to profiling of the individual.

The policy option does **not impose a disproportionate and excessive burden** on the persons affected by the limitation in relation to the specific objective of clarifying the rules on Europol's data processing activities to enable the agency to fulfil its mandate, and hence to the objectives of fighting serious crime and terrorism as objectives of general interest in EU law. As regards the first aspect on an initial data processing, the **sole purpose of the interference** is to verify, in case of doubt, if personal data submitted in the context of preventing and countering crimes falling under Europol's mandate actually fall within one of the specific categories of data subjects listed in annex II of the Europol Regulation. In other words, the sole purpose of the interference is to determine if Europol is authorised to process further such personal data. If this pre-analysis shows that personal data does not fall within one of the specific categories of data subjects listed in annex II of the Europol Regulation, Europol is not allowed to further process that data and needs to delete it. As regards the second aspect on the analysis of large and complex datasets, the **sole purpose of the interference** is to enable Europol to process, as part of the large and complex dataset, the data of persons who are related to the serious crime or act of terrorism under investigation. For persons whose data is included in the large and complex dataset although they do not have any link to the crime under investigation, their data is not relevant to the criminal investigation and shall not be used therein.

Step 3: 'Fair balance' evaluation of the measure

Weighing up the intensity of the interference with the Fundamental Rights to the protection of personal data and to respect for private life, as described under step 3, with the legitimacy of the objectives to fight against serious crime and terrorism as objectives

of general interest in EU law, the policy option constitutes a **proportionate response** to the need to solve the problem resulting from the lack of clarity in Europol's legal mandate as regards data processing activities, as well as from the need to process large and complex datasets in support of a specific criminal investigation.

However, in order to establish a balance between the extent and nature of the interference and the reasons for interfering as translated into the objective of enabling Europol to fulfil its mandate when processing personal data received, including for preventive action and criminal intelligence, and including large and complex datasets in support of a specific criminal investigation, a **number of safeguards are necessary** (see step 4 below).

Step 4: Identification and introduction of safeguards

All applicable rules on data processing in the Europol mandate will also apply to the data processing foreseen under policy option 4. Further to that, a **number of safeguards** are necessary in order to establish a balance between the extent and nature of the interference and the reasons for interfering as translated into the objective of enabling Europol to fulfil its mandate when processing personal data received, and including large and complex datasets in support of a specific criminal investigation:

- Ensuring that the **sole purpose** of the initial processing of personal data is the verification if data submitted to Europol relates to the specific categories of data subjects set out in annex II of the Europol Regulation. If this verification confirms that the data is related to a crime that falls under Europol's mandate, and hence falls into one of the categories of data subjects in annex II, Europol is authorised to further process the data for the purposes for which it was submitted. If, instead, the verification does not indicate any link to a crime, and hence the personal data does not fall into any of the categories of data subjects in annex II, Europol is not authorised to process the data further. It needs to delete that data.
- Ensuring that, in case of doubt, the verification of personal data submitted by Member States takes place **within six months of receipt** of the data by Europol, in line with the six-month period provided for in Article 18(6) of the Europol Regulation to determine whether data is relevant to Europol's tasks.
- Ensuring that the **exceptional extension of the six-month time limit** that applies to the initial data processing is limited to specific situations where such an exceptions is strictly necessary. Any exceptional extension of the six-month time limit shall be subject to prior authorisation.
- Ensuring that the **exceptional processing** of data of persons who are not related to a crime is strictly limited to **narrow and justified exceptions**, namely to the **specific situation** where such processing is strictly necessary to enable Europol to analysis a large and complex dataset it received from a Member State for operational support to a specific criminal investigation. In other words, such exceptional data processing shall only be allowed if it is not possible for Europol to carry out the operational analysis of the large dataset without processing personal data that falls into one of the categories of data subjects in annex II of the Europol Regulation. **This requires a clear definition of the situations where the narrow and justified exception applies.**
- Ensuring that the **sole purpose** of the processing of data of persons who are not related to a crime, but whose data is part of the large and complex dataset, is the operational support that Europol provides to the specific criminal investigation in

the Member State that submitted the dataset. Alternatively and subsequently, the purpose of ensuring the veracity, reliability and traceability of the criminal intelligence process for judicial proceedings following the criminal investigation.

- Ensuring the processing of data of persons who are not related to a crime, but whose data is part of the large and complex dataset, is **only allowed for as long as Europol supports the specific criminal investigation** for which the large dataset was provided or, **only for as long as it is necessary for judicial proceedings related to the criminal investigation in a Member State. During that period, the data shall be blocked for any other processing**.

Policy option 5: introducing a new category of data subjects

1. Checklist for assessing necessity of new legislative measures

Step 1: Factual description of the measure

This policy option consists of **introducing a new category of data subjects** in annex II of the Europol Regulation covering persons who do not have any connection to a crime. This regulatory intervention would maintain the obligation on Europol to limit its data processing to categories of data subjects listed in annex II. However, it would significantly extend the scope of persons covered by these categories. It would set out specific requirements and safeguards for the processing of persons falling into this new category of data subjects.

The policy option provides for the processing of personal data as it would introduce a new category of data subjects in annex II of the Europol Regulation. As a consequence, and contrary to the existing Europol mandate, the agency would be authorised to process the data of persons who do not have any link to a crime. In line with the overall objective of clarifying Europol's mandate in a way that enables the agency to fulfil its mandate and support Member States effectively, the new category of data subjects would allow Europol to process further any personal data submitted by Member States, including large and complex datasets, even if the data subjects do not have any link to a crime. Authorised staff at Europol would process the personal data falling under the new category of data subjects, subject to specific requirements and safeguards.

Step 2: Identification of Fundamental Rights limited by the measure

The policy option limits the Fundamental Right to the protection of personal data as guaranteed by Article 8 of the Charter. As the policy option entails the processing by a public authority of data relating to the private life of an individual, it also limits the Fundamental Right to respect for private life (Article 7 of the Charter). Consequently, the policy option needs to comply with the conditions laid down in Article 52(1) of the Charter.

The policy option does **not adversely affect the essence** of the Fundamental Rights to the protection of personal data and respect for private life.

Step 3: Definition of objectives of the measure

The policy option addresses the **problem of a lack of clarity on information processing activities in the Europol Regulation**, as clearly identified and described in detail in chapter 2 of the impact assessment, including for the processing of large and complex datasets. Europol's legal basis limits the processing of personal data by Europol

to data related to specific categories of data subjects listed in annex II of the Regulation (i.e. persons related to a crime for which Europol is competent). However, the Regulation does not explicitly set out how to comply with this safeguard when Europol receives personal data from Member State and when there is doubt whether that data falls into the specific categories of data subjects listed in annex II.

The policy option aims to achieve the specific objective of **enabling Europol to fulfil its mandate and support Member States effectively** when they submit data in the context of preventing and combating crimes that fall under Europol's mandate, including large and complex datasets. Chapter 4 of the impact assessment precisely defines that objective. The policy option therefore falls within the scope of the fight against serious crime and terrorism, which are recognised as objectives of general interest in EU law.

Step 4: Choice of option that is effective and least intrusive

The policy option is **genuinely effective** as it achieves the specific objective of enabling Europol to fulfil its mandate and support Member States effectively, and therefore the fight against serious crime and terrorism as objectives of general interest of the EU. Introducing the new category of data subjects would allow Europol to process any personal data submitted by Member States in order to meet its objectives and fulfil its tasks, including large and complex datasets.

Introducing a new category of data subjects in annex II of the Europol Regulation **effectively contributes to achieve the objective** of enabling Europol to fulfil its mandate and support Member States when they submit data in the context of preventing and combating crimes that fall under Europol's mandate. Indeed, with the new category of data subjects, Europol would be able to process further any data submitted by Member States.

The policy option addresses the problem **equally effective** as policy option 4.[110] The latter would provide for an initial cross-check of personal data submitted by Member States against data held in Europol's databases, for the sole purpose of verifying if the data received relates to the specific categories of data subjects set out in annex II of the Europol Regulation. However, **policy option 4 is less intrusive**, as it would maintain the existing categories of data subjects as set out in annex II of the Europol Regulation. While policy option 5 basically undermines the requirement and safeguard related to the categories of data subjects, policy option 4 maintains that requirement while providing Europol with a possibility to fulfil it in practice.

Consequently, as a less intrusive measure is available that is equally effective in meeting the objective, policy option 5 is not limited to what is strictly necessary to achieve the objective. **The policy option does therefore not pass the necessity test.** The policy option shall therefore **not be assessed in terms of its proportionality**.[111]

---

[110] See the assessment of policy option 4 above.

[111] As set out in the toolkit provided by the EDPS on assessing necessity, "*only if existing or less intrusive measures are not available according to an evidence-based analysis, and only if such analysis shows that the envisaged measure is essential and limited to what is absolutely necessary to achieve the objective of general interest, this measure should proceed on to the proportionality test*". Likewise, the Commission's Operational guidance on taking account of Fundamental Rights in Commission impact assessments states that "*if it can be established that there are two policy options which are equally effective in achieving the objective but have different negative impacts on*

2. Checklist for assessing proportionality of new legislative measures

As the policy option did not pass the necessity test, therefore, it is not limited to what is strictly necessary, the policy option shall **not be assessed in terms of its proportionality**.

2.3. *Objective III*: Enabling Member States to use new technologies for law enforcement

***Policy option 6**: regulating the innovation lab at Europol, and its support to the innovation hub and the EU security research programme*

This policy option would regulate the existing innovation lab at Europol as well as Europol's support to the EU innovation hub for internal security. This regulatory intervention would provide Europol with a mandate to support Member States in countering serious crimes and terrorism by way of:

- proactively **monitoring** research and innovation activities relevant for law enforcement;
- assisting the Member States and the Commission in identifying key research themes as well as in drawing up and implementing the relevant Union framework programme (i.e. the upcoming **Horizon Europe**[112]) for research and innovation activities in the area of law enforcement, covering the entire cycle from the selection of priority, the programming of calls, the assessment of application, the implementation of projects and the application of their results; and
- implementing **pilot projects** regarding matters covered by Europol's legal mandate, covering notably the uptake of applied research (prototypes) towards deployment, and the work towards a final product available for the use by law enforcement, based on specific authorisations for each such pilot project;
- supporting the **uptake of the results of EU-financed research projects**, including by disseminating the results of that research to authorised bodies, analysing the implementation of pilot projects, and formulating general recommendations, including for technical standards for interoperability purposes and best practices. Europol may use those results as appropriate in fulfilling its support role for Member States' law enforcement authorities, subject to ethical standards, Fundamental Rights considerations and intellectual property limitations.

Europol's innovation lab would not be involved in fundamental research. Instead, the work of the **Europol innovation lab** would focus on:

- supporting (groups of) Member States in their work on innovative technologies to develop tools and provide solutions to serve the operational needs of law enforcement;
- producing technology foresight and provide assessment on the risks, threats and opportunities of emerging technologies for law enforcement;
- maintaining and using networks for outreach to industry, civil society, international organisations and academia; and

---

fundamental rights, then it is necessary to choose that option which is the least intrusive".

112 COM(2018) 435 final (7.6.2018).

- supporting the screening of specific cases of foreign direct investments that concern contract providers of technologies and software for police forces, in line with the Regulation on establishing a framework for the screening of foreign direct investments into the Union.[113]

Europol would also provide secretarial support to the **EU innovation hub for internal security** that is currently being set up among EU agencies and the Commission's Joint Research Centre, based on their existing legal mandates, to serve as a collaborative network of their innovation labs. Responding to a request by Member States in the Council, the EU innovation hub will primarily be a coordination mechanism to support the participating entities in the sharing of information and knowledge, the setting up of joint projects, and the dissemination of finding and technological solutions developed.

Option 6 does not provide for any new legal grounds for Europol for the processing of personal data. It does not limit any Fundamental Rights. The involvement of Europol in innovation and research activities related to law enforcement, and notably its support role in the management of research activities under the upcoming Horizon Europe programme, exposes Europol to the general risks implied in security research, notably risks related to ethical principles. The overall legal framework for EU security research contains the necessary safeguards to mitigate these risks.[114] These safeguard will thus also apply directly to Europol's support to the management of research activities.

Policy option 7: enabling Europol to process personal data for the purpose of innovation in areas relevant for its support to law enforcement

1. Checklist for assessing necessity of new legislative measures

Step 1: Factual description of the measure

This policy option would build on policy option 6[115] and include all aspects listed above under that policy option. It would enable Europol to **process personal data**, including large amounts of personal data, for the purpose of innovation in areas relevant for its support to law enforcement. This would include the training, testing and validation of algorithms for the development of digital tools including AI-based systems for law enforcement.

This regulatory intervention would therefore amend the purposes of data processing at Europol. Prior authorisation would be required for the processing of personal data for a specific technological application.

The policy option entails the processing of personal data as it would enable Europol to process personal data for the purpose of innovation in areas relevant for its support to Member States' law enforcement authorities. This would complement and extend the possibility provided under the current Europol Regulation to further process personal

[113] Regulation (EU) 2019/452.

[114] Under the current Horizon 2020 programme, all research and innovation activities shall comply with ethical principles and relevant national, Union and international legislation, including the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights and its Supplementary Protocols (Article 19 of Regulation (EU) 1291/2013). Procedures such as ethical screening and security scrutiny are in place to ensure compliance with these principles and legal requirements.

[115] See chapter 5 of the impact assessment.

data for historical, statistical or scientific research purposes.[116] In line with the overall objective of enabling Europol to provide effective support to Member States on the use of new technologies for law enforcement, the **purpose** of this data processing would be to train, test and validate algorithms for the development of digital tools including AI-based systems for law enforcement.

The data processing would concern **operational data** already processed by Europol under the current Europol Regulation for its objectives[117] and tasks[118] in line with the provisions[119] on Europol's purposes of information processing activities. The **categories of personal data** and the **categories of data subjects** whose data may be processed by Europol are listed in annex II of the Europol Regulation. They would remain unchanged under this sup-option.

The personal data would be processed by specifically authorised staff at Europol.

Step 2: Identification of Fundamental Rights limited by the measure

The policy options limits the Fundamental Right to the **protection of personal data** as guaranteed by Article 8 of the Charter. As the policy option entails processing by a public authority of data relating to the private life of an individual, it also limits the Fundamental Right to **respect for private life** (Article 7 of the Charter). Consequently, the policy option needs to comply with the conditions laid down in Article 52(1) of the Charter.

The policy option does **not adversely affect the essence** of the Fundamental Rights to the protection of personal data and to respect for private life.

Step 3: Definition of objectives of the measure

The policy option addresses the problem resulting from **gaps at national level on innovation and research relevant for law enforcement**, as clearly identified and described in detail in chapter 2 of the impact assessment. There are gaps at national level on innovation and research relevant for law enforcement. New technological developments offer enormous opportunities as well as considerable challenges to the EU's internal security.[120] However, Member States have sometimes difficulties in detecting and investigating crimes that are prepared or carried out with the support of new technologies. At the same time, they are not able to exploit fully the advantages of new technologies for fighting serious crime and terrorism.

The policy option aims to achieve the specific objective of **enabling Europol to provide effective support to Member States on the use of new technologies for law enforcement**, as precisely defined in chapter 4 of the impact assessment. The policy option therefore falls within the scope of the fight against serious crime and terrorism which are recognised as objectives of general interest in EU law.

Step 4: Choice of option that is effective and least intrusive

116 Article 28(1)(b) of Regulation (EU) 2016/794.
117 Article 3 of Regulation (EU) 2016/794.
118 Article 4 of Regulation (EU) 2016/794.
119 Article 18 of Regulation (EU) 2016/794.
120 These include developments such as 5G mobile networks, artificial intelligence, the internet of things, drones, anonymisation and encryption, 3D printing and biotechnology.

The policy option is **genuinely effective** as it is essential to achieve the specific objective of enabling Europol to provide effective support to Member States on the use of new technologies for law enforcement, and therefore the fight against serious crime and terrorism as objectives of general interest in EU law.

The processing of personal data to train, test and validate algorithms for the development of digital tools including AI-based systems for law enforcement **effectively contributes to achieve the objective** of enabling Europol to provide effective support to Member States on the use of new technologies for law enforcement. It would enable Europol to develop effective digital tools for law enforcement and make those tools available to Member States, thus allowing Member States to use the opportunities offered by innovation and research for law enforcement.

The policy option addresses the problem resulting from gaps at national level on innovation and research relevant for law enforcement **more effectively** than policy option 6. Indeed, policy option 6 is less intrusive as it does not provide for the processing of personal data, but it is insufficient to address the problem. The use of AI and algorithms in the area of law enforcement needs testing, as highlighted in the European ethical Charter on the use of artificial intelligence in judicial systems.[121] For this testing to be effective, the processing of personal data is necessary. Without testing on real data, an algorithm cannot produce results that are sufficiently precise.

Existing rules on the processing of personal data by Europol for statistical or scientific research purposes are too general and therefore **insufficient** to address the problem, even if their application is reinforced.

Consequently, the policy option is **essential and limited** to what is absolutely necessary to achieve the specific objective of enabling Europol to provide effective support to Member States on the use of new technologies for law enforcement, and hence the fight against serious crime and terrorism as objectives of general interest in EU law.

2. Checklist for assessing proportionality of new legislative measures

Step 1: Importance of the objective and whether the measure meets the objective

The policy option addresses the problem resulting from **gaps at national level on innovation and research relevant for law enforcement**. The problem and its drivers are described in detail in chapter 2 of the impact assessment. There are gaps at national level on innovation and research relevant for law enforcement. New technological developments offer enormous opportunities as well as considerable challenges to the EU's internal security.[122] However, Member States have sometimes difficulties in detecting and investigating crimes that are prepared or carried out with the support of new technologies. At the same time, they are not able to exploit fully the advantages of new technologies for fighting serious crime and terrorism.

As set out in chapter 2 of the impact assessment, there is indeed a **need to address the problem** as it will otherwise increase, given that criminals have proven very effective in

[121] European Commission for the Efficiency of Justice of the Council of Europe: European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment (3-4.12.2018).

[122] These include developments such as 5G mobile networks, artificial intelligence, the internet of things, drones, anonymisation and encryption, 3D printing and biotechnology.

exploiting the opportunities offered by new technologies. There is indeed a pressing social need to enable law enforcement authorities keep abreast of technological developments and their misuse by criminals.

The policy option and its purpose of enabling Europol to process personal data for the purpose of innovation in areas relevant for its support to Member States' law enforcement authorities **correspond to the identified need and solves the problem**. The policy option is effective and efficient to fulfil the objective.

Step 2: Assessment of the scope, the extent and the intensity of the interference

The policy option affects persons whose personal data is processed by Europol in accordance with its existing tasks and objectives, as this personal data would also be processed to train, test and validate algorithms for the development of digital tools including AI-based systems for law enforcement.

Given the processing of personal data for the development of algorithms, the policy option risks having a harmful effect on the Fundamental Right to **non-discrimination** (Article 21 of the Charter).[123] This risk might even increase with the use of low data quality.[124] Moreover, Europol would use part of its operational data for the development of algorithms, and such law enforcement data was collected for the purposes of crime fighting and is not representative for the entire population. The use of such specific data for the development of algorithms might entail the risk of biased results. These risks will be mitigated with the introduction of necessary safeguards in step 4.

The policy option restricts the Fundamental Rights of the data subjects by processing their personal data for the training, testing and validating of algorithms. This would **not include the processing of special categories** of data.

As part of the training, testing and validating of algorithms, the processing of personal data amounts to **profiling** of individuals. This needs to be accompanied with the necessary safeguards.

The policy option does **not impose a disproportionate and excessive burden** on the persons affected by the limitation (i.e. persons for whom Europol processes information in accordance with its existing tasks and objective) in relation to the specific objective of enabling Europol to provide effective support to Member States on the use of new technologies for law enforcement, and hence to the objectives of fighting serious crime and terrorism as objectives of general interest in EU law.

Step 3: 'Fair balance' evaluation of the measure

Weighing up the intensity of the interference with the Fundamental Rights to the protection of personal data and to respect for private life as described under step 3 with the legitimacy of the objectives to fight against serious crime and terrorism as objectives of general interest in EU law, the policy option constitutes a **proportionate response** to the need to solve the problem resulting from gaps at national level on innovation and

123 EU Agency for Fundamental Rights: #BiGData: Dicrimination in data-supported decision making (2018).

124 EU Agency for Fundamental Rights: Data quality and artificial intelligence – mitigating bias and error to protect Fundamental Rights (2019).

research relevant for law enforcement.[125]

The fundamental data protection principles – especially purpose limitation and minimisation – should be interpreted in such a way that they do not exclude the use of personal data for machine learning purposes.[126] They should not preclude the creation of training sets and the construction of algorithmic models, whenever the resulting AI systems are socially beneficial and compliant with data protection rights.

However, in order to establish a balance between the extent and nature of the interference and the reasons for interfering as translated into the objective of enabling Europol to provide effective support to Member States on the use of new technologies for law enforcement, a **number of safeguards are necessary** (see step 4).

Step 4: Identification and introduction of safeguards

A **number of safeguards are necessary** in order to establish a balance between the extent and nature of the interference and the reasons for interfering as translated into the objective of enabling Member States to use new technologies for law enforcement:

- Requirement to conduct a **fundamental rights impact assessment**[127] prior to any training, testing and validation of algorithms for the development of digital tools including AI-based systems for law enforcement:
  - assessing necessity and proportionality separately for each application;
  - ensuring compliance with ethical standards;
  - identifying potential biases in the operational data to be used for the development of algorithms, including an assessment of the potential for discrimination;
  - identifying potential biases and abuses in the application of and output from algorithms, including an assessment of the potential for discrimination; and
  - requiring prior authorisation of for each application, taking into account risk of biased outcomes resulting from the use of law enforcement data.
- Requirement to ensure the **quality of the data**[128] used for the training, testing and validation of algorithms: while it may be challenging to assess the quality of all data used for building algorithms, it is essential to collect metadata and make quality assessments of the correctness and generalizability of the data.
- Requirement to ensure **separate data processing environment**:
  - separating the processing for training, testing and validation of algorithms from any processing of personal data for the operational tasks of

[125] See the study of the European Parliamentary Research Service on The impact of the General Data Protection Regulation (GDPR) on artificial intelligence (June 2020): "*In general, the inclusion of a person's data in a training set is not going to affect to a large extent that particular person, since the record concerning a single individual is unlikely to a make a difference in a model that is based in a vast set of such records. However, the inclusion of a single record exposes the data subject to risks concerning the possible misuse of his or her data, unless the information concerning that person is anonymised or deleted once the model is constructed.*"

[126] Study of the European Parliamentary Research Service on The impact of the General Data Protection Regulation (GDPR) on artificial intelligence (June 2020)

[127] EU Agency for Fundamental Rights: #BiGData: Dicrimination in data-supported decision making (2018).

[128] EU Agency for Fundamental Rights: Data quality and artificial intelligence – mitigating bias and error to protect Fundamental Rights (2019).

objectives of Europol;
- setting out clear criteria, and requiring specific authorisation, for the temporary transfer of data from the operational data processing environment to the separate data processing environment for the development of algorithms, based on strict necessity;
- limiting the access to the separate data processing environment to specifically authorised staff of Europol;
- deleting the outcome of the processing of personal data for training, testing and validation of algorithms once the digital tool is validated.[129]

- Requirement to keep the **data retention rules** and periods applicable: re-purposing the data does not result in the prolongation or re-initiation of the retention periods. Therefore, any technical solution must ensure the timely and automatic deletion of data used for the development of algorithms once the retention period of the corresponding data in the operational environment ends.
- Requirement to ensure that data processed for training, testing and validation of algorithms is **not used to support measures or decisions regarding individuals**:[130] avoiding any use of the personal data for predictions or decisions concerning individuals.
- Requirement to embed **lawfulness 'by design' and 'by default'**:[131]
  - limiting the processing of different types of personal data to what is strictly necessary for a specific purpose, e.g. processing anonymised and pseudonymised data for the development of algorithms;
  - processing of full data for testing in an operational scenario.
- Requirement to ensure **transparency** about the way the algorithm was built and operates, including a general description of the process and rationale behind the calculations feeding the decision making, and possible biases resulting from the data used: facilitating access for remedies for people who challenge subsequent data-supported decisions taken on the basis of the algorithm.[132]
- Requirement to avoid the use of artificial intelligence where certain uses of the technology are **evidently incompatible with Fundamental Rights**:[133] applying a cautious and risk-adapted approach by completely or partially banning algorithmic systems with an untenable potential for harm.[134]

2.4. *Objective of annex 6*: Providing frontline officers (police officers and border guards) with the result of the analysis of data received from third countries

Policy option 8: enabling Europol to issue 'discreet check' alerts in the Schengen Information System

[129] European Parliamentary Research Service: The impact of the General Data Protection Regulation (GDPR) on artificial intelligence (June 2020).
[130] European Data Protection Supervisor: A Preliminary Opinion on data protection and scientific research (6.1.2020).
[131] EU Agency for Fundamental Rights: Preventing unlawful profiling today and in the future: a guide (2018).
[132] EU Agency for Fundamental Rights: #BiGData: Dicrimination in data-supported decision making (2018).
[133] European Data Protection Supervisor: EDPS opinion on the European Commission's White Paper on Artificial Intelligence – A European approach to excellenec and trust (29.6.2020).
[134] Data Ethics Commission: Opinion of the Data Ethics Commission (22.1.2020).

1. Checklist for assessing necessity of new legislative measures

Step 1: Factual description of the measure

Policy option 8 would enable Europol to issue alerts on persons in the Schengen Information System, using so-called **"discreet check" alerts** as existing alert category.[135] Europol would be able to issue such alerts on suspects and criminals in certain specific and well-defined cases and circumstances, and within the scope of crimes falling under Europol's competence.[136] When Member States' frontline officers encounter the person subject to the alert in the context of a check at the EU's external border or within the Schengen area, they would be required to discreetly collect as much information as possible from the person on the circumstances of the hit without making the person aware of the existence of the alert.

The policy option entails the processing of personal data as it foresees the possibility for Europol to issue 'discreet check' alerts[137] in the Schengen Information System. The **overall objective** is to provide frontline officers (police officers and border guards) with the result of the analysis of data received from third countries when and where this is necessary. The underlying goal is to enable frontline officers to take informed decisions when they check a person at the external border or within Schengen area.

In line with that objective, the **purpose of the data processing** is to inform frontline officers, when they checking a person on which Europol issued an alert, about information the agency holds on that person. The alert would inform the frontline officers that the information held by Europol indicates that this person intends to commit or is committing one of the offences falling under Europol's competence, or that an overall assessment of the information available to Europol gives reason to believe that the person may commit such offence in future. The alert would therefore enable the frontline officers to take informed decisions.

As established under the rules governing the issuing of 'discreet check' alerts in the Schengen Information System, the policy option provides for the **processing of information on persons in relation to whom an alert has been entered**.[138] It provides for the processing of personal data of persons for whom Europol holds information indicating that these persons intend to commit or are committing one of the offences falling under Europol's competence, or that an overall assessment of the information available to Europol gives reason to believe that these persons may commit such offence in future. The personal data would be processed by Europol when issuing the alert, and by the frontline officers of national authorities when they check the person subject to the alert at the EU external border or within the Schengen area, thus creating a 'hit'. The executing authority (i.e. the authority of the Member State where the 'hit' occurred)

---

135 Article 36 of Regulation (EU) 2018/1862.

136 In line with Article 36 of Regulation (EU) 2018/1862, this would cover persons where there is a clear indication that they intend to commit or are committing any of the crimes for which Europol is competent, or persons where an overall assessment (in particular on the basis of past criminal offences) gives reasons to believe that they may commit in future one of the crimes for which Europol is competent.

137 Article 36 of Regulation (EU) 2018/1862.

138 See Article 20 of Regulation (EU) 2018/1862. Any alert in SIS which includes information on persons shall contain only a limited set of data clearly identified in that Article, including surnames; forenames; names at birth; previously used names and aliases; any specific, objective, physical characteristics not subject to change; place of birth; date of birth; gender; any nationalities held.

would inform Europol about the 'hit' and would be required to discreetly check the person concerned and collect a certain set of detailed information from the person if they encounter him or her at the external border or within the Schengen territory. Moreover, the executing authority and Europol might subsequently exchange supplementary information via the SIRENE network.[139]

Step 2: Identification of Fundamental Rights limited by the measure

The policy option limits the Fundamental Right to the **protection of personal data** as guaranteed by Article 8 of the Charter. As the policy option entails the processing by a public authority of data relating to the private life of an individual, it also limits the Fundamental Right to **respect for private life** (Article 7 of the Charter). Consequently, the policy option needs to comply with the conditions laid down in Article 52(1) of the Charter.

The policy option does **not adversely affect the essence** of the Fundamental Rights to the protection of personal data and to respect for private life.

Step 3: Definition of objectives of the measure

The policy option addresses the **problem** of limits in the direct sharing of information resulting from the analysis of third-country sourced data on suspects and criminals. More specifically, it addresses Europol's ability to share promptly its analysis with frontline officers in the Member States (police officers and border guards) when and where they need it, notably Europol's analysis of data it received from third countries on suspects and criminals. Chapter 2 of the impact assessment clearly identifies the problem and describes in detail. While the information that third countries share with the EU is increasingly relevant for EU internal security, there are limits in the sharing of that information within the EU. This is notably the case for Europol's analysis of data it received from third countries on suspects and criminals.[140] Consequently, Member States' frontline officers might have insufficient information available when they check a person at the external border or within the Schengen area. This problem arises in the context of on-going efforts to detect foreign terrorist fighters, but also on persons involved in organised crime (e.g. drugs trafficking) or serious crime (e.g. child sexual abuse).

The policy option aims to achieve the **specific objective** to provide frontline officers (police officers and border guards) with the result of the analysis of data received from third countries when and where this is necessary, as precisely defined in chapter 4 of the impact assessment. The policy option therefore falls within the scope of the fight against serious crime and terrorism which are recognised as **objectives of general interest** in EU law.

Step 4: Choice of option that is effective and least intrusive

---

139 SIRENE stands for "Supplementary Information Request at the National Entries". Each Member State operating the Schengen Information System has set up a national SIRENE Bureau, operational 24/7, that is responsible for any supplementary information exchange and coordination of activities connected to alerts.

140 In this context, the reference to '*suspects and criminals*' covers: (a) Persons who are suspected of having committed or having taken part in a criminal offence in respect of which Europol is competent, or who have been convicted of such an offence. (b) Persons regarding whom there are factual indications or reasonable grounds to believe that they will commit criminal offences in respect of which Europol is competent.

The policy option is **genuinely effective** as it achieves the specific objective of providing frontline officers (police officers and border guards) with the result of the analysis of data received from third countries when and where this is necessary, and therefore the fight against serious crime and terrorism as objectives of general interest in EU law.

The processing of personal data by way of the issuing of 'discreet check' alerts by Europol in the Schengen Information System, and the subsequent 'hit' with such an alert when a frontline officer checks the person concerned against the Schengen Information System, **effectively contributes to achieve the objective**.

Existing possibilities to enhance the availability of Europol data to end-users, notably the roll-out of QUEST[141], are insufficient to address the problem, even if their implementation and application is reinforced.[142] QUEST facilitates the access and use of Europol's databases by investigators, criminal intelligence officers and analysts in the Member States, but not by frontline officers as the actual target group of objective identified. Likewise, Europol existing cooperation with Member States, where the agency encourages national authorities to issue alerts in the Schengen Information System, is insufficient to address the problem. This existing practice is not transparent, it raises legal concerns (e.g. on responsibility and liability), and it causes operational difficulties (in case of a 'hit' on such an alert issued by a Member State, the underlying analysis held by Europol would be needed for an effective follow up).

Existing or planned EU information systems do also not address sufficiently the problem identified:

- **passenger name record data**[143] is not directly available to frontline officers;
- the **EU Entry/Exit System**[144] will register travellers from third-countries, both short-stay visa holders and visa exempt travellers, each time they cross an EU external border. While Europol will be able to access the system under for specific purposes and under strict conditions, the system will not enable Europol to share its information on suspects and criminals with frontline officers;
- the **European Travel Information and Authorisation System** (ETIAS)[145] will help identifying security risks posed by visa-exempt visitors travelling to the Schengen area. After filling in an online application form, the system will conduct checks against EU information systems for security, including an ETIAS watchlist. Europol will be able to enter data into the ETIAS watchlist to provide Member States with information it holds related to persons who are suspected of having committed or having taken part in a terrorist offence or other serious criminal offence, or regarding whom there are factual indications or reasonable grounds to believe that they will commit a terrorist offence or other serious criminal offences. ETIAS will however not support the work of frontline officers within the Schengen area in case they check a person who entered the EU irregularly. In addition, contrary to the Schengen Information System, ETIAS does not contain biometrics or detailed identity information on persons of interest

141 QUEST (QUerying Europol SysTems) is a system interface that allows integrating automatic queries to Europol databases from national police information systems in the Member States.
142 See annex VII on policy options discarded at an early stage.
143 Directive (EU) 2016/681 (27.4.2016).
144 REGULATION (EU) 2017/2226 (30.11.2017).
145 Regulation (EU) 2018/1240 (12.9.2018).

subject to an alert. Finally, while ETIAS provides for the possibility to refuse a travel authorisation if the legal grounds for such a refusal are fulfilled, it does not allow for other security-related measures such as the monitoring of travel movements.

- the proposed upgrading of the **Visa Information System**[146] foresees that personal data contained in visa applications will be compared with Europol data. However, such comparisons will be limited to persons applying for a visa. The upgrade Visa Information System will not support the work of frontline officers within the Schengen area in case they check a person who entered the EU irregularly. Finally, while the Visa Information System provides for the possibility to refuse a visa if the legal grounds for such a refusal are fulfilled, it does not allow for other security-related measures such as the monitoring of travel movements.

The policy option addresses the problem **equally effective** as policy option 9 on introducing a new alert category in the Schengen Information System for Europol.[147] However, policy option 9 establishes a new alert category in the Schengen Information System that would be exclusively used by Europol, which would provide the opportunity to set out specific provisions and safeguards to be fulfilled by Europol upon entering such alert in the Schengen Information System. In addition, policy option 9 is **less intrusive** as it does not oblige the frontline officer to carry out a 'discreet check' as foreseen under policy option 8, which would imply discreetly collecting as much additional information as possible on the person subject to the alert and the circumstances of the hit (see below on policy option 9). Instead, under policy option 9, the frontline officer would need to report immediately the occurrence of the hit to the national SIRENE Bureau which would contact Europol, and, as a further follow-up action, could get further background information from Europol through the SIRENE network.[148] Beyond this reporting obligation as a non-coercive measure, there would be no further obligation on the Member States where the 'hit' occurred. Instead, with relevant national authorities of the Member State concerned would need to determine, on a case-by-case basis, including based on the background information provided by Europol, whether further measures need to be taken with regard to the person. Such further measures would take place under national law and the full discretion of the Member State. This provides for the possibility of less intrusive consequences for the data subject.

Consequently, as a less intrusive measure is available that is equally effective in meeting the objective, policy option 8 is not limited to what is strictly necessary to achieve the objective. **The policy option does therefore not pass the necessity test.** The policy option shall therefore **not be assessed in terms of its proportionality**.[149]

---

146 COM(2018) 302 final (16.5.2018).

147 See the assessment of policy option 9 below.

148 SIRENE stands for "Supplementary Information Request at the National Entries". Each Member State operating the Schengen Information System has set up a national SIRENE Bureau, operational 24/7, that is responsible for any supplementary information exchange and coordination of activities connected to alerts.

149 As set out in the toolkit provided by the EDPS on assessing necessity, "*only if existing or less intrusive measures are not available according to an evidence-based analysis, and only if such analysis shows that the envisaged measure is essential and limited to what is absolutely necessary to achieve the objective of general interest, this measure should proceed on to the proportionality test*". Likewise, the Commission's Operational guidance on taking account of Fundamental Rights in Commission impact assessments states that "*if it can be established that there are two policy options*

2. Checklist for assessing proportionality of new legislative measures

As the policy option did not pass the necessity test, and therefore is not limited to what is strictly necessary, the policy option shall **not be assessed in terms of its proportionality**.

Policy option 9: introducing a new alert category in Schengen Information System to be used exclusively by Europol

1. Checklist for assessing necessity of new legislative measures

Step 1: Factual description of the measure

Policy option 9 would introduce a **new alert category** in the Schengen Information System exclusively for Europol, namely a so-called "information alert", with specific requirements and safeguards reflecting Europol's role. In case of a 'hit', the alert would inform the frontline officer that Europol holds information on the person. More specifically, the alert would inform that Europol holds information indicating that this person intends to commit or is committing one of the offences falling under Europol's competence, or that an overall assessment of the information available to Europol gives reason to believe that the person may commit such offence in future. In reaction to that, the frontline officer would need to report immediately the occurrence of the 'hit' to the national SIRENE Bureau, which would contact Europol, and, as a further follow-up action, could get further background information from Europol through the SIRENE channel. Beyond this reporting obligation as a non-coercive measure, there would be no further obligation on the Member States where the 'hit' occurred. Instead, the relevant national authorities of the Member State concerned would need to determine, on a case-by-case basis, including based on the background information provided by Europol whether further measures need to be taken with regard to the person. Such further measures would take place under national law and the full discretion of the Member State.

The policy option entails the **processing of personal data** as it foresees the possibility for Europol to issue a new and dedicated alert category ('information alert') in the Schengen Information System.

The **overall objective** is to provide frontline officers (police officers and border guards) with the result of the analysis of data received from third countries when and where this is necessary. The underlying goal is to enable frontline officers to take informed decisions when they check a person at the external border or within Schengen area.

In line with that objective, the **purpose of the data processing** is to inform frontline officers, when checking a person on which Europol issued an alert, about information the Agency holds on that person. The alert would inform the frontline officers the information held by Europol indicates that this person intends to commit or is committing one of the offences falling under Europol's competence, or that an overall assessment of the information available to Europol gives reason to believe that the person may commit such offence in future. The alert would therefore enable the frontline officers to take informed decisions.

---

which are equally effective in achieving the objective but have different negative impacts on fundamental rights, then it is necessary to choose that option which is the least intrusive".

In terms of processing of personal data, the new alert category ('information alert') would lay down a specifically defined set of rules governing the issuing of alerts in the Schengen Information System. In that respect, the policy option provides for the **processing of information on persons in relation to whom an alert has been entered**.[150] It provides for the processing of personal data of persons for whom Europol holds information indicating that these persons intend to commit or are committing one of the offences falling under Europol's competence, or that an overall assessment of the information available to Europol gives reason to believe that these persons may commit such offence in future. The personal data would be processed by Europol when issuing the alert and by the frontline officers of national authorities when they check the person subject to the alert at the EU external border or within the Schengen area, thus creating a 'hit'. The executing authority (i.e. the authority of the Member State where the 'hit' occurred) would inform Europol about the 'hit'. Moreover, the executing authority and Europol might subsequently exchange supplementary information via the SIRENE channel.

Step 2: Identification of Fundamental Rights limited by the measure

The policy option limits the Fundamental Right to the **protection of personal data** as guaranteed by Article 8 of the Charter. As the policy option entails the processing by a public authority of data relating to the private life of an individual, it also limits the Fundamental Right to **respect for private life** (Article 7 of the Charter). Consequently, the policy option needs to comply with the conditions laid down in Article 52(1) of the Charter.

The policy option does **not adversely affect the essence** of the Fundamental Rights to the protection of personal data and to respect for private life.

Step 3: Definition of objectives of the measure

The policy option addresses the problem of **limits in the direct sharing of data resulting from the analysis of third-country sourced information**. More specifically, it addresses Europol's ability to share promptly its analysis with frontline officers in the Member States (police officers and border guards) when and where they need it, notably Europol's analysis of data it received from third countries. Chapter 2 of the impact assessment clearly identifies the problem and describes in detail. While the information that third countries share with the EU is increasingly relevant for EU internal security, there are limits in the sharing of that information within the EU. This is notably the case for Europol's analysis of data it received from third countries on suspects and criminals.[151] Consequently, Member States' frontline officers might have insufficient information available when they check a person at the external border or within the Schengen area. This problem arises in the context of on-going efforts to detect foreign

---

150 See Article 20 of Regulation (EU) 2018/1862. Any alert in SIS which includes information on persons shall contain only a limited set of data clearly identified in that Article, including surnames; forenames; names at birth; previously used names and aliases; any specific, objective, physical characteristics not subject to change; place of birth; date of birth; gender; any nationalities held.

151 In this context, the reference to '*suspects and criminals*' covers: (a) Persons who are suspected of having committed or having taken part in a criminal offence in respect of which Europol is competent, or who have been convicted of such an offence. (b) Persons regarding whom there are factual indications or reasonable grounds to believe that they will commit criminal offences in respect of which Europol is competent.

terrorist fighters, but also on persons involved in organised crime (e.g. drugs trafficking) or serious crime (e.g. child sexual abuse).

The policy option aims to achieve the specific objective to **providing frontline officers (police officers and border guards) with the result of the analysis of data received from third countries**, as precisely defined in chapter 4 of the impact assessment. The policy option therefore falls within the scope of the fight against serious crime and terrorism which are recognised as objectives of general interest in EU law.

Step 4: Choice of option that is effective and least intrusive

The policy option is **genuinely effective** as it is essential to achieve the specific objective of providing frontline officers (police officers and border guards) with the result of the analysis of data received from third countries when and where this is necessary, and therefore the fight against serious crime and terrorism as objectives of general interest in EU law.

The processing of personal data by way of the issuing of a new and dedicated alert category ('information alert') by Europol in the Schengen Information System, and the subsequent 'hit' with such an alert when a frontline officer checks the person concerned against the Schengen Information System, **effectively contributes to achieve the objective**.

As set out above, **existing possibilities** to enhance the availability of Europol data to end-users, are insufficient to address the problem, even if their implementation and application is reinforced.[152]

The policy option addresses the problem **equally effective** as policy option 8 on enabling Europol to issue existing "discreet check" alerts in the Schengen Information System. However, policy option 9 establishes a new alert category that would be exclusively used by Europol, which would provide the opportunity to set out specific provisions and safeguards to be fulfilled by Europol upon entering such alert in the Schengen information System. In addition, policy option 9 is **less intrusive** compared to policy option 8. It does not oblige the frontline officer to carry out a 'discreet check' as foreseen under policy option 8, which would imply discreetly collecting as much additional information as possible on the person subject to the alert and the circumstances of the hit. Instead, under policy option 9, the frontline officer would need to report immediately the occurrence of the hit to the national SIRENE bureau which would contact Europol, and, as a further follow-up action, could get further background information from Europol through the SIRENE channel. Beyond this reporting obligation as a non-coercive measure, there would be no further obligation on the Member States where the 'hit' occurred. Instead, the relevant national authorities of the Member State concerned would need to determine, on a case-by-case basis, including based on the background information provided by Europol whether further measures need to be taken with regard to the person. Such further measures would take place under national law and the full discretion of the Member State. This provides for the possibility of less intrusive consequences for the data subject.

Consequently, the policy option is **essential and limited to what is strictly necessary** to achieve the specific objective of providing frontline officers (police officers and border

[152] See above the assessment of policy option 8.

guards) with the result of the analysis of data received from third countries, and hence to fight serious crime and terrorism as objectives of general interest in EU law.

2. Checklist for assessing proportionality of new legislative measures

Step 1: Importance of the objective and whether the measure meets the objective

The policy option addresses the problem of **limits in the direct sharing of data resulting from the analysis of third-country sourced information**. More specifically, it addresses Europol's ability to share promptly its analysis with frontline officers in the Member States (police officers and border guards) when and where they need it, notably Europol's analysis of data it received from third countries. The problem and its drivers are described in detail in chapter 2 of the impact assessment. While the information that third countries share with the EU is increasingly relevant for EU internal security, there are limits in the sharing of that information within the EU. This is notably the case for Europol's analysis of data it received from third countries on suspects and criminals.[153] Consequently, Member States' frontline officers might have insufficient information available when they check a person at the external border or within the Schengen area. This problem arises in the context of on-going efforts to detect foreign terrorist fighters, but also on persons involved in organised crime (e.g. drugs trafficking) or serious crime (e.g. child sexual abuse).

As set out in chapter 2 of the impact assessment, there is indeed a **need to address the problem** as it will otherwise increase, notably in the context of the threat posed by foreign terrorist fighters.[154]

The policy option and its purpose of enabling Europol to issue a new and dedicated alert category in the Schengen Information System ('information alert') **correspond to the identified need**. They solve the problem resulting from limits in Europol's ability to share promptly its analysis with frontline officers in the Member States. The policy option is **effective and efficient** to fulfil the objective.

Step 2: Assessment of the scope, the extent and the intensity of the interference

The policy option **affects persons** for whom Europol holds information indicating that the person intends to commit or is committing one of the offences falling under Europol's competence, or that an overall assessment of the information available to Europol gives reason to believe that the person may commit such offence in future.

There may be a **potential harmful effect** of the policy option on the Fundamental Right to liberty and security (Article 6 of the Charter), to the extent that a third country might try to encourage Europol to issue an alert based on political, military, religious or racial

153 In this context, the reference to '*suspects and criminals*' covers: (a) Persons who are suspected of having committed or having taken part in a criminal offence in respect of which Europol is competent, or who have been convicted of such an offence. (b) Persons regarding whom there are factual indications or reasonable grounds to believe that they will commit criminal offences in respect of which Europol is competent.

154 Europol's Terrorism Situation and Trend report (TESAT) of June 2020 states that while many foreign terrorist fighters are believed to have been either killed or confined in detention or refugee camps in north-eastern Syria, there are a substantial number of EU foreign terrorist fighters still unaccounted for. According to the report, chaos and lack of information from the conflict zone have resulted in the information available to Member States about foreign terrorist fighters being limited and unverifiable.

reasons.[155] There may also be a potential harmful effect of the policy option on the principle of *non-refoulement* as encompassed in Articles 18 and 19 of the Charter.[156] An information alert by Europol might contribute to the decision of a border guard to refuse entry to the person subject to the alert, thus affecting the access to international protection at the EU external border. These risks will be mitigated with the introduction of necessary safeguards in step 4.

The policy option restricts the Fundamental Rights of the data subjects by the issuing of 'information alert' in which Europol sets out personal data that enables the frontline officer to identify the person during (1) a border check at the EU external border (where the cross-checking of each person against the Schengen Information System is obligatory); or (2) an on-spot police check within the Schengen territory (where the cross-checking against the Schengen Information System is recommended but not obligatory).

In line with the existing rules on the Schengen Information System,[157] the alert shall be kept only for the time required to achieve the purpose for which it was entered (more details are set out in step 4 on safeguards).

The issuing of an 'information alert' in the Schengen Information System does not require the processing of special categories of data.

The issuing of alerts in the Schengen Information System does not amount to profiling of the individual and does not entail the use of automated decision making.

The policy option does **not impose a disproportionate nor an excessive burden** on the persons affected by the limitation (i.e. persons for whom Europol holds information indicating that the person intends to commit or is committing one of the offences falling under Europol's competence, or that an overall assessment of the information available to Europol gives reason to believe that the person may commit such offence in future) in relation to the specific objective of providing frontline officers with the information they need, and hence to the objectives of fighting serious crime and terrorism as objectives of general interest in EU law.

Step 3: 'Fair balance' evaluation of the measure

Weighing up the intensity of the interference with the Fundamental Rights to the protection of personal data and to respect for private life as described under step 3 with the legitimacy of the objectives to fight against serious crime and terrorism as objectives of general interest in EU law, the policy option constitutes a **proportionate response** to the need to solve the problem resulting from limits in Europol's ability to share promptly its analysis with frontline officers in the Member States when and where they need it.

However, in order to establish a balance between the extent and nature of the interference and the reasons for interfering as translated into the objective of providing frontline officers (police officers and border guards) with the result of the analysis of data received from third countries when and where this is necessary, a **number of safeguards are**

155 See p. 19 of the Opinion of the EU Agency for Fundamental Rights: Interoperability and Fundamental Rights implications (11.4.2018).

156 Fundamental Rights Agency: Guidance on how to reduce the risk of refoulement in external border management when working in or together with third countries (2016).

157 Article 53 of Regulation (EU) 2018/1862.

necessary (see step 4).

Step 4: Identification and introduction of safeguards

A **number of safeguards are necessary** in order to establish a balance between the extent and nature of the interference and the reasons for interfering as translated into the objective of providing frontline officers (police officers and border guards) with the result of the analysis of data received from third countries:

- All **safeguards** set out in the rules applicable to the Schengen Information System[158] would also need to apply to alerts issued by Europol, and would be reflected in the revised Europol Regulation where needed.
- The revised Europol Regulation and Schengen Information System Regulation would need to limit the issuing of alerts by Europol to what is **strictly necessary**. Europol would not be allowed to issue alerts in SIS on third country nationals residing in an EU Member State. When Europol receives data on non-third country nationals from a third country, it would instead contact the Member State concerned directly and not issue an alert in SIS. In such cases, it would be up to the Member State of nationality to assess whether issuing an alert in the Schengen Information System is necessary and proportionate.
- In addition, with regard to data on third country nationals, there is a need for preparatory steps and a **prior consultation of all Member States** by Europol before issuing an alert in the Schengen Information System. As a first step, Europol should verify if there is an alert already issued on the person in the Schengen Information System, in which case no second alert should be issues. Second, a prior consultation with the Member States should be launched, informing about the data Europol received from third countries. These steps would ensure that:
    - no Member State has already issued an alert on the person;
    - no Member State intends to issue an alert on the person (also in light of the data available to Europol);
    - no Member State otherwise objects to the issuing of an alert by Europol, e.g. for reasons of national security.
- Consequently, the **personal scope of the alerts** would be limited to third country nationals not residing in the EU in respect of whom no alert in the Schengen Information System has been issued by any Member State and where Member States have no objection to the issuing of an alert.
- The revised Europol Regulation and Schengen Information System Regulation would need to set clearly the **conditions, requirements and safeguards** under which Europol would issue 'information alerts' in the Schengen Information System. This would include the analysis that Europol would need to undertake prior to issuing an alert to verify the quality and reliability of the data it received, and to enrich the data with information it holds in its databases on the person concerned. Moreover, given that this policy option would lead to the establishment of a dedicated alert category in the Schengen Information System for exclusive use by Europol, the respective limitations and safeguards for this alert category in the legal basis of the Schengen Information System would be tailored to the situation of Europol and to what is strictly necessary.

[158] Regulation (EU) 2018/1862.

- Alerts issued by Europol would be kept only for the time that is strictly necessary to achieve the purpose for which they were entered. In analogy with the existing rules applicable to the Schengen Information System,[159] Europol may enter an alert **for a period of one year**, with the obligation to review the need to retain the alert within the one-year period.
- The revised Europol Regulation and Schengen Information System Regulation would need to **restrict the number of persons** authorised to issue alerts in the Schengen Information System and to access the information received in case of a 'hit' from the Member State concerned to what is strictly necessary.
- In analogy with the existing rules applicable to the Schengen Information System[160], Europol would need the prior consent of the Member State in which the hit occurred to **transfer data** resulting from a 'hit' with its alerts **to third countries** or international organisations.
- The revised Europol Regulation would need to ensure the possibility for an individual to **pursue legal remedies**, implementing all related provisions in the rules applicable to the Schengen Information System,[161] and building on the related provisions in the current Europol Regulation.[162]

159 See Article 53(4) of Regulation (EU) 2018/1862.
160 See Article 65 of Regulation (EU) 2018/1862.
161 See Regulation (EU) 2018/1862, notably: Article 67 on Right of access, rectification of inaccurate data and erasure of unlawfully stored data; Article 68 on Remedies; Article 72 on Liability.
162 Chapter VII of Regulation (EU) 2016/794.

Annex 6: Europol and the Schengen Information System

1. PROBLEM DEFINITION

1.1. What is the problem?

Crime and terrorism operate across borders, as criminals and terrorists exploit the advantages that globalisation and mobility bring about. Consequently, the information that third countries share with the EU about criminals and terrorists is increasingly relevant for EU internal security, notably at the EU external border. However, there are currently limits in the sharing of third-country sourced information on suspects and criminals within the EU. [163] More specifically, there are **limits in the sharing of third-country sourced information with frontline officers in the Member States** (police officers and border guards) when and where they need it.

For example, this **problem arises in the context of on-going efforts to detect foreign terrorist fighters**. Europol's Terrorism Situation and Trend report[164] of June 2020 states that while many foreign terrorist fighters are believed to have been either killed or confined in detention or refugee camps in north-eastern Syria, there are a substantial number of foreign terrorist fighters still unaccounted for. According to the report, chaos and lack of information from the conflict zone have resulted in the information available to Member States about foreign terrorist fighters being limited and unverifiable. Likewise, the June 2020 Council Conclusions on EU external action on preventing and countering terrorism and violent extremism recognise that "*foreign terrorist fighters will remain a major common security challenge for the years to come*", calling for enhanced and timely cooperation and information sharing among Member States, with Europol and other relevant EU actors.[165]

However, Europol estimates that currently **information on approximately 1000 non-EU foreign terrorist fighters**, provided by trusted third countries to Europol and individual Member States, **has not been inserted into the Schengen Information System**. As the most widely used information-sharing database in the EU, the Schengen Information System provides frontline officers with access to alerts on persons and objects, including alerts on suspects and criminals. In the absence of alerts in the Schengen Information System on the 1000 non-EU foreign terrorist fighters, there is a risk that border guards do not detect them when they seek to enter the EU, or when police officers check them within the Schengen area. This constitutes a considerable security gap.

In that respect, the June 2018 Council Conclusions on strengthening the cooperation and use of the Schengen Information System to deal with persons involved in terrorism or

---

163 In this context, the reference to '*suspects and criminals*' covers: (a) Persons who are suspected of having committed or having taken part in a criminal offence in respect of which Europol is competent, or who have been convicted of such an offence. (b) Persons regarding whom there are factual indications or reasonable grounds to believe that they will commit criminal offences in respect of which Europol is competent.

164 https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2020.

165 https://www.consilium.europa.eu/en/press/press-releases/2020/06/16/preventing-and-countering-terrorism-and-violent-extremism-council-adopts-conclusions-on-eu-external-action/.

terrorism-related activities already recalled the need to "*ensure that information on FTFs is consistently and systematically uploaded to European systems and platforms*".[166] The Council referred to a "*three-tier information sharing approach regarding FTFs by making optimal and consistent use of SIS and Europol data that Europol processes for cross-checking and for analysis in the relevant Analysis projects.*" However, **Member States are not always able to enter third-country sourced information on foreign terrorist fighters into the Schengen Information System** to make them available to the frontline officers in other Member States. First, some third countries share data on suspects and criminals only with Europol and possibly with some Member States. Second, even if a Member State receives the information on suspects and criminals directly from the third country or via Europol, it might not be able to issue an alert on the person concerned due to restrictions in national law (e.g. the need to establish a link to national jurisdiction). This leads to a gap between the information on suspects and criminals that third countries make available to Europol and Member States, and the availability of such information to frontline officers when and where they need it.

In terms of a **possible EU-level solution**, it is widely acknowledged that **Europol** holds valuable information on suspects and criminals that it received from third countries. Once Europol analysed information it received from third countries on suspects and criminals, including by cross checking it against information it already holds in its databases to confirm the accuracy of the information and complement it with other data, Europol needs to make the result of its analysis available to all Member States. To that end, Europol uses its information systems to make its analysis of third-country sourced information on suspects and criminals available to Member States. Europol will also enter third-country sourced information into the watchlist of the European Travel Information and Authorisation System (ETIAS) for third-country nationals exempt from the requirement to be in possession of a visa when crossing the EU external borders.[167] The watchlist will support Member States in assessing whether a person applying for a travel authorisation poses a security risk.

However, **Europol is not able to provide frontline officers in the Member States with the third-country sourced information it holds on suspects and criminals**. Frontline officers do not have access to Europol's information systems or to the data entered by Europol in the ETIAS watchlist. At the same time, Europol is not able to issue alerts in the Schengen Information System as the most widely used information-sharing database in the EU that is directly accessible for border guards and police officers. Crucial third-country sourced information held by Europol on suspects and criminals might therefore not reach the end-users at national level when and where they need it. This includes Europol's analysis of data it received from third countries on foreign terrorist fighters, but also on persons involved in organised crime (e.g. drugs trafficking) or serious crime (e.g. child sexual abuse).

As the exchange of third-country sourced information on suspects and criminals includes the processing of personal data, the assessment of policy options to address the identified problem needs to take **full account of Fundamental Rights and notably the right to the protection of personal data**.

166 https://www.consilium.europa.eu/media/36284/st09680-en18.pdf.
167 Regulation (EU) 2018/1240.

1.2. What are the problem drivers?

There are three problem drivers for the limits in the sharing of third-country sourced information on suspects and criminals.

As a *first problem driver*, and as a consequence of criminals and terrorists exploiting the advantages that globalisation and mobility bring about, the **information that third countries share with the EU about criminals and terrorists is increasingly relevant for EU internal security**. In 2019, Europol accepted almost 12 000 operational contributions from third countries. In 2019, there were over 700 000 objects recorded in the Europol Information System that stem from Europol's analysis of data it received from third countries.

As a *second problem driver*, **frontline officers do not have access to Europol's information systems**. Consequently, frontline officers do not have access to the third-country sourced information that Europol holds on suspects and criminals. Europol's information systems support the work of investigators, criminal intelligence officers and analysts in the Member States. While it is for each Member State to decide which competent national authorities are allowed to cooperate directly with Europol, they do not give their frontline officers access to Europol's information systems.[168] This is due to the way information is stored and provided in Europol's information systems. The information they contain supports the work of investigators and analysis, but it is not suited for direct use in the work of border guards and police officers carrying out a check (i.e. the information is not 'actionable'). Instead, Member States use the Schengen Information System to help frontline officers in other Member States to take informed decisions when they encounter the suspect or criminal under alert. Reflecting the differences in purpose between Europol's information systems and the Schengen Information System, there is a considerable difference in the outreach of these systems.

	Europol Information System	**Schengen Information System**
users	8 587users (end of 2019)	every frontline officer in the Member States[169] (border guards and police officers)
number of checks (in 2019)[170]	5.4 million	6.6 billion

168 It is for each Member State to decide which competent national authorities are allowed to cooperate directly with Europol (Article 7(5) of Regulation (EU) 2016/794.

169 25 Member States participate in the Schengen Information System (Austria, Belgium, Bulgaria, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden). Four Schengen Associated Countries are connected to the system (Iceland, Liechtenstein, Norway and Switzerland). Europol and the EU Agency for criminal justice cooperation Eurojust have access to specific parts of the system but cannot issue alerts in the system.

170 For the Schengen Information System, the table shows all checks carried out in 2019 by all users who have access to the system. When checking the Schengen Information System, users are checking data against those alerts to which they have access (which does not in all cases include law enforcement alerts).

While the sharing with third-country sourced information on suspects and criminals with frontline officers in Member States would enable these frontline officers to more effectively perform their duties, Europol is not able to create alerts in the Schengen Information System. This **restriction in the Europol Regulation and the legal basis governing the Schengen Information System**[171] constitutes a *third problem driver*. While Europol is able to check persons against the Schengen Information System, and is informed about hits on terrorism-related alerts issued by other Member States, Europol cannot issue its own alerts in the system and there are no other ways for Europol to alert front line officers. Therefore, and despite the operational need, Europol cannot share with frontline officers the third-country sourced information it holds on foreign terrorist fighters or persons involved in organised crime (e.g. drugs trafficking) or serious crime (child sexual abuse).

1.3. How will the problem evolve without intervention?

Without any intervention, the limits in the sharing of third-country sourced information on suspects and criminals will persist. As the information that third countries share with the EU about criminals and terrorists will become even more relevant for EU internal security, the impact of this security gap would be expected to grow as well. This is because the cooperation with third countries, and hence the effective use of information they provide on suspects and criminals, is likely to become even more important in the future. As set out above, Member States would not always be able to address this problem, as the obstacles identified above would sometimes prevent Member States from entering important third-country sourced information on suspects and criminals into the Schengen Information System to make them available to the frontline officers in other Member States.

In terms of a possible EU-level solution Europol as the EU criminal information hub is best placed to support Member States by making third-country sourced information available to frontline officers where necessary. However, without any intervention, and despite a growing operational need, Europol would not be able share with frontline officers the third-country sourced information it holds on foreign terrorist fighters or persons involved in organised crime (e.g. drugs trafficking) or serious crime (child sexual abuse).

2. OBJECTIVES: WHAT IS TO BE ACHIEVED?

2.1. Specific objectives

The specific objective is to **provide frontline officers with the result of the analysis of information received from third countries** on suspects and criminals when and where this is necessary. The underlying goal is to enable frontline officers to take informed decisions when they check a person at the external border or within Schengen area. For that, the information received by third countries first needs to be analysed, e.g. by way of checking it against other available information, to verify its accuracy and to complement the information picture.

This specific objective addresses the problem of **limits in the sharing of third-country sourced information on suspects and criminals**. As criminals and terrorists exploit the

[171] Regulation (EU) 2018/1862.

advantages that globalisation and mobility bring about, the information that third countries share with the EU about suspects and criminals is increasingly relevant for EU internal security.

As set out above, **Member States** would not always be able to address this problem. They might not be able to issue an alert in the Schengen Information System on the person concerned due to restrictions in national law (e.g. the need to establish a link to national jurisdiction).

This calls for **EU-level support** for the sharing of third-country sourced information on suspects and criminals with Member States' frontline officers, when and where this is necessary.

This specific objective raises the **policy choice** whether Europol should be able to issue alerts on suspects and criminals in the Schengen Information System on the basis of its analysis of information received from third countries. In terms of possible EU-level solution, Europol as the EU criminal information hub would indeed be best placed to support the sharing of third-country sourced information on suspects and criminals.

As the sharing of information on suspect and criminals includes the processing of personal data, the assessment of policy options to achieve the identified objective needs to take **full account of Fundamental Rights and notably the right to the protection of personal data**.

3. WHAT ARE THE AVAILABLE POLICY OPTIONS?

3.1. Baseline representing current situation

The baseline scenario takes account of the changes brought about by the interoperability[172] of EU information systems for security, border and migration management. Given that interoperability will not change existing access rights of national authorities to EU databases, it will not change the fact that frontline officers do not have access to Europol's information systems. The baseline scenario also considers Europol's on-going work to roll out QUEST[173] (Querying Europol Systems) in the Member States. Moreover, Europol also cooperates with Member States and encourages them to issue alerts in the Schengen Information System. This practice is not transparent, it raises legal concerns (e.g. on responsibility and liability), and it causes operational difficulties (in case of a 'hit' on such an alert issued by a Member State, the underlying analysis held by Europol would be needed for an effective follow up). Consequently, it would hamper the effective sharing of third-country sourced information on suspects and criminals with frontline officers in the Member States, with the risk that border guards and police officers have incomplete information when they check a person.

3.2. Description of policy options requiring a regulatory or non-regulatory intervention

***Policy option 8*: enabling Europol to issue 'discreet check' alerts in the Schengen Information System**

[172] Regulation (EU) 2019/818.

[173] QUEST is a system interface to allow Member States' investigators, criminal intelligence officers and analysts to search and access Europol's databases using their own national information systems.

This policy option consists of **enabling Europol to issue alerts on persons in the Schengen Information System**, based on its analysis of third-country sourced information, with a view to enable frontline officers to take informed decisions when they check a person at the external border or within Schengen area.

The policy option is inspired by the logic of the **Council's three-tier information sharing approach** regarding foreign terrorist fighters, in which the Council calls for "*making optimal and consistent use of SIS and Europol data that Europol processes for cross-checking and for analysis in the relevant Analysis projects.*"[174] The policy option is also inspired by the involvement of Europol in the **European Travel Information and Authorisation System** (ETIAS) for third-country nationals exempt from the requirement to be in possession of a visa when crossing the EU external borders.[175] Europol supports Member States in assessing whether a person applying for a travel authorisation poses a security risk. To that end, Europol will enter data into the ETIAS watchlist to provide Member States with information it holds related to persons who are suspected of having committed or having taken part in a terrorist offence or other serious criminal offence, or regarding whom there are factual indications or reasonable grounds to believe that they will commit a terrorist offence or other serious criminal offences.

As set out above, **Member States** are not always able to issue an alert in the Schengen Information System on the person concerned based on third-country sourced information due to restrictions in national law (e.g. the need to establish a link to national jurisdiction). **EU-level support** would prevent this third-country sourced information on suspects and criminals not being available to Member States, in particular frontline officers, when and where this is necessary. Europol as the EU criminal information hub would be best placed to support the sharing of third-country sourced information on suspects and criminals.

The policy option would enable Europol to issue alerts on suspects and criminals in the Schengen Information System in certain specific and well-defined cases and circumstances, and within the scope of crimes falling under Europol's competence,[176] using so-called **"discreet check" alerts** as an existing alert category.[177] Europol would be able to issue such alerts on the basis of its analysis of third-country sources information on suspects and criminals. When Member States' frontline officers encounter the person under alert in the context of a check at the EU's external border or within the Schengen area, they would be required to discreetly collect as much information as possible on the circumstances of the hit without making the person aware of the existence of the alert. This would require consequential changes to the legal basis governing the Schengen Information System.[178]

This policy option addresses the problem of **limits in the sharing of third-country sourced information on suspects and criminals**. As criminals and terrorists exploit the

---

174 https://www.consilium.europa.eu/media/36284/st09680-en18.pdf.

175 Regulation (EU) 2018/1240.

176 In line with Article 36 of Regulation (EU) 2018/1862, this would cover persons where there is a clear indication that they intend to commit or are committing any of the crimes for which Europol is competent, or persons where an overall assessment (in particular on the basis of past criminal offences) gives reasons to believe that they may commit in future one of the crimes for which Europol is competent.

177 Article 36 of Regulation (EU) 2018/1862.

178 Regulation (EU) 2018/1862.

advantages that globalisation and mobility bring about, the information that third countries share with the EU about suspects and criminals is increasingly relevant for EU internal security. By enabling Europol to issue "discreet check" alerts in the Schengen Information System, the policy option would address the second problem driver identified in section 2.3 above (i.e. frontline officers do not have access to Europol's information systems).

This specific objective raises the **policy choice** whether Europol should be able to issue "discreet check" alerts on suspects and criminals in the Schengen Information System on the basis of its analysis of information received from third countries. "Discreet check" alerts in the Schengen Information System may be issued by national competent authorities, in the context of criminal investigations or to prevent threats to public or national security. The conditions and safeguards under which national competent authorities issue such alerts in Schengen Information Systems are laid down in the related EU regulation[179] and in national law. Through "discreet checks" alerts in the Schengen Information System, national competent authorities in one Member State instruct other Member States' frontline officers to check, in a discreet manner, the person under alert and to collect a set of detailed information from the person if they encounter him/her at the external border or within the Schengen territory. Enabling Europol to issue "discreet alerts" would enhance Europol's capability to provide frontline officers with its analysis of third-country sourced information on suspects and criminals, but at the same time require frontline officers to collect and further process detailed information which could limit the exercise of Fundamental Rights notably the right to the protection of personal data.

As the policy option would enhance the sharing of information on suspect and criminals, and hence lead to the processing of personal data, **the assessment of the impact of this policy option needs to take full account of Fundamental Rights and notably the right to the protection of personal data**.

***Policy option 9*: introducing a new alert category in the Schengen Information System to be used exclusively by Europol**

This policy option consists of introducing a **new alert category** in the Schengen Information System exclusively for Europol, namely a so-called "information alert", with specific requirements and safeguards reflecting Europol's role. Based on Europol's analysis of third-country sourced information, the new alert category would enable frontline officers to take informed decisions when they check a person at the external border or within Schengen area. This policy option is a genuine alternative to policy option 8.

Similar to policy option 8, this policy option is also inspired by the logic of the **Council's three-tier information sharing approach** regarding foreign terrorist fighters, in which the Council calls for "*making optimal and consistent use of SIS and Europol data that Europol processes for cross-checking and for analysis in the relevant Analysis projects.*"[180] The policy option is also inspired by the involvement of Europol in the **European Travel Information and Authorisation System** (ETIAS) for third-country nationals exempt from the requirement to be in possession of a visa when crossing the

[179] Regulation (EU) 2018/1862.

[180] https://www.consilium.europa.eu/media/36284/st09680-en18.pdf.

EU external borders (see the description of policy option 8 above for more details).[181]

As set out above, **Member States** are not always able to issue an alert in the Schengen Information System on the person concerned due to restrictions in national law (e.g. the need to establish a link to national jurisdiction). This calls for **EU-level support** for the sharing of third-country sourced information on suspects and criminals with Member States' frontline officers, when and where this is necessary. Europol as the EU criminal information hub would be best placed to support the sharing of third-country sourced information on suspects and criminals

The policy option would enable Europol to issue 'information alerts' on suspects and criminals as a **new alert category in the Schengen Information System, for exclusive use by Europol** in certain specific and well-defined cases and circumstances. Europol would be able to issue such alerts on the basis of its analysis of third-country sourced information, and within the scope of crimes falling under Europol's competence.[182] In case of a 'hit', the alert would inform the frontline officer that Europol holds information on the person. More specifically, the alert would inform that Europol holds information indicating that this person intends to commit or is committing one of the offences falling under Europol's competence, or that an overall assessment of the information available to Europol gives reason to believe that the person may commit such offence in future.

As a **minimum action to be taken**, the frontline officer would need to report immediately the occurrence of the 'hit' to the national SIRENE Bureau, which would contact Europol, and, as a further follow-up action, could get further background information. Beyond this reporting obligation as a non-coercive measure, there would be no further obligation on the Member State where the 'hit' occurred. Instead, with the relevant national authorities of the Member State concerned would be able to determine, on a case-by-case basis, including based on the background information received from Europol whether further measures need to be taken with regard to the person. Such further measures would take place under national law and the full discretion of the Member State.[183]

This policy option addresses the problem of the **limits in sharing third-country sourced information on suspects and criminals**. As criminals and terrorists exploit the advantages that globalisation and mobility bring about, the information that third countries share with the EU about suspects and criminals is increasingly relevant for EU internal security. By enabling Europol to issue "information alerts" in the Schengen Information System, the policy option would address the second problem driver identified in section 2.3 above.

This specific objective raises the **policy choice** whether Europol should be able to issue

---

181 Regulation (EU) 2018/1240.

182 In line with Article 36 of Regulation (EU) 2018/1862, this would cover persons where there is a clear indication that they intend to commit or are committing any of the crimes for which Europol is competent, or persons where an overall assessment (in particular on the basis of past criminal offences) gives reasons to believe that they may commit in future one of the crimes for which Europol is competent.

183 In the course of the consultation process, more specifically in the context of the Law Enforcement Working Party (LEWP) forum, delegations stressed that only Member States should decide on action to be taken as a follow up on a tailored-made dedicated alert category for Europol in the Schengen Information System (SIS) (see annex 2).

"information alerts" on suspects and criminals in the Schengen Information System on the basis of its analysis of information received from third countries. Unlike under policy option 8, the new alert category would be exclusively used by Europol, which would provide the opportunity to set out specific provisions and safeguards to be fulfilled by Europol upon entering such an alert in the Schengen Information System. In addition, the "information alert" would not instruct Member States' frontline officers to discreetly check the person under alert and collect a set of detailed information if they encounter him/her at the external border or within the Schengen territory. Instead, it would only require the frontline officers to report the occurrence of a hit, whereas the decision on any further measures would be taken on a case-by-case basis by the Member State that has encountered the "hit" on the alert. Still, this policy option would enhance Europol's capability to provide frontline officers with its analysis of third-country sourced information on suspects and criminals, but at the same limit the exercise of Fundamental Rights notably the right to the protection of personal data.

As the policy option would enhance the sharing of information on suspect and criminals, and hence lead to the processing of personal data, **the assessment of the impact of this policy option need to take full account of Fundamental Rights and notably the right to the protection of personal data**.

4. WHAT ARE THE IMPACTS OF THE POLICY OPTIONS?

***Policy option 8*: enabling Europol to issue 'discreet check' alerts in the Schengen Information System**

Expected impact of policy option 8[184]
1) impact on citizens [+]
• It would provide frontline officers with the result of Europol's analysis of relevant data received from third countries on suspects and criminals. It would support them in taking informed decisions when carrying out a check, at the EU external border or within the Schengen area, on a person on which Europol issued an alert. This will enhance EU internal security and have a positive impact on citizens.
2) impact on national authorities [+]
• Frontline officers at the EU external border and within the Schengen area would receive a 'hit' in the Schengen Information System when they check a person on which Europol issued an alert. • In Member States' view, this advantage is partially counterbalanced by the obligation a 'discreet check' alert issued by Europol would impose. Frontline officers would be obliged to perform a 'discreet check' when they encounter the person under alert, i.e. they would need to collect as much information as possible on the person. As Europol does not have executive powers, it may be legally questionable whether it would be possible for Europol to issue 'discreet check' alerts requiring such a coercive measure by national authorities in case of a 'hit'. • There would be marginal costs for Member States to update their national systems allowing their end-users to see the alerts issued by Europol, as well as to update their SIRENE workflows.[185]

[184] The impacts are assessed on a scale ranging from 'very positive impact' (++) to 'very negative impact' (--), with intermediate scores: 'positive impact' (+), 'no impact' (0) and 'negative impact' (-).

[185] SIRENE stands for "Supplementary Information Request at the National Entries". The national

3) impact on EU bodies [++]

- Europol would be able to issue 'discreet check' alerts in the SIS, providing Member States' frontline officers with the result of its analysis of data received from third countries on suspects and criminals. In case of a 'hit' in a Member State related to an alert issued by Europol, the national authorities concerned would need to perform a 'discreet check' on that person and inform Europol of the result thereof. This would significantly increase Europol's analytical capability (e.g. to establish a picture of travel movements of the person under alert), in order to provide a more complete information product to Member States.
- There would be marginal costs for Europol to be able to send data in a structured way to the central component of the Schengen Information System when they issue an alert.
- There would be costs for eu-LISA,[186] the EU agency responsible for the operational management of the Schengen Information System, to update the central system to enable Europol as a new user to create alerts, as well as some elements of the SIRENE mail exchange. These costs would be below EUR 1.5 million.

4) impact on businesses [0]

- There will be no impact on businesses.

5) impact on Fundamental Rights [--]

a) identification of Fundamental Rights limited by the measure

- The policy option limits the Fundamental Right to the **protection of personal data** as guaranteed by Article 8 of the Charter. As the policy option entails the processing by a public authority of data relating to the private life of an individual, it also limits the Fundamental Right to **respect for private life** (Article 7 of the Charter). Consequently, the policy option needs to comply with the conditions laid down in Article 52(1) of the Charter.
- The policy option does **not adversely affect the essence** of the Fundamental Rights to the protection of personal data and to respect for private life.

b) assessment of necessity

- The policy option is **genuinely effective** as it achieves the specific objective of providing frontline officers (police officers and border guards) with the result of the analysis of data received from third countries when and where this is necessary, and therefore the fight against serious crime and terrorism as objectives of general interest in EU law.
- **Existing possibilities** to enhance the availability of Europol data to end-users, notably the roll-out of QUEST[187], are insufficient to address the problem, even if their implementation and application is reinforced.[188] QUEST facilitates the access and use of Europol's databases by investigators, criminal intelligence officers and analysts in the Member States, but not by frontline officers as the actual target group of objective identified. Likewise, Europol existing cooperation with Member States, where the agency encourages national authorities to issue alerts in the Schengen Information System, is insufficient to address the problem. This existing practice is not transparent, it raises legal concerns (e.g. on responsibility and liability), and it causes operational difficulties (in case of a 'hit' on such an alert issued by a Member State, the underlying analysis held by Europol would be needed for an effective follow up).
- **Existing or planned EU information systems** do also not address sufficiently the problem

SIRENE Bureau is operational 24/7 and responsible for any supplementary information exchange.

186 EU Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice.

187 QUEST (Querying Europol Systems) is a system interface that allows integrating automatic queries to Europol databases from national police information systems in the Member States.

188 See annex VII on policy options discarded at an early stage.

identified. In particular, frontline officers do not have access to Europol's information systems or to the data entered by Europol in the ETIAS watchlist. At the same time, Europol is not able to issue alerts in the Schengen Information System as the most widely used information-sharing database in the EU that is directly accessible for border guards and police officers. [189]

- In terms of **alternatives**, the policy option addresses the problem **equally effective** as policy option 9 on introducing a new alert category in the Schengen Information System for Europol.[190] However, policy option 9 establishes a new alert category that would be exclusively used by Europol, which would provide the opportunity to set out specific provisions and safeguards to be fulfilled by Europol upon entering such alert in the Schengen Information System. In addition, policy option 9 is **less intrusive** as it does not oblige the frontline officer to carry out a 'discreet check' as foreseen under policy option 8, which would imply discreetly collecting as much additional information as possible on the person subject to the alert and the circumstances of the hit (see below on policy option 9). Instead, under policy option 9, the frontline officer would need to report immediately the occurrence of the hit to the national SIRENE Bureau which would contact Europol, and, as a further follow-up action, could get further background information through the SIRENE channel.[191] Beyond this reporting obligation as a non-coercive measure, there would be no further obligation on the Member States where the 'hit' occurred. Instead, the relevant national authorities of the Member State concerned would determine, on a case-by-case, whether it is needed to take further measures with regard to the person. Such further measures would take place under national law and the full discretion of the Member State, including on the basis of the background information provided by Europol. This provides for the possibility of less intrusive consequences for the data subject.
- Consequently, as a less intrusive measure is available that is equally effective in meeting the objective, policy option 8 is not limited to what is strictly necessary to achieve the objective. **The policy option does therefore not pass the necessity test.** The policy option shall therefore **not be assessed in terms of its proportionality**.[192]

c) assessment of proportionality

- As the policy option did not pass the necessity test, and therefore is not limited to what is strictly necessary, the policy option shall **not be assessed in terms of its proportionality**.

6) effectiveness in meeting the policy objectives [++]

- This policy effectively meets the objective of providing frontline officers with the result of Europol's analysis of third-countries sourced information on suspects and criminals when and where this is necessary.

7) efficiency in meeting the policy objectives [+]

- While there would be some costs for eu-LISA as well as marginal costs for Member States

189 See the description of existing or planned EU information systems in section 2.3.

190 See the assessment of policy option 9 below.

191 SIRENE stands for "Supplementary Information Request at the National Entries". Each Member State operating the Schengen Information System has set up a national SIRENE Bureau, operational 24/7, that is responsible for any supplementary information exchange and coordination of activities connected to alerts.

192 As set out in the toolkit provided by the EDPS on assessing necessity, "*only if existing or less intrusive measures are not available according to an evidence-based analysis, and only if such analysis shows that the envisaged measure is essential and limited to what is absolutely necessary to achieve the objective of general interest, this measure should proceed on to the proportionality test*". Likewise, the Commission's Operational guidance on taking account of Fundamental Rights in Commission impact assessments states that "*if it can be established that there are two policy options which are equally effective in achieving the objective but have different negative impacts on fundamental rights, then it is necessary to choose that option which is the least intrusive*".

and Europol, this policy option would provide an efficient solution to address the problem of limits in the sharing of third-country sourced information, as it used the Schengen Information System with its existing infrastructure to enable Europol to share the result of its analysis of third-countries sourced information on suspects and criminals with Member States' frontline officers.
8) legal/technical feasibility [-]
• As Europol does not have executive powers, it may be legally questionable whether it would be possible for Europol to issue 'discreet check' alerts requiring such a coercive measure by national authorities in case of a 'hit'. • This policy options requires changes to the rules applicable to the Schengen Information System.[193]
9) political feasibility [-]
• Member States have signaled in the Council's Law Enforcement Working Party that they oppose the issuing of "discreet check" alerts by Europol. • The position of the European Parliament is not clear at this stage. The aspect of extending the legal grounds for data processing by Europol is expected to be carefully assessed by the European Parliament.
10) coherence with other measures [+]
• The policy option would reinforce the Schengen Information System and its purpose of information sharing with frontline officers, as it would extend the scope of this information sharing to the results of Europol's analysis of third-country sourced information on suspects and criminals.

***Policy option 9*: introducing a new alert category in Schengen Information System to be used exclusively by Europol**

Expected impact of policy option 9[194]
1) impact on citizens [+]
• It would provide frontline officers with the result of Europol's analysis of relevant data received from third countries on suspects and criminals. It would support them in taking informed decisions when carrying out a check, at the EU external border or within the Schengen area, on a person on which Europol issued an alert. This will enhance EU internal security and have a positive impact on citizens.
2) impact on national authorities [++]
• Frontline officers at the EU external border and within the Schengen area would receive a 'hit' in the SIS when they check a person on which Europol issued an alert. • Following a 'hit' with an alert issued by Europol, the frontline officer would need to report immediately the occurrence of the hit to the national SIRENE Bureau, which would get in touch with Europol to get further background information. Any further action following a 'hit' would be in the discretion of the authorities of the Member State including on the basis of the background information provided by Europol. Any further action would be taken by the national competent authorities based on an overall assessment of the situation, and on the basis of national law.

193 Regulation (EU) 2018/1862.

194 The impacts are assessed on a scale ranging from 'very positive impact' (++) to 'very negative impact' (--), with intermediate scores: 'positive impact' (+), 'no impact' (0) and 'negative impact' (-).

- There would be marginal costs for Member States to update their national systems allowing their end-users to see the alerts issued by Europol, as well as to update their SIRENE workflows.

3) impact on EU bodies [+]

- Europol would be able to issue a dedicated alert category ('information alert') in the SIS, providing frontline officers with the result of its analysis of data received from third countries on suspects and criminals. In case of a 'hit' with an alert issued by Europol, the national authorities would inform Europol of the 'hit' and its circumstances. They might exchange supplementary information. This would increase Europol's analytical capability (e.g. to establish a picture of travel movements of the person under alert), enabling Europol to provide a more complete information product to Member States.
- There would be marginal costs for Europol to be able to send data in a structured way to the central component of the SIS when they issue an alert.
- There would be costs for eu-LISA to update the central system to enable Europol as a new user to create alerts, and some elements of the SIRENE mail exchange, with costs would be below EUR 1.5 million.

4) impact on businesses [0]

- There would be no impact on businesses.

5) impact on Fundamental Rights [-]

a) identification of Fundamental Rights limited by the measure

- The policy option limits the Fundamental Right to the **protection of personal data** as guaranteed by Article 8 of the Charter. As the policy option entails the processing by a public authority of data relating to the private life of an individual, it also limits the Fundamental Right to **respect for private life** (Article 7 of the Charter). Consequently, the policy option needs to comply with the conditions laid down in Article 52(1) of the Charter.
- The policy option does **not adversely affect the essence** of the Fundamental Rights to the protection of personal data and to respect for private life.

b) assessment of necessity

- The policy option is **genuinely effective** to achieve the specific objective of providing frontline officers (police officers and border guards) with the result of the analysis of data received from third countries when and where this is necessary, and therefore the fight against serious crime and terrorism as objectives of general interest in EU law.
- **Existing possibilities** to enhance the availability of Europol data to end-users, notably the roll-out of QUEST[195], are insufficient to address the problem, even if their implementation and application is reinforced.[196] QUEST facilitates the access and use of Europol's databases by investigators, criminal intelligence officers and analysts in the Member States, but not by frontline officers as the actual target group of objective identified. Likewise, Europol existing cooperation with Member States, where the agency encourages national authorities to issue alerts in the Schengen Information System, is insufficient to address the problem. This existing practice is not transparent, it raises legal concerns (e.g. on responsibility and liability), and it causes operational difficulties (in case of a 'hit' on such an alert issued by a Member State, the underlying analysis held by Europol would be needed for an effective follow up).
- **Existing or planned EU information systems** do also <u>not</u> address sufficiently the problem identified. In particular, frontline officers do not have access to Europol's information

[195] QUEST (Querying Europol Systems) is a system interface that allows integrating automatic queries to Europol databases from national police information systems in the Member States.

[196] See annex VII on policy options discarded at an early stage.

systems or to the data entered by Europol in the ETIAS watchlist. At the same time, Europol is not able to issue alerts in the Schengen Information System as the most widely used information-sharing database in the EU that is directly accessible for border guards and police officers[197]

- In terms of **alternatives**, the policy option addresses the problem **equally effective** as policy option 8 on enabling Europol to issue existing "discreet check" alerts in the Schengen Information System.
- However, policy option 9 establishes a new alert category that would be exclusively used by Europol, which would provide the opportunity to set out specific provisions and safeguards to be fulfilled by Europol upon entering such alert in the Schengen information System. In addition, policy option 9 is **less intrusive** compared to policy option 8. It does not oblige the frontline officer to carry out a 'discreet check' as foreseen under policy option 8, which would imply discreetly collecting as much additional information as possible on the person subject to the alert and the circumstances of the hit. Instead, under policy option 9, the frontline officer would need to report immediately the occurrence of the hit to the national SIRENE Bureau which would contact Europol, and, as a further follow-up action, could get further background information through the SIRENE network. Beyond this reporting obligation as a non-coercive measure, there would be no further obligation on the Member States where the 'hit' occurred. Instead, the national competent authorities of the Member State concerned would determine, on a case-by-case basis, whether further measures need to be taken with regard to the person. Such further measures would take place under national law and the full discretion of the Member State, including on the basis of the background information provided by Europol. This provides for the possibility of less intrusive consequences for the data subject.
- Consequently, the policy option is **essential and limited to what is strictly necessary** to achieve the specific objective of providing frontline officers (police officers and border guards) with the result of the analysis of data received from third countries, and hence to fight serious crime and terrorism as objectives of general interest in EU law.

c) assessment of proportionality

- The policy option and its purpose of enabling Europol to issue a new and dedicated alert category in the Schengen Information System ('information alert') **correspond to the identified need**. They solve the problem resulting from limits in Europol's ability to share promptly its analysis with frontline officers in the Member States. The policy option is **effective and efficient** to fulfil the objective.
- The policy option **affects persons** for whom Europol holds information indicating that the person intends to commit or is committing one of the offences falling under Europol's competence, or that an overall assessment of the information available to Europol gives reason to believe that the person may commit such offence in future.
- The policy option **may raise collateral intrusions** as it could leads to an interference with the privacy of persons travelling together with persons on which Europol issued an alert. In response to a 'hit', the frontline officer might inform Europol about the persons accompanying the subject of the alert.[198] The policy option may therefore limit the Fundamental Rights of persons other than the targeted individual of the alert. This risk will be mitigated with the introduction of necessary safeguards set out below.
- There may be a **potential harmful effect** of the policy option on the Fundamental Right to liberty and security (Article 6 of the Charter), to the extent that a third country may request Europol to issue an alert based on political, military, religious or racial reasons.[199] There may

197 See the description of existing or planned EU information systems in section 2.3.

198 See Article 37(1)(d) of Regulation (EU) 2018/1862.

199 See p. 19 of the Opinion of the EU Agency for Fundamental Rights: Interoperability and Fundamental Rights implications (11.4.2018).

also be a potential harmful effect of the policy option on the principle of *non-refoulement* as encompassed in Articles 18 and 19 of the Charter.[200] An information alert by Europol might contribute to the decision of a border guard to refuse entry to the person subject to the alert, thus affecting the access to international protection at the EU external border. These risks will be mitigated with the introduction of necessary safeguards set out below.

- In line with the existing rules on the Schengen Information System,[201] **the alert shall be kept only for the time required to achieve the purpose** for which it was entered (more details are set out below on safeguards). The issuing of an 'information alert' in the Schengen Information System does **not require the processing of special categories of data**. The issuing of alerts in the Schengen Information System does not amount to profiling of the individual and does **not entail the use of automated decision making**.
- Consequently, the policy option does **not impose a disproportionate and excessive burden** on the persons affected by the limitation (i.e. persons for whom Europol holds information indicating that the person intends to commit or is committing one of the offences falling under Europol's competence, or that an overall assessment of the information available to Europol gives reason to believe that the person may commit such offence in future) in relation to the specific objective of providing frontline officers with the information they need, and hence to the objectives of fighting serious crime and terrorism as objectives of general interest in EU law.
- Weighing up the intensity of the interference with the Fundamental Rights to the protection of personal data and to respect for private life as described under step 3 with the legitimacy of the objectives to fight against serious crime and terrorism as objectives of general interest in EU law, the policy option constitutes a **proportionate response** to the need to solve the problem resulting from limits in Europol's ability to share promptly its analysis with frontline officers in the Member States when and where they need it.
- However, in order to establish a balance between the extent and nature of the interference and the reasons for interfering as translated into the objective of providing frontline officers (police officers and border guards) with the result of the analysis of data received from third countries when and where this is necessary, a **number of safeguards are necessary** (see below).

d) necessary safeguards

- All **safeguards** set out in the rules applicable to the Schengen Information System[202] would also need to apply to alerts issued by Europol, and would be reflected in the revised Europol Regulation where needed.
- The revised Europol Regulation would need to limit the issuing of alerts by Europol to what is **strictly necessary**. Europol would only be allowed to issue alerts in SIS on third country nationals. When Europol receives data on non-third countries nationals from a third country, it would instead contact the Member State concerned directly and not issue an alert in SIS. In such cases, it would be up to the Member State of nationality to assess whether issuing an alert in the Schengen Information System is necessary and proportionate.
- In addition, with regard to data on third country nationals, there is a need for preparatory steps and a **prior consultation of all Member States** by Europol before issuing an alert in the Schengen Information System. As a first step, Europol should verify if there is an alert already issued on the person in the Schengen Information System, in which case no second alert should be issues. Second, a prior consultation with the Member States should be launched, informing about the data Europol received from third countries. These steps would ensure that:

[200] Fundamental Rights Agency: Guidance on how to reduce the risk of refoulement in external border management when working in or together with third countries (2016).

[201] Article 53 of Regulation (EU) 2018/1862.

[202] Regulation (EU) 2018/1862.

- no Member State has already issued an alert on the person;
- no Member State intends to issue an alert on the person (also in light of the data available to Europol);
- no Member State otherwise objects to the issuing of an alert by Europol, e.g. for reasons of national security.

- Consequently, the **personal scope of the alerts** would be limited to third country nationals in respect of whom no alert in the Schengen Information System has been issued by any Member State.
- The revised Europol Regulation would need to set clearly the **conditions, requirements and safeguards** under which Europol would issue 'information alerts' in the Schengen Information System. This would include the analysis that Europol would need to undertake prior to issuing an alert to verify the quality and reliability of the data it received, and to enrich the data with information it holds in its databases on the person concerned. Moreover, given that this policy option would lead to the establishment of a dedicated alert category in the Schengen Information System for exclusive use by Europol, the respective limitations and safeguards for this alert category in the legal basis of the Schengen Information System would be tailored to the situation of Europol and to what is strictly necessary.
- Alerts issued by Europol would be kept only for the time that is strictly necessary to achieve the purpose for which they were entered. In analogy with the existing rules applicable to the Schengen Information System[203], Europol may enter an alert **for a period of one year**, with the obligation to review the need to retain the alert within the one-year period.
- The revised Europol Regulation would need to **restrict the number of persons** authorised to issue alerts in the Schengen Information System and to access the information received in case of a 'hit' from the Member State concerned to what is strictly necessary.
- In analogy with the existing rules applicable to the Schengen Information System[204], Europol would need the prior consent of the Member State in which the hit occurred to **transfer data** resulting from a 'hit' with its alerts **to third countries** or international organisations.
- Safeguards for **persons in need of protection,** safeguards that exclude alerts based on political, military, religious or racial reasons, and safeguards that ensure the principle of *non-refoulement*.[205]
- The revised Europol Regulation would need to ensure the possibility for an individual to **pursue legal remedies**, implementing all related provisions in the rules applicable to the Schengen Information System,[206] and building on the related provisions in the current Europol Regulation.[207]

6) effectiveness in meeting the policy objectives [++]

- This policy effectively meets the objective of providing frontline officers with the result of Europol's analysis of third-countries sourced information on suspects and criminals when and where this is necessary.

7) efficiency in meeting the policy objectives [+]

- While there would be some costs for eu-LISA as well as marginal costs for Member States and Europol, this policy option would provide an efficient solution to address the problem of limits in the sharing of third-country sourced information, as it used the Schengen

203 See Article 53(4) of Regulation (EU) 2018/1862.
204 See Article 65 of Regulation (EU) 2018/1862.
205 See pp. 19f of the Opinion of the EU Agency for Fundamental Rights: Interoperability and Fundamental Rights implications (11.4.2018).
206 See Regulation (EU) 2018/1862, notably: Article 67 on Right of access, rectification of inaccurate data and erasure of unlawfully stored data; Article 68 on Remedies; Article 72 on Liability.
207 Chapter VII of Regulation (EU) 2016/794.

Information System with its existing infrastructure to enable Europol to share the result of its analysis of third-countries sourced information on suspects and criminals with Member States' frontline officers.
8) legal/technical feasibility [+]
• This policy provides a feasible way to meet the objective of providing frontline officers with the result of Europol's analysis of data received from third countries on suspects and criminals when and where this is necessary. • This policy option requires changes to the rules applicable to the Schengen Information System.[208]
9) political feasibility [0]
• The aspect of extending the legal grounds for data processing by Europol is expected to be carefully assessed by the co-legislators. • Member States in the Council are expected to support the policy option, given the Council's call for "*making optimal and consistent use of SIS and Europol data that Europol processes for cross-checking and for analysis in the relevant Analysis projects.*" • The position of the European Parliament is not clear at this stage.
10) coherence with other measures [+]
• The policy option would reinforce the Schengen Information System and its purpose of information sharing with frontline officers, as it would extend the scope of this information sharing to the results of Europol's analysis of third-country sourced information on suspects and criminals.

5. HOW DO THE OPTIONS COMPARE?

Comparative assessment		
	option 8	**option 9**
1) impact on citizens	+	+
2) impact on national authorities	+	++
3) impact on EU bodies	++	+
4) impact on businesses	0	0
5) impact on Fundamental Rights	--	-
6) effectiveness in meeting the policy objectives	++	++
7) efficiency in meeting the policy objectives	+	+
8) legal/technical feasibility	-	+
9) political feasibility	-	0
10) coherence with other measures	+	+
preferred policy option		**X**

[208] Regulation (EU) 2018/1862.

Policy option 9 is a genuine alternative to policy option 8.

For both policy options, there would be costs for eu-LISA to update the central system to enable Europol as a new user to create alerts, as well as some elements of the SIRENE mail exchange. Moreover, there would be some marginal costs for Member States and Europol. Still, both policy options would provide an **efficient solution** to address the problem of limits in the sharing of third-country sourced information, as it used the Schengen Information System with its existing infrastructure to enable Europol to share the result of its analysis of third-countries sourced information on suspects and criminals with Member States' frontline officers.

Both policy options are **equally effective** in meeting the objective of providing frontline officers with the result of Europol's analysis of data received from third countries on suspects and criminals. In doing so, both policy options would provide clear **EU added value**. Moreover, beyond that objective, policy option 8 would also provide Europol with additional information collected by frontline officers when carrying out a 'discreet check' when they encounter the person under alert. However, policy option 9 better takes into account the existing legal framework of the Schengen Information System, under which only national competent authorities may issue 'discreet check' alerts requiring a coercive measure in case of a 'hit'. Policy option 9 would create slightly higher one-off costs than policy option 8 due to the need to create a new alert category, but these slightly higher costs are justified by the legal clarity and additional safeguards it brings about.

More importantly, **policy option 9 is less intrusive compared to policy option 8** in terms of limitations on the exercise of Fundamental Rights, as it does not oblige the frontline officer to collect extensive information on the person subject to the alert and the circumstances of the 'hit' (i.e. a 'discreet check' under policy option 8). Under policy option 9, the frontline officer would inform its SIRENE Bureau of the hit. Any further action would be in the discretion of the national authorities and their overall assessment of the situation, thus allowing for less intrusive consequences for the data subject.

Consequently, as a less intrusive measure is available that is equally effective in meeting the objective, policy option 8 is not limited to what is strictly necessary to achieve the objective. **Policy option 8 does therefore not pass the necessity test.** Policy option 8 shall therefore **not be assessed in terms of its proportionality**.[209] Moreover, Member States also strongly oppose policy option 8.

Policy option 9 also limits the exercise of Fundamental Rights. These limitations can be justified, as the policy option constitutes a necessary and proportionate response to the need provide frontline officers with the result of the analysis of third-countries sourced information. Moreover, the identified safeguards will mitigate the limitations on the exercise of Fundamental Rights.

Policy option 9, instead, passes both the necessity and proportionality tests and is

[209] As set out in the toolkit provided by the EDPS on assessing necessity, "*only if existing or less intrusive measures are not available according to an evidence-based analysis, and only if such analysis shows that the envisaged measure is essential and limited to what is absolutely necessary to achieve the objective of general interest, this measure should proceed on to the proportionality test*". Likewise, the Commission's Operational guidance on taking account of Fundamental Rights in Commission impact assessments states that "*if it can be established that there are two policy options which are equally effective in achieving the objective but have different negative impacts on fundamental rights, then it is necessary to choose that option which is the least intrusive*".

the preferred option.

In order to remain strictly necessary, policy option 9 would require preparatory steps and a prior consultation of all Member States by Europol before issuing an alert in the Schengen Information System. As a first step, Europol should verify if there is an alert already issued on the person in the Schengen Information System. Second, a prior consultation with the Member States should be launched. These steps would ensure that:

- no Member State has already issued an alert on the person;
- no Member State intends to issue an alert on the person;
- no Member State otherwise objects to the issuing of an alert by Europol, e.g. for reasons of national security.

The issuing of alerts by Europol in the Schengen Information System would be limited to third country nationals not residing in EU. Appropriate substantive and procedural conditions for issuing the alerts would need to be set out in the future regulatory framework.

Annex 7: Facilitating Third Country Cooperation

1. PROBLEM DEFINITION

1.1. What is the problem?

Serious crime and terrorism often have links beyond the territory of the Union.[210] Large-scale internationally operating criminal networks pose a significant threat to the EU's security. To effectively counter serious crimes such as drug trafficking, trafficking of human beings and international terrorism, it is essential to cooperate with law enforcement authorities of third countries, which hold crucial information to facilitate and support investigations. Due to the international aspect of criminal phenomena, cooperation at the national level is not always sufficient to effectively address the needs of the Member States' law enforcement authorities and shortcomings in cooperation with third countries.

Enhancing the cooperation with third countries is an important aspect of the support that Europol provides to Member States.[211] A July 2020 European Parliament Resolution[212] states that "*cross-border information exchange between all relevant law enforcement agencies, within the EU and with global partners, should be prioritised in order to fight serious crime and terrorism more effectively*." Indeed, countering terrorism effectively requires cooperation with external partners.[213] On serious crime, the 2017 Council Conclusions[214] on the continuation of the EU Policy Cycle for organised and serious international crime stressed "*the external dimension of internal security and the importance of further developing cooperation with relevant third countries*." The Council called on the Commission to facilitate the participation of third countries in the

---

210 According to the 2017 Serious and Organised Crime Threat Assessment (SOCTA), '*More than 5,000 OCGs operating on an international level are currently under investigation in the EU. The number of OCGs operating internationally highlights the substantial scope and potential impact of serious and organised crime on the EU'*. Moreover, SOCTA provides that *'Over the past few years, criminals of more than 180 nationalities were involved in serious and organised crime in the EU. The majority of OCGs operating on an international level are composed of members of more than one nationality.'*

211 Europol cooperates with third countries. Strategic agreements with third countries provide for the exchange of general intelligence as well as strategic and technical information, whereas operational agreements allow for the exchange of information, including personal data. In addition, third countries with which Europol has concluded cooperation agreements are represented by Liaison Officers at Europol headquarters, similarly to the Liaison Officers of the Member States. Liaison Officers communicate over SIENA system, a tool that enables swift, secure and user-friendly communication and exchange of operational and strategic crime-related information and intelligence between Europol, Member States and third parties that have cooperation agreements with Europol. Third countries' Liaison Officers can be used as an entry point of cooperation with Member States.

212 European Parliament resolution of 10 July 2020 on the European Parliament recommendation to the Council and the Commission concerning the conclusion of an agreement, under negotiation, between the European Union and New Zealand on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the New Zealand authorities competent for fighting serious crime and terrorism

213 EU Terrorism Situation and Trend report 2020. See the description of *Problem III* for the importance of sharing information with third countries on foreign terrorist fighters.

214 Council Conclusions on the continuation of the EU Policy Cycle for organised and serious international crime for the period 2018-2021. The objective of the EU Policy Cycle is to ensure effective cooperation between Member States' law enforcement authorities, Europol and other EU bodies in their operational action targeting the most pressing criminal threats facing the EU.

operational implementation of the EU Policy Cycle, which in turn requires the exchange of personal data with these third countries.

As illustrated by the Home Affairs Ministers of the European Union in their October 2020 Declaration 'Ten points on the Future of Europol'[215] '*cooperation with third countries is essential to the success of Europol's work. Successful work in fighting terrorism and organised crime requires cooperation beyond the European level'.* The Declaration highlights that *'if Europol is to properly fulfil its role as EU criminal information hub, more effective mechanisms must be put in place through which it can exchange information with other third countries'*.

As highlighted in the July 2020 Commission Communication[216] on the EU Security Union Strategy, Europol can play a key role in expanding its cooperation with third countries to counter crime and terrorism in coherence with other EU external polices and tools. Europol can already now receive personal data from third countries, but cannot share personal data with third countries in an effective manner. Europol can structurally exchange data with countries based on cooperation agreements concluded under the previous Council Decision 2009/371/JHA, international agreements under the existing Regulation or adequacy decisions under Directive 2016/680 (article 25(1) of the Europol Regulation). However, since the entry into application of the current Europol Regulation in 2017, and hence of the legal grounds it provides for Europol to enter into an structural cooperation with third countries and transfer personal data, related efforts have not progressed at the desired pace and have not yet led to tangible results in terms of establishing such cooperation:[217]

1) The Commission has not adopted yet any **adequacy decision** in accordance with the Data Protection Law Enforcement Directive that would allow for the free transfer of personal data to a third country.

2) Due to various reasons, following the adoption by the Council of eight mandates[218] in June 2018 for the Commission to negotiate **international agreements** with priority third countries on strengthening the cooperation with Europol, the subsequent efforts by the Commission have not yet led to conclusion of such agreements. While negotiations have led to considerable progress with one key foreign partner, political reasons have prevented such progress in another case (repeated elections in the partner country). For the remaining cases, the third

---

215 Declaration of the Home Affairs Ministers of the European Union, Ten points on the future of Europol, Berlin, 21 October 2020, https://www.eu2020.de/blob/2408882/6dd454a9c78a5e600f065ac3a6f03d2e/10-22-pdf-virtbrotzeit-europol-en-data.pdf

216 COM(2020) 605 final (24.7.2020).

217 The Europol Regulation sets outs three ways to establish a structural cooperation with a third countries that would provide legal grounds based on which Europol could lawfully transfer personal data to authorities of that third countries: (1) a Commission adequacy decision adopted in accordance with Article 36 of Directive (EU) 2016/680; (2) an international agreement concluded by the Union pursuant to Article 218 TFEU; (3) an authorisation by the Europol Management Board, in agreement with the EDPS, based on a self-assessment that adequate safeguards for the protection of privacy and fundamental rights exist. Moreover, in specific situations on a case-by-case basis, the Europol Executive Director may authorise the transfer of personal data.

218 The negotiating mandates approved by the Council allow the Commission to enter into negotiations with eight priority countries on behalf of the EU: Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia and Turkey.

countries have not shown an interest in entering into such negotiations. So although the Council and the Commission consider it necessary to establish a structural cooperation between Europol and these eight priority countries, it has not yet been possible to achieve this. On the other hand, as regards the mandate the Commission received in 2020 to open negotiations with New Zealand, informal discussions have started with good prospects.

As regards the possibility[219] to transfer personal data in specific situations on a case-by-case basis (Article 25(5) of the Europol Regulation), the Europol Executive Director made use of this **derogation** in two case, including in the cooperation with New Zealand in the follow up to the March 2019 Christchurch attack.

The possibility to transfer personal data based on a **self-assessment of the adequate level of safeguards** and an authorisation by the Europol Management Board, in agreement with the EDPS Article 25(6) of the Europol Regulation), has not been applied in practice. In one case, preparatory steps have been taken for such an authorisation. This case seems to indicate that there are uncertainties around the conditions under which such transfer mechanism can be used.

Consequently, and besides the cooperation that takes place on the basis of cooperation agreements[220] concluded before the entry into application of the current Europol Regulation, uncertainties around the use of mechanisms to exchange personal data with third countries seem to affect the agency's ability to support national law enforcement authorities through its cooperation with these third countries.[221]

1.2. What are the problem drivers?

The main obstacle to cooperation with some third countries is that the level of data protection in those countries is not adequate to meet EU data protection requirements. The level of data protection at Europol is a crucial aspect for the work and success of the agency. For Europol to fulfil its mandate effectively and successfully, it is essential that all data processing by Europol and through its infrastructure takes place with the **highest level of data protection**. Firstly, providing the highest level of data protection is necessary for citizens to have trust in the work of Europol. Secondly, Member States likewise demand that Europol processes data with the highest data protection standards, as they need to be confident that Europol provides for data security and confidentiality before they share their data with the agency.[222] At the same time, Member States recognised the need to receive data from third countries in order to deal with the evolving nature of internet-based and cross-border crime.

---

219 Article 25(5) of Regulation (EU) 2016/794.

220 Europol has cooperation agreements in place with 17 countries: Albania, Australia, Bosnia and Herzegovina, Canada, Columbia, Georgia, Iceland, Liechtenstein, Moldova, Monaco, Montenegro, North Macedonia, Norway, Serbia, Switzerland, Ukraine, United States of America.

221 40.85 % of the participants of the targeted consultation by way of questionnaire (see Annex 11) 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. 39. 44 % consider that the rules currently in place allow Europol to efficiently establish cooperative relations with third countries.

222 This was found both during the consultation on the inception impact assessment and targeted consultation via EU survey, where a large majority of respondents referred to the need to safeguard and uphold fundamental rights when cooperating with third countries.

In order to enter into a structural cooperation with Europol, EU data protection law requires that a third country ensures an adequate level of data protection to the data received from Europol. According to the case law of the CJEU, a transfer of personal data from the EU to a third country may take place only if that country ensures a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the EU.[223] This requirement under EU law will need to be met in any case, irrespective of the legal grounds used for the structural transfer of personal data. Consequently, for third countries that are unable or unwilling to provide a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the EU, Europol will not be able to transfer personal on a structural basis.

However, two further aspects act as drivers for the lack of exchange of personal data between Europol and third countries. Firstly, the legal grounds available in the Europol Regulation are not used to the same extent as the corresponding legal grounds provided to Member States in the Data Protection Law Enforcement Directive.[224] There may be a lack of clarity or guidance regarding the proper use of the various transfer grounds under the Europol Regulation. In any case, there is an under-use of these legal grounds, and this under-use constitutes an obstacle to cooperation with third countries. For example, Member States often rely on the derogations for the transfer of personal data in specific situations on a case-by-case basis. This is not surprising, as there are regularly situations where cooperation with a third country is necessary for law enforcement to prevent or investigate a specific criminal offence. In that respect, the under-use of the legal grounds available in the Europol Regulation might constitute an obstacle to cooperation with third countries. The same seems to be true for the transfer of data on the basis of a self-assessment of the third country's legal system. As part of that, there may be a lack of clarity or guidance regarding the proper use of the various transfer grounds under the Europol Regulation, possibly resulting in the under-use of certain of these grounds.

Secondly, there are differences in the legal grounds for the transfer of personal data between the Europol Regulation and the Data Protection Law Enforcement Directive. As regards the possibility to transfer personal data to a third country based on a self-assessment of the adequate level of safeguards, the Europol Regulation sets procedural requirements that do not apply in the Data Protection Law Enforcement Directive, such as a time limit ("*not exceeding one year*").

Moreover, when it comes to the possibility to transfer personal data in specific situations on a case-by-case basis, the Data Protection Law Enforcement Directive[225] allows for the use of this derogation for "*a transfer or a category of transfers of personal data*". This allows for transfers of a category of personal data such as data of persons that are related to the specific crime where this is necessary for the investigation, while the exact scope of the persons implied might not be known yet when the authorisation for the transfers is sought. The derogation in the Europol Regulation, instead, only applies to a "*transfer of personal data*". This limitation led to operational challenges when Europol applied the derogation to support New Zealand in the investigation of the March 2019 Christchurch

223 Opinion 1/15, *EU-Canada PNR Agreement*, EU:C:2017:592 (26.7.2017); judgment of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650; judgement of 16 July 2020, C-311/18, *Schrems II*, EU:C:2020:559.

224 Article 38 of Directive (EU) 2016/680.

225 Article 38(1) of Directive (EU) 2016/680.

attack.[226]

The limitations in the Europol Regulation, when compared to the Data Protection Law Enforcement Directive, might therefore constitute an obstacle to cooperation with third countries.

Consequently, the lack of operational cooperation and exchange of personal data between Europol and third countries might, at least to some extent, result from an under-use of available legal grounds set out in the Europol Regulation, as well as from certain limitations in these legal grounds.[227]

1.3. How will the problem evolve without intervention?

The obstacles posed by the limitations in the current Europol Regulation when it comes to **operational cooperation with priority third countries** will persist, and hence the hindrance of exchange of personal data between Europol and these third countries. Given the expectation that the links that serious crime and terrorism have beyond the territory of the Union will increase further, also due to digitalisation, there will also be an increase in the negative impact on the EU's internal security resulting from a lack of effective operational cooperation between Europol and some third countries.

2. OBJECTIVES: WHAT IS TO BE ACHIEVED?

2.1. Specific objectives

The specific objective is to facilitate operational cooperation between Europol and third countries including the transfer of personal data where this is necessary for law enforcement and EU internal security, making use of the full potential of the different legal grounds for data transfers, while ensuing full compliance with EU data protection requirements. In that way, Europol could better support national law enforcement authorities through its cooperation with third countries.

This specific objective raises the **policy choice** whether a **targeted revision** of the provision in the Europol Regulation on a **self-assessment of the adequate level of safeguards** should be pursued or a **targeted revision** of the provision in the Europol Regulation on the **transfer of personal data in specific situations** on a case-by-case basis or to **seek best practices and guidance** on the application of specific provisions of the current Europol Regulation. This relates to the essence of Europol's working methods and operational support capabilities, and therefore a core task of Europol under its legal mandate that Member States expect from the agency.

---

[226] The provision in the Europol Regulation requires a dedicated authorisation – and hence a dedicated procedure and justification – for each transfer of personal data. Moreover, the actual personal data to be transferred in a case-specific cooperation with a third country is not always clear from the outset, as a key purpose of such cooperation is to identify accomplices and other associates of a criminal that were previously unknown.

[227] The responses to the questionnaire during the consultation of the stakeholders showed that only 39. 44 % of the respondents believe that the rules currently in place allow Europol to efficiently establish cooperative relations with third countries.

3. WHAT ARE THE AVAILABLE POLICY OPTIONS?

3.1. Baseline representing current situation

The baseline is a 'no policy change' scenario. As regards the **cooperation with third countries**, the baseline scenario assumes that the provisions of the Europol mandate on personal data transfers to third countries remain unchanged, including the limitations identified. The Europol Regulation foresees that by June 2021, the Commission shall assess the cooperation agreements for the exchange of personal data that Europol concluded with third countries before that Regulation entered into application.[228]

3.2. Description of policy options requiring a regulatory or non-regulatory intervention

This impact assessment will assess three policy options to strengthen Europol's capacity to cooperate with third countries. The problems present above cannot be solved by co-operation at the national level because cooperating with third countries can be best achieved via Europol as it affects the Union as a whole and can conduct international agreements with third countries on behalf of Member States.

***Policy option 10*:**

This policy option consists of a **targeted revision** of the provision in the Europol Regulation[229] on a Europol **self-assessment of the adequate level of safeguards** and an authorisation by the Europol Management Board in agreement with the EDPS. This regulatory intervention would introduce some flexibility on how to meet the requirement of adequate safeguards in specific situations (targeted to specific purposes and a specific national authority, with conditions attached to be fulfilled by the third country). It would introduce some flexibility in procedural terms (no time limitation, but with the possibility for the EDPS to end the data transfer if requirements are no longer fulfilled).

The targeted revision foreseen under this policy option would not affect the Commission's obligation to assess, by June 2021, the cooperation agreements for the exchange of personal data that Europol concluded with third countries before the Europol Regulation entered into application.[230]

***Policy option 11*:**

This policy option consists of a **targeted revision** of the provision in the Europol Regulation[231] on the **transfer of personal data in specific situations** on a case-by-case basis. This regulatory intervention would clarify that the provision is also applicable to a category of transfers of personal data rather than only a single transfer, aligning it with the Data Protection Law Enforcement Directive.[232] The policy option would therefore lead to the possibility of transferring a category of personal data to a third country on the basis of one single justification and authorisation. This would cover the transfer of personal data of persons who are involved in or otherwise linked to the specific criminal offence for which the authorisation is sought, in line with the categories of personal data

228 Article 25(4) of Regulation (EU) 2016/794.
229 Article 25(6) of Regulation (EU) 2016/794 (11.5.2016).
230 Article 25(4) of Regulation (EU) 2016/794 (11.5.2016).
231 Article 25(5) of Regulation (EU) 2016/794 (11.5.2016).
232 Article 37(1)(b) and Article 38 of Directive (EU) 2016/680 (27.4.2016).

and categories of data subjects set out in annex II of the Europol Regulation, provided that each such transfer of personal data is strictly necessary.

The targeted revision foreseen under this policy option would not affect the Commission's obligation to assess, by June 2021, the cooperation agreements for the exchange of personal data that Europol concluded with third countries before the Europol Regulation entered into application.[233]

Policy option 12:

This policy option consists of **seeking best practices and guidance** on the application of specific provisions of the current Europol Regulation, namely:

- guidance from the European Data Protection Supervisor on the effective application of the provision in the current Europol Regulation[234] on a self-assessment of the adequate level of safeguards and an authorisation by the Europol Management Board in agreement with the EDPS;

- best practices from Member States on how they apply the corresponding provision in the Data Protection Law Enforcement Directive[235] on the transfer of personal data in specific situations on a case-by-case basis as well as on the basis of a self-assessments on the level of safeguards in the third country, as a source of inspiration for the application of the respective provision in the current Europol Regulation.[236]

The analysis of policy options 10, 11 and 12 addressing the identified problems hindering effective third country cooperation take full account of Fundamental Rights and notably, the right to the protection of personal data.

4. WHAT ARE THE IMPACTS OF THE POLICY OPTIONS?

***Policy option 10*: targeted revision of the provisions on self-assessment of the adequate level of safeguards**

Expected impact of policy option 10[237]
1) impact on citizens [+]
• Given that the requirement of essential equivalence as set by CJEU case law applies to any structural transfer of personal data to third countries, the changes foreseen by the policy option would have to comply with that standard. To the extent that the policy option facilitates the transfer of personal data from Europol to a third country within that framework, it would have a positive impact on EU internal security and hence on citizens.
2) impact on national authorities [+]
• Given that the requirement of essential equivalence as set by CJEU case law applies to any structural transfer of personal data to third countries, the changes foreseen by the policy

233 Article 25(4) of Regulation (EU) 2016/794 (11.5.2016).
234 Article 25(6) of Regulation (EU) 2016/794 (11.5.2016).
235 Article 38 of Directive (EU) 2016/680 (27.4.2016).
236 Article 25(5) of Regulation (EU) 2016/794 (11.5.2016).
237 The impacts are assessed on a scale ranging from 'very positive impact' (++) to 'very negative impact' (--), with intermediate scores: 'positive impact' (+), 'no impact' (0) and 'negative impact' (-).

option would have to comply with that standard. To the extent that the policy option facilitates the transfer of personal data from Europol to a third country within that framework, it would have a positive impact on national law enforcement authorities as they would benefit from increased cooperation between Europol and that third country.

3) impact on EU bodies [+]

- Given that the requirement of essential equivalence as set by CJEU case law applies to any structural transfer of personal data to third countries, the changes foreseen by the policy option would need to comply with such standard. To the extent that the policy option facilitates the transfer of personal data from Europol to a third country within that framework, it would enable Europol to better support Member States with the results of such enhanced cooperation with the third country.

4) impact on businesses [0]

- There will be no impact on businesses.

5) impact on Fundamental Rights [0]

- Policy option 10 would modify an existing legal ground for Europol for the processing of personal data. According to the case law of the CJEU, a transfer of personal data from the EU to a third country may take place only if that country ensures a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the EU thus, protecting fundamental rights. The changes foreseen will have to comply with that standard. Consequently, and irrespective of any change to the provision in the Europol Regulation on a self-assessment of the adequate level of safeguards, that legal ground can only be applied for the transfer of personal data to a third country if that country ensures a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the EU.

6) effectiveness in meeting the policy objectives [-]

- Given that the requirement of essential equivalence as set by CJEU case law applies to any transfer of personal data to third countries and hence irrespective of any change to the provision on self-assessment of the adequate level of safeguards, the changes foreseen by the policy option would not provide any new legal grounds for the transfer of personal data. Consequently, the policy option would not meet the policy objective of facilitating Europol's cooperation with third countries, thus it is not an effective option.

7) efficiency in meeting the policy objectives [-]

- Partially efficient option meeting the objective of facilitating operational cooperation between Europol and third countries including the transfer of personal data where this is necessary for law enforcement and EU internal security, as it facilitates the transfer of personal data in specific situations. National competent authorities in the Member States will profit form this possibility by saving valuable and indispensable resources.

8) legal/technical feasibility [0]

- Given that the requirement of essential equivalence as set by CJEU case law applies to any transfer of personal data to third countries and hence irrespective of any change to the provision on self-assessment of the adequate level of safeguards, the changes foreseen by the policy option would not provide any new legal grounds for the transfer of personal data and are thus feasible.

9) political feasibility [-]

- It is expected that the European Parliament would oppose any changes to the provisions on self-assessment of the adequate level of safeguards as an attempt to bypass the legal ground for the transfer of personal data provided by an international agreement on the basis of

Article 218 TFEU, and hence of the European Parliament's right to give consent.
10) coherence with other measures [0]
• Not applicable.

***Policy option 11*: targeted revision aligning the provision on the transfer of personal data in specific situations with the provision of the Data Protection Law Enforcement Police Directive**

Expected impact of policy option 11[238]
1) impact on citizens [+]
• As the policy option facilitates the transfer of personal data to a third country in specific situations where this is necessary for a specific investigation of a case of serious crime or terrorism, it enhances EU internal security and therefore can have a positive impact on citizens outweighing, at least in part, the limitations on privacy.
2) impact on national authorities [+]
• As the policy option facilitates the transfer of personal data from Europol to a third country in specific situations where this is necessary for a specific investigation of a case of serious crime or terrorism, national authorities will benefit from this enhanced possibility for cooperation between Europol and third countries.
3) impact on EU bodies [+]
• The policy option facilitates the transfer of personal data from Europol to a third country in specific situations where this is necessary for a specific investigation of a case of serious crime or terrorism, thus enhancing the possibilities for Europol to cooperate with third countries.
4) impact on businesses [0]
• There is no impact on businesses.
5) impact on Fundamental Rights [0]
• The alignment with the respective provision in the Data Protection Police Directive[239] extends the scope of the provision in the Europol Regulation[240] on the transfer of personal data in specific situations (from "*the transfer of personal data*" to "*a category of transfers of personal data*"). The policy option therefore leads to the possibility of transferring a category of personal data to a third country on the basis of one single justification and authorisation, which further limits the Fundamental Right to the **protection of personal data** as guaranteed by Article 8 of the Charter. As the policy option entails the processing by a public authority of data relating to the private life of an individual, it also limits the Fundamental Right to **respect for private life** (Article 7 of the Charter). Consequently, the policy option needs to comply with the conditions laid down in Article 52(1) of the Charter. • The sub-option does **not adversely affect the essence** of the Fundamental Rights to the protection of personal data and to respect for private life. The policy option is limited to what is strictly necessary and proportionate. For more information, see the detailed analysis of the impact on Fundamental Rights in Annex 5.

238 The impacts are assessed on a scale ranging from 'very positive impact' (++) to 'very negative impact' (--), with intermediate scores: 'positive impact' (+), 'no impact' (0) and 'negative impact' (-).

239 Article 38(1) of Directive (EU) 2016/680.

240 Article 25(5) of Regulation (EU) 2016/794.

- All **requirements** and **safeguards** set out in the existing provision of the Europol Regulation on transfer of personal data in specific situations will remain applicable. Moreover, **further safeguards** are necessary in order to establish a balance between the extent and nature of the interference and the reasons for interfering as translated into the objective of facilitating Europol's cooperation with third countries:
  - Limiting the **scope of persons** potentially covered by a category of transfers of personal data to persons who are involved in or otherwise linked to the specific criminal offence for the investigation of which personal data is transferred, in line with the categories of personal data and categories of data subjects set out in annex II of the Europol Regulation.
  - For each personal data to be transferred as part of the category of transfers of personal data, such transfer must be strictly necessary and proportionate to fulfil the overall purpose of the cooperation with the third country in the specific situation.
  - All requirements and safeguards set out in the existing provision of the Europol Regulation on transfer of personal data in specific situations will apply to each personal data to be transferred as part of the category of transfers of personal data. This includes the prohibition to transfer such data if the Fundamental Rights and freedoms of the data subject concerned override the public interest in the transfer. The transfer of personal data is strictly time-limited to what is necessary to fulfil the purpose of the category of transfers of personal data in a specific situation. Once the purpose of the category of transfers of personal data in a specific situation is fulfilled, no further personal data can be transferred on that legal ground.

6) effectiveness in meeting the policy objectives [+]

- The policy option partially meets the objective of facilitating operational cooperation between Europol and third countries including the transfer of personal data where this is necessary for law enforcement and EU internal security, as it facilitates the transfer of personal data in specific situations.
- At the same time, such specific situations (e.g. individual investigations, imminent threat to public security) cover a large number of the operational needs of law enforcement authorities, as shown by Member State authorities' use of such derogations.

7) efficiency in meeting the policy objectives [+]

- National competent authorities in the Member States will save valuable and indispensable resources. It will reduce the costs for national authorities as they will benefit from Europol's cooperation with third countries.

8) legal/technical feasibility [+]

- As the policy option consists of an alignment of the provision on the transfer of personal data in specific situations with the respective provision in the Data Protection Law Enforcement Directive, it is considered a feasible way forward.

9) political feasibility [+]

- As this option aims to improve Europol's cooperation with third countries thus overall enhancing the support Europol can give to Member States therefore, wide support is expected. The position of the European Parliament is not clear at this stage.

10) coherence with other measures [0]

- Not applicable.

Policy option 12: **seeking best practices and guidance on the application of provisions of the Europol Regulation**

Expected impact of policy option 12[241]
1) impact on citizens [++]
• Best practices and guidance on the application of the Europol Regulation for the cooperation with third countries might enhance that cooperation and therefore EU internal security, which would have a positive impact on citizens.
2) impact on national authorities [+]
• Best practices and guidance on the application of the Europol Regulation for the cooperation with third countries might enhance that cooperation and therefore enable Europol to better support Member States with the result of its cooperation with third countries.
3) impact on EU bodies [+]
• Best practices and guidance on the application of the Europol Regulation for the cooperation with third countries might enhance that cooperation and therefore enable Europol to better support Member States with the result of its cooperation with third countries.
4) impact on businesses [0]
• There is no impact on businesses.
5) impact on Fundamental Rights [0]
• Policy option 12 does not provide for any new legal grounds for Europol for the processing of personal data. It does not limit any Fundamental Right. Any processing of personal data from Europol and a third country would take place on the basis of the current Europol Regulation, in line with all the requirements, limitations and safeguards set out therein.
6) effectiveness in meeting the policy objectives [0]
• The policy option is only partially effective in meeting the policy objectives. Guidance by the European Data Protection Supervisor on the effective application of the provision in the current Europol Regulation on a self-assessment of the adequate level of safeguards might indeed enable Europol to address the current under-use of this provision. • However, best practices from Member States on how they apply the provision in the Data Protection Law Enforcement Directive on the transfer of personal data in specific situations would only bring added value if the respective provision in the Europol Regulation was aligned with the provision in the Data Protection Law Enforcement Directive (policy option 10).
7) efficiency in meeting the policy objectives [+]
• National competent authorities in the Member States will save valuable and indispensable resources. It will reduce the costs for national authorities as they will benefit from Europol's cooperation with third countries.
8) legal/technical feasibility [+]
• No legal obstacles foreseen. On the technical level, it will be feasible to conduct research into best practices and guidance among Member States and not require much resources.
9) political feasibility [+]

[241] The impacts are assessed on a scale ranging from 'very positive impact' (++) to 'very negative impact' (--), with intermediate scores: 'positive impact' (+), 'no impact' (0) and 'negative impact' (-).

• Seeking best practices and guidance is expected to be supported.
10) coherence with other measures [0]
• Not applicable.

5. HOW DO THE OPTIONS COMPARE?

Comparative assessment for the objective: facilitating Europol's cooperation with third countries			
	option 10	option 11	option 12
1) impact on citizens	+	+	++
2) impact on national authorities	+	+	+
3) impact on EU bodies	+	+	+
4) impact on businesses	0	0	0
5) impact on Fundamental Rights	0	0	0
6) effectiveness in meeting the policy objectives	-	+	0
7) efficiency in meeting the policy objectives	-	+	+
8) legal/technical feasibility	0	+	+
9) political feasibility	-	**+**	+
10) coherence with other measures	**0**	**0**	**0**
preferred policy options		**X**	**X**

Given that the requirement of essential equivalence as set by CJEU case law[242] applies to any transfer of personal data to third countries and hence irrespective of any change to the provision on self-assessment of the adequate level of safeguards, the changes foreseen by **policy option 10** would not provide any new legal ground for the transfer of personal data. Consequently, the policy option would not be effective in meeting the policy objective of facilitating Europol's cooperation with third countries. Instead, the European Parliament would oppose any changes to the provisions on self-assessment of the adequate level of safeguards as an attempt to bypass the legal ground for the transfer of personal data provided by an international agreement on the basis of Article 218 TFEU, and hence of the European Parliament's right to give consent.

Policy option 11 partially meets the objective of facilitating operational cooperation between Europol and third countries including the transfer of personal data where this is necessary for law enforcement and EU internal security, as it facilitates the transfer of personal data in specific situations. **Policy option 12** complements that with guidance by the European Data Protection Supervisor on the effective application of the provision in the current Europol Regulation on a self-assessment of the adequate level of safeguards. This might indeed enable Europol to address the current under-use of this provision. However, best practices from

[242] Opinion 1/15, *EU-Canada PNR Agreement*, EU:C:2017:592 (26.7.2017); judgment of 6 October 2015, *Schrems*, C- 362/14, EU:C:2015:650; judgement of 16 July 2020, C- 311/18, *Schrems II*, EU:C:2020:559.

Member States on how they apply the provision in the Data Protection Law Enforcement Directive on the transfer of personal data in specific situations, as also foreseen under **policy option 12**, would only bring added value if the respective provision in the Europol Regulation was aligned with the Data Protection Law Enforcement Directive as foreseen under **policy option 11**. Both policy options are also efficient as they would reduce the costs for national authorities as they will benefit from Europol's cooperation with third countries.

Consequently, the effective and preferred option is **combination of policy options 11 and 12**.

Annex 8: Europol's capacity to request the initiation of criminal investigations

1. PROBLEM DEFINITION

1.1. What is the problem?

Serious and organised crime is a key threat to the security of the European Union. It concerns not only forms of crime that affect two or more Member States. It also includes crimes that involve only one Member State, but affect a common interest covered by a Union policy, such as the rule of law.[243]

These crimes affect not only the Member State where they are manifested but in fact all the Member States and the foundations of the Union, which is built on shared values and expected to provide European policies to the benefit of the European citizens.[244] These crime threats transcend national boundaries, diffuse and permeate European societies and require a collective response. Thus, the Union has a shared stake and a key role to play in supporting Member States to effectively address them. Such cases investigated individually by Member States can be high profile, complex, sensitive and draw wide public, media and political attention across the EU. They are also resource-demanding and require advanced expertise. Consequently, action and cooperation at the national level is not always enough to effectively address them.

An EU-level strengthened, proactive and bespoke operational support offered to the Member States investigating crimes affecting a common interest covered by a Union policy, except facilitating and stepping up Member States' continuous efforts to tackle such complex crimes, would enhance legality, transparency, accountability, impartiality and quality of the investigations[245] of these high profile and sensitive cases, building more trust to public institutions and safeguarding citizens' right to security.

The Treaty of the Functioning of the European Union in Article 88(1), provides for such a specific role for Europol, by recognising that Europol's mission shall be to support and strengthen action by the Member States' law enforcement authorities in preventing and combating not only serious crime affecting two or more Member States and terrorism, but

---

243 The rule of law is enshrined in Article 2 of the Treaty on European Union as one of the common values for all Member States. The EU is based on the rule of law. Strengthening the rule of law is a priority for an effective functioning of the Union. Threats to the rule of law challenge its legal, political and economic basis. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 2020, Rule of Law Report, The rule of law situation in the European Union, COM(2020) 580 final (30.9.2020). *'The rule of law helps protect people from the rule of the powerful. It is the guarantor of our most basic of every day rights and freedoms. It allows us to give our opinion and be informed by a free press'.* President von der Leyen, State of the Union Address 2020.

244 For instance, the rule of law has a direct impact on the life of every citizen. It is a precondition for ensuring equal treatment before the law and for the defence of citizens' rights. It is essential to the implementation of EU laws and policies, and central to a Union of equality, opportunity and social fairness.

245 The rule of law includes such principles. These principles have been recognised by the European Court of Justice and the European Court of Human Rights. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 2020, Rule of Law Report, The rule of law situation in the European Union, COM(2020) 580 final (30.9.2020).

also forms of crime which affect a common interest covered by a Union policy. This is reflected in Europol's objectives in Article 3(1) of the Europol Regulation (EU) 2016/794. Europol achieves its objectives through a series of tasks[246] (e.g. notifying Member States of any information concerning them, providing analytical support).

Recent experience has demonstrated the benefits of Europol's role in supporting individual Member States' investigations concerning high profile sensitive cases that drew extensive public, media and political attention across the EU.[247] Indeed, Europol has the tools, services and capabilities to provide an EU-level advanced operational support to these investigations.[248]

However, the current Europol mandate only foresees a rather light form of engagement between Europol and the Member State concerned in such cases. This notably concerns the ability of Europol to request the initiation of criminal investigations, which is indispensable in providing a proactive and tailored-made support, flagging to the Member States crimes which affect a common interest covered by a Union policy, requesting them to initiate an investigation and supporting it. Bringing these cases to the attention of the Member States is the first step in taking action.

In that respect, a European Parliament Resolution of July 2020 stated that "*strengthening Europol's capacity to request the initiation of cross-border investigations, particularly in cases of serious attacks against whistleblowers and investigative journalists who play an essential role in exposing corruption, fraud, mismanagement and other wrongdoing in the public and private sectors, should be a priority*".[249]

Likewise, a March 2019 European Parliament Resolution called on the Commission "*to strengthen the mandate of Europol so as to enable it to participate more proactively in investigations into leading organised crime groups in Member States where there are serious doubts about the independence and quality of such investigations*".[250]

1.2. What are the problem drivers?

Crimes that affect a common interest covered by a Union policy affect all the Member States. Potential gaps in the investigation of such crimes in one Member State are gaps in the security of all Member States and the Union itself. Furthermore, as these cases investigated individually by Member States can be high profile, complex, resource-demanding, sensitive

246 '*Europol's tasks are closely connected with maintaining law and order and safeguarding internal security – a core area of Member State sovereignty'.* Declaration of the Home Affairs Ministers of the European Union 'Ten points on the Future of Europol', Berlin, 21.10.2020.

247 In the December 2019 European Parliament Resolution on the Rule of Law in Malta, after the revelations around the murder of Daphne Caruana Galizia, the European Parliament reiterated its call for the full and continuous involvement of Europol in all aspects of the murder investigation and all related investigations, and called for Europol's involvement to be reinforced as it yields results. Similar calls came from civil society (see the letter by the Committee to Protect Journalists: https://cpj.org/2020/05/malta-attorney-general-europol-murdered-daphne-caruana-galizia/).

248 Article 4(1) of Europol Regulation (EU) 2016/794.

249 European Parliament resolution of 10 July 2020 on a comprehensive Union policy on preventing money laundering and terrorist financing (2020/2686(RSP)).

250 European Parliament resolution of 28 March 2019 on the situation of the rule of law and the fight against corruption in the EU, specifically in Malta and Slovakia (2018/2965(RSP)). The European Parliament also observed in this Resolution that the current budgetary and human resources and mandate of Europol is not sufficient for the agency to provide full and proactive EU added value in carrying out investigations such as in the cases of the murders of Daphne Caruana Galizia and of Ján Kuciak and Martina Kušnírová.

and draw wide public, media and political attention across the EU, the problem of the insufficient support of these investigations cannot be solved at the national level. The investigations of crimes affecting the EU as a whole requires EU-level support.

This EU-level proactive, advanced and tailored-made operational support to the Member States in investigating crimes affecting a common interest covered by a Union policy can only be provided by Europol, due to the nature of the support (i.e. operational support to Member States' criminal investigations). Europol's capacities stemming from its current mandate is the place to search and identify the drivers of the problem.

Europol's current mandate does not allow Europol to address holistically the insufficient support to individual Member States' investigations. Europol's overall objectives include the support to Member States for forms of crime which affect a common interest covered by a Union policy, and hence, also the support for investigating such crimes if they only affect one Member State.[251] However, Europol's ability to request the initiation of a criminal investigation in a Member State is limited to specific cases where cross-border cooperation would add value, which excludes high profile cases that only affect one Member State.[252]

The European Parliament called for "*strengthening Europol's capacity to request the initiation of cross-border investigations, particularly in cases of serious attacks against whistleblowers and investigative journalists who play an essential role in exposing corruption, fraud, mismanagement and other wrongdoing in the public and private sectors, should be a priority*".[253] This suggests that the related provisions in the Europol Regulation are insufficient in enabling Europol to identify and support such cases.[254]

1.3. How will the problem evolve without intervention?

Without any intervention, the aforementioned problem will persist or even increase over time. The criminal cases national authorities need to investigate become more and more complex and demanding. Law enforcement authorities often have to analyse large volume of data, decrypt communications and uncover the business model of sophisticated and polycriminal organised crime groups and individual criminal entrepreneurs. The use of corruption, modern technology, countermeasures, violence and extortion are only some of the means at the disposal of contemporary criminals.[255]

2. OBJECTIVES: WHAT IS TO BE ACHIEVED?

2.1. Specific objectives

In the context of the general objectives of this initiative which result from the Treaty-based goals,[256] the specific objective to be achieved is to strengthen Europol's capacity to request the

---

251 Article 3(1) of Regulation (EU) 2016/794 that mirrors Article 88(1) TFEU. Moreover, recital 6 of Europol Regulation mentions that Europol, as the Union law enforcement agency, should also support and strengthen actions and cooperation in tackling forms of crime that affect the interests of the Union. However, it should be noted that this possibility provided by the Europol Regulation is currently underused.

252 Article 6 of Regulation (EU) 2016/794 in conjunction with recital 11 of that Regulation.

253 European Parliament resolution of 10 July 2020 on a comprehensive Union policy on preventing money laundering and terrorist financing (2020/2686(RSP)).

254 Article 6 of Regulation (EU) 2016/794.

255 2017 EU Serious and Organised Threat Assessment.

256 According to Articles 67 and 88 TFEU, these goals are: a) for Europol to support and strengthen action by the Member States' law enforcement authorities and their mutual cooperation in preventing and combating

initiation of criminal investigations, in full respect of Member States' prerogatives[257] on maintaining law and order and safeguarding internal security.

This objective raises the policy choice whether to strengthen the mechanism foreseen under the current Europol Regulation for requesting the initiation of cross-border investigations or enabling Europol to request Member States the initiation of criminal investigations in cases affecting only one Member State.

3. WHAT ARE THE AVAILABLE POLICY OPTIONS?

3.1. Baseline representing current situation

The baseline is a 'no policy change' scenario. In regards to Europol's capability to **request the initiation of investigations** in specific cases, the baseline scenario assumes that the provisions of Article 6 of the Europol Regulation (EU) 2016/794 remain unchanged. This means that Europol, in specific cases where it considers that a criminal investigation should be initiated on a crime falling within the scope of its objectives, it shall request the competent authorities of the Member States concerned to initiate, conduct or coordinate such a criminal investigation. Following recital 11 of Europol Regulation, Europol should be able to make such requests in specific cases where cross-border cooperation would add value.

3.2. Description of policy options requiring a regulatory or non-regulatory intervention

The impact assessment will assess two policy options to strengthen Europol's capacity to request the initiation of criminal investigations. As the problem and its drivers relate to the limitations identified in the Europol legal mandate, the available policy option cannot but focus on the agency's mandate.

***Policy option 13*:**

This policy option addresses the problem of insufficient support to individual Member States in high profile cases by **strengthening the mechanism for requesting the initiation of cross-border investigations**, namely by changing the mechanism of Article 6[258] of the Europol Regulation (regulatory intervention). This change would foresee that in case a Member State would decide not to accede to a request made by Europol for the initiation of an investigation, Europol could bring the matter to the attention of the Europol Management Board or, eventually, to the Council. This policy choice originates from reflection on the current Europol Regulation. It raises the political choice whether Europol should be entitled to

---

serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy; b) to endeavour to ensure a high level of security through measures to prevent and combat crime.

257 Article 4(2) TEU and Article 72 TFEU.

258 According to Article 6 of Europol Regulation, in specific cases where Europol considers that a criminal investigation should be initiated into a crime falling within the scope of its objectives, it shall request the competent authorities of the Member States concerned via the national units to initiate, conduct or coordinate such a criminal investigation. The national units shall inform Europol without delay of the decision of the competent authorities of the Member States concerning any such request. If the competent authorities of a Member State decide not to accede to this request made by Europol, they shall inform Europol of the reasons for their decision without undue delay, preferably within one month of receipt of the request. 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.

continue pursuing the initiation and conduct of an investigation by a Member State after its decision to accede to Europol's request.

***Policy option 14*:**

This policy option addresses the problem of insufficient support to individual Member States in high profile cases by **enabling Europol to request Member States the initiation of criminal investigations in cases affecting only one Member State** that concern forms of crime that affect a common interest covered by a Union policy. This would entail clarifying, in the Europol Regulation, that the entire scope of the objectives of Europol set out in Article 3(1)[259] and hence, crimes that only involve one Member State but have an effect on the Union as a whole, applies also to Europol's possibilities to request the initiation of criminal investigations. More specifically, this regulatory intervention would modify recital 11 of Europol Regulation[260] in order to cover not only cases where cross-border cooperation would add value but also cases of crimes, which affect a common interest covered by a Union policy. This policy choice which also originates from reflection on the current Europol Regulation does not complement policy option 1 and represents a genuine alternative. It raises the political choice whether Europol should be entitled to request the initiation of criminal investigations in cases affecting only one Member State that concern forms of crime that affect a common interest covered by a Union policy, similarly to specific cases where cross-border cooperation would add value.

4. WHAT ARE THE IMPACTS OF THE POLICY OPTIONS?

***Policy option 13*: strengthening the mechanism for requesting the initiation of investigations**

Expected impact of policy option 13[261]
1) impact on citizens [+]
• Indirect positive impact to the security of the EU citizens and societies. It will clear up any doubts on the independence and quality of investigations, build more public-trust to the Member States' criminal justice systems and safeguard citizens' right to security. However, this policy option will cover only cross-border cases as it will change only the current mechanism for requesting the initiation of cross-border investigations, which does not cover crimes that affect a common interest covered by a Union policy (according to recital 11 of Europol Regulation). • Slight negative impact on EU citizens, as some citizens might object considering this policy as the Union intervening in the internal matters and sovereignty of their country, and its prerogative to initiate and conduct criminal investigations.
2) impact on national authorities [0]
• Direct positive impact to national law enforcement and judicial authorities investigating serious organised crime in the Member States. Benefit from Europol's enhanced capabilities and resources to provide specialised operational support and expertise, in particular in complex,

259 Article 3(1) of Regulation (EU) 2016/794 refers to '*forms of crime which affect a common interest covered by a Union policy'*.

260 Recital 11 of Regulation (EU) 2016/794: '*Europol should be able to request Member States to initiate, conduct or coordinate criminal investigations in specific cases where cross-border cooperation would add value. Europol should inform Eurojust of such requests'.*

261 The impacts are assessed on a scale ranging from 'very positive impact' (++) to 'very negative impact' (--), with intermediate scores: 'positive impact' (+), 'no impact' (0) and 'negative impact' (-).

polycriminal, time-consuming and resource-demanding high-profile cases.

- Direct positive impact to valuable and indispensable resource allocation by the national competent authorities. Positive impacts refer only to cross-border cases.
- Significant negative impact on national law enforcement and judicial authorities. Establishes 'another layer of pressure' to the one of Article 6(3) of the Europol Regulation. Can be considered as an intervention in the prerogative of the national competent authorities to initiate criminal investigations. Involvement of the Council can be considered as an intervention of the political level to the judicial and executive ones (in contrary to the independence of the powers). Consultation revealed that Member States strongly oppose any change to the mechanism of Article 6.

3) impact on EU bodies [+]

- Significant direct impact to Europol, as it enhances its role as the EU information hub and a provider of agile operational support to the Member States. However, it will not expand its capability to request the initiation of criminal investigations to cases that do not have a cross-border nature.
- Entails administrative and logistical costs to Europol, as one of its tasks will practically expand in scope.

4) impact on businesses [+]

- Indirect positive impact on businesses. The option will enhance security in the EU, taking into account that maintaining a secure environment is an important prerequisite for conducting business.

5) impact on Fundamental Rights [0]

- It **does not limit any fundamental right** and **promotes the rights of victims of crime**.
- Policy option 13 does not provide for any new legal grounds for Europol for the processing of personal data. Any processing of personal data between Europol and the Member State concerned, in the context of Europol's request for the initiation of criminal investigations takes place on the basis of the current Europol Regulation. All safeguards applicable under this Regulation to mitigate the limitation of Fundamental Rights apply.
- Policy option 13 promotes the rights of victims of crime. According to case law of the European Court of Human Rights, states are under a positive obligation to ensure that national criminal law provides for the prosecution and punishment of violations of certain rights. Such a duty to investigate, and where justified to prosecute, is affirmed in relation to victims whose Fundamental Rights have been violated. Strengthening the mechanism under which Europol would request the initiation of criminal investigations might lead to the opening of investigations, and where to justified prosecutions, in cases where Member States' authorities would otherwise not have taken action.

6) effectiveness in meeting the policy objectives [+]

- Partially an effective option. It will enhance the mechanism of Article 6, but it will not fully address the problem. Recital 11 of Europol Regulation points that Article 6 applies in cases where cross-border cooperation would add value, which does not cover crimes that affect a common interest covered by a Union policy.

7) efficiency in meeting the policy objectives [+]

- Partially efficient option in terms of Member States benefiting from Europol enhanced capabilities and resources to provide specialised operational support and expertise, in particular in complex, polycriminal, time-consuming and resource-demanding high-profile cases. National competent authorities in the Member States will save valuable and indispensable resources. However, positive efficiency impacts refer only to cross-border cases, as this policy option will

change only the current mechanism for requesting the initiation of cross-border investigations, which does not cover crimes that affect a common interest covered by a Union policy (according to recital 11 of Europol Regulation).
8) legal/technical feasibility [0]
• Not applicable as the option needs to be dismissed as result of the comparison with option 14.
9) political feasibility [--]
• Member States strongly oppose any amendment to the mechanism of Article 6. It introduces an escalation of Europol's ability to request the initiation of criminal investigations, which can be considered as an intervention in the aforementioned Member States' prerogative. It is doubtful whether such an option would gain the European Parliament's support. Its March 2019 and July 2020 Resolutions did not call for a change in the mechanism of Article 6 of the Europol Regulation.
10) coherence with other measures [0]
• Not applicable.

***Policy option 14*: enabling Europol to request the initiation of criminal investigations in cases affecting only one Member State that concern forms of crime which affect a common interest covered by a Union policy**

Expected impact of policy option 14[262]:
1) impact on citizens [+]
• Indirect positive impact to the security of the European citizens and societies. It will enhance the protection of common interests (e.g. the rule of law in the EU) and facilitate Member Sates' efforts to investigate serious organised crime and its key enablers (e.g. corruption). It will also clear up any doubts about the independence and quality of investigations. It will build more public-trust to the criminal justice systems of the Member States and safeguard citizens' right to security.
2) impact on national authorities [++]
• Direct positive impact to law enforcement and judicial authorities investigating serious organised crime in the Member States, which will benefit from Europol's enhanced capabilities and resources to provide specialised operational support and expertise (i.e. technical, forensic analytical), especially in serious, complex, polycriminal, time-consuming and resource-demanding high-profile cases. • Direct positive impact to valuable and indispensable resource allocation by the national competent authorities.
3) impact on EU bodies [+]
• Significant direct impact to Europol, as it enhances its role as the EU criminal information hub and a provider of agile operational support to the Member States. It will not affect the established mechanism of requesting investigations according to Article 6 of Europol Regulation. • It entails administrative and logistical costs to Europol, as one of its tasks will practically expand in scope.

[262] The impacts are assessed on a scale ranging from 'very positive impact' (++) to 'very negative impact' (--), with intermediate scores for 'positive impact' (+), 'no impact' (0) and 'negative impact' (-).

4) impact on businesses [+]

- Indirect positive impact on businesses, as it will enhance security in the EU. Maintaining a secure environment is an important prerequisite for conducting business. The improved fight against serious and organised crime will also help to protect the legal economy against infiltration by organised crime.

5) impact on Fundamental Rights [0]

- It **does not limit any fundamental right** and **promotes the rights of victims of crime**.
- Policy option 14 does not provide for any new legal grounds for Europol for the processing of personal data. Any processing of personal data between Europol and the Member State concerned, in the context of Europol' request for the initiation of criminal investigations takes place on the basis of the current Europol Regulation. All safeguards applicable under this Regulation to mitigate the limitation of Fundamental Rights apply.
- Policy option 14 promotes the rights of victims of crime. According to case law of the European Court of Human Rights, states are under a positive obligation to ensure that national criminal law provides for the prosecution and punishment of violations of certain rights. Such a duty to investigate, and where justified to prosecute, is affirmed in relation to victims whose Fundamental Rights have been violated. Enabling Europol to request the initiation of criminal investigations in cases affecting only one Member State extends the scope of application of Europol's related competence. This might lead to the opening of investigations, and where justified to prosecutions, in cases where Member States' authorities would otherwise not have taken action.

6) effectiveness in meeting the policy objectives [++]

- Very effective option that fully meets the policy objective. Empowering Europol to detect cases affecting only one Member State that concern forms of crime that affect a common interest covered by a Union policy, to request the initiation of investigations and support them would address the problem holistically and effectively. Member States' prerogative to launch investigations will remain, as the mechanism of Article 6 of Europol Regulation will not change, in line with the TFEU.

7) efficiency in meeting the policy objectives [++]

- Efficient option in terms of Member States benefiting from Europol's enhanced capabilities and resources to provide specialised operational support and expertise, in particular in complex, polycriminal, time-consuming and resource-demanding high-profile cases. National competent authorities in the Member States will save valuable and indispensable resources.

8) legal/technical feasibility [++]

- This option provides a feasible way to meet the objective of strengthening Europol's capacity to request the initiation of investigations. This option requires minimal changes by introducing a new recital clarifying the full scope of the existing article 6 of Europol Regulation.

9) political feasibility [++]

- It is expected to gain support in Member States, as it in conformity with the provisions of the TFEU and provides another supporting possibility to their benefit, without affecting the mechanism of Article 6 and their prerogative to initiate investigations.[263] Taking into account European Parliament Resolutions of March 2019[264] and July 2020[265] and relevant civil society

[263] *'Europol supports the national law enforcement authorities of the Member States, which retain exclusive executive power including the initiation and conducting of investigations'.* Declaration of the Home Affairs Ministers of the European Union 'Ten points on the Future of Europol', Berlin, 21.10.2020.

[264] European Parliament resolution of 28 March 2019 on the situation of the rule of law and the fight against corruption in the EU, specifically in Malta and Slovakia (2018/2965(RSP)) called on the Commission "*to*

calls, this option is also expected to receive support from the European Parliament, the Council and the public, respectively.
8) coherence with other measures [0]
• Not applicable.

5. HOW DO THE OPTIONS COMPARE?

Comparative assessment: strengthening Europol's capacity to request the initiation of criminal investigations		
	option 13	**option 14**
1) impact on citizens	+	+
2) impact on national authorities	0	++
3) impact on EU bodies	+	+
4) impact on businesses	+	+
5) impact on Fundamental Rights	0	0
6) effectiveness in meeting the policy objectives	+	++
7) efficiency in meeting the policy objectives	+	++
8) legal/technical feasibility	+	++
9) political feasibility	0	++
10) coherence with other measures	--	0
preferred policy options		**X**

Policy option 13 is a partially effective and efficient option. It will enhance the mechanism of Article 6, but it will not fully address the problem, as recital 11 of Europol Regulation points that Article 6 applies in cases where cross-border cooperation would add value, which does not cover crimes that affect a common interest covered by a Union policy. Member States will benefit from Europol's enhanced capabilities and resources to provide specialised operational support and expertise, in particular in complex, polycriminal, time-consuming and resource-demanding high-profile cases. National competent authorities in the Member States will save valuable and indispensable resources. However, positive efficiency impacts refer only to

strengthen the mandate of Europol so as to enable it to participate more proactively in investigations into leading organised crime groups in Member States where there are serious doubts about the independence and quality of such investigations. The European Parliament also observed in this Resolution that the current budgetary and human resources and mandate of Europol is not sufficient for the agency to provide full and proactive EU added value in carrying out investigations such as in the cases of the murders of Daphne Caruana Galizia and of Ján Kuciak and Martina Kušnírová.

265 The European Parliament called for "strengthening Europol's capacity to request the initiation of cross-border investigations, particularly in cases of serious attacks against whistleblowers and investigative journalists who play an essential role in exposing corruption, fraud, mismanagement and other wrongdoing in the public and private sectors, should be a priority." European Parliament resolution of 10 July 2020 on a comprehensive Union policy on preventing money laundering and terrorist financing (2020/2686(RSP)).

cross-border cases, as this policy option will change only the current mechanism for requesting the initiation of cross-border investigations, which does not cover crimes that affect a common interest covered by a Union policy (according to recital 11 of Europol Regulation).

Policy option 14 is both a very effective and efficient option. Empowering Europol to detect cases affecting only one Member State that concern forms of crime that affect a common interest covered by a Union policy, to request the initiation of investigations and support them would address the problem holistically and effectively. Member States' prerogative to launch investigations will remain, as the mechanism of Article 6 of Europol Regulation will not change, in line with the TFEU. Member States will benefit from Europol's enhanced capabilities and resources to provide specialised operational support and expertise, in particular in complex, polycriminal, time-consuming and resource-demanding high-profile cases. National competent authorities in the Member States will save valuable and indispensable resources. Furthermore, is expected to gain support in Member States, as it in conformity with the provisions of the TFEU and provides another supporting possibility to their benefit, without affecting the mechanism of Article 6 and their prerogative to initiate investigations. **Policy option 14 is the preferred policy option.**

Annex 9: Policy options discarded at an early stage

In the process of preparing the Impact Assessment, a several policy options were discarded at an early stage, notably because they were legally or otherwise not feasible, or because they would have a serious adverse impact on Fundamental Rights.

Objective I: Enabling effective cooperation between private parties and law enforcement authorities to counter the abuse of cross-border services by criminals

The impact assessment will not address the policy option to improve cooperation between Member States' law enforcement authorities and private parties within the existing framework by non-regulatory measures. During the consultation process, some law enforcement authorities noted that the exchange of personal data with private parties could be improved by sharing best practices among each other. Such an approach might indeed improve the way that law enforcement agencies issue their respective requests to private parties, and subsequently somewhat increase the response rate. However, it would not address the other problems of the current system, such as providing a point of contact for private parties in multi-jurisdictional cases or in cases where the jurisdiction is unclear, or ensuring that this type of data is shared with other Member States concerned. For these reasons, this policy option was discarded.

Objective II: Enabling law enforcement to analyse large and complex datasets to detect cross-border links, in full compliance with Fundamental Rights

The impact assessment will not address the policy option to remove the requirement[266] related to the specific categories of data subjects listed in annex II of the Europol Regulation. This policy option would undermine the existing level of data protection at Europol. The policy option would have a serious adverse impact on Fundamental Rights that justifies discarding the policy option.

Likewise, this impact assessment will not address the policy option to take inspiration from the related but different provision of the Regulation[267] on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies that obliges the data controller to make a clear distinction, as far as possible, between the personal data of different categories of data subjects. While this provision provides more flexibility to the controller, it pursues a different goal compared to the safeguards in the Europol Regulation that limit the processing of personal data by Europol to the categories of data subjects listed in annex II of that Regulation (namely suspects, convicted criminals, potential future criminals, contacts and associates, victims, witnesses and informants). This policy option would also undermine the existing level of data protection at Europol.

Consequently, both policy options were discarded at an early stage.

Objective of annex 6: Providing frontline officers (police officers and border guards) with

[266] Article 18(5) of Regulation (EU) 2016/794 (11.5.2016). The categories of data subjects are listed in annex II of that Regulation.

[267] Article 73 of Regulation (EU) 2018/1725 (23.10.2018). A similar provision is set out in the Data Protection Law Enforcement Directive that obliges national law enforcement authorities "*to make a clear distinction between personal data of different categories of data subjects*" (Article 6 of Directive (EU) 2016/794 (27.4.2016)).

the result of the analysis of third-countries sourced information

The impact assessment will not address the policy option to foster the roll-out of QUEST. This non-regulatory policy option would facilitate the access and use of Europol's databases by investigators, criminal intelligence officers and analysts in the Member States, but not by frontline officers as the actual target group.

Likewise, this impact assessment will not address the policy option of encouraging Europol to request Member States to create alerts in the Schengen Information System on its behalf. This non-regulatory policy as a less intrusive measure is available that is equally effective option is already part of the baseline scenario and raises legal and operational concerns.

Objective of annex 7: Facilitating operational cooperation between Europol and third countries

One policy option to facilitate Europol's cooperation with third countries was discarded at an early stage, namely the policy option to introduce a provision inspired by the Data Protection Law Enforcement Directive[268] and by the legal mandate of Eurojust[269] that refer to "*appropriate safeguards with regard to the protection of personal data are provided for in a legally binding instrument*".

At EU level, a legally binding instrument for the transfer of personal data to a third country requires an international agreement under Article 218 TFEU.[270] The Europol Regulation already provides for this possibility.[271]

Objective of annex 8: Strengthening Europol's capacity to request the initiation of criminal investigations

A policy option in the context of strengthening Europol's capability to request the initiation of cross-border investigations which was dismissed at an early stage was extending the material scope of Article 6 of the Europol Regulation. This would entail a reference to cases that involve only one Member State but which have *repercussions at Union level* (cf. Article 3(6) of Eurojust Regulation 2018/1727). However, as the material scope of Article 6 is determined by the wording of Article 3(1) of the Europol Regulation on objectives, and given that the wording of Article 3(1) is mirroring Article 88(1) TFEU, there is legally no scope to extend the material scope of Article 6.

---

268 Article 37(1)(a) of Directive 2016/680 (27.4.2016).

269 Article 58(1)(a) of Regulation 2018/1727 (14.11.2018).

270 At national level, implementing the Data Protection Law Enforcement Directive, such legally binding instruments could be legally binding bilateral agreements. As regards the Eurojust Regulation, it remains unclear how the provision referring to a "legally binding instrument" could be applied, and it is therefore not used in practice.

271 Article 25(1)(b) of Regulation (EU) 2016/794 (11.5.2016). The Europol Regulation sets outs three ways to establish a structural cooperation with a third countries that would provide legal grounds based on which Europol could lawfully transfer personal data to authorities of that third countries: (1) a Commission adequacy decision adopted in accordance with Article 36 of Directive (EU) 2016/680; (2) an international agreement concluded by the Union pursuant to Article 218 TFEU; (3) an authorisation by the Europol Management Board, in agreement with the European Data Protection Supervisor, based on a self-assessment that adequate safeguards for the protection of privacy and fundamental rights exist.

Annex 10: Questionnaire

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.

1. 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.

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.

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.

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.

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.

Other

If other, please explain.

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.

2. 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.

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.

3. 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.

4. 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.

5. 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.

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.

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

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.

6. 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.

7. 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.

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.

8. 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.

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.

9. 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

Annex 11: Replies to the questionnaire[272]

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?

		Answers	Ratio
Yes		52	73.24 %
No		8	11.27 %
Other		11	15.49 %
No Answer		0	0 %

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?

		Answers	Ratio
Yes		55	77.46 %
No		1	1.41 %
Other		9	12.68 %
No Answer		6	8.45 %

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?

		Answers	Ratio
Yes		46	64.79 %
No		12	16.9 %
Other		7	9.86 %
No Answer		6	8.45 %

[272] The annex does not depict the answers to questions 7, 14, 18 and 20, as these questions allowed for free text responses only.

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

		Answers	Ratio
Risk of loss of information (e.g. where Europol does not have enough information to identify the Member State concerned).		36	50.7 %
Risk of delays (e.g. where the identification of the Member State concerned is difficult and time-consuming).		39	54.93 %
Lack of legal certainty for private parties, when they submit personal data to Europol.		29	40.85 %
Inability of Europol to support Member States law enforcement authorities in obtaining personal data from a private party outside their jurisdiction.		37	52.11 %
Other		3	4.23 %
No Answer		23	32.39 %

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?

		Answers	Ratio
Yes		36	50.7 %
No		14	19.72 %
Other		15	21.13 %
No Answer		6	8.45 %

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?

		Answers	Ratio
Yes		36	50.7 %
No		15	21.13 %
Other		13	18.31 %
No Answer		7	9.86 %

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)

		Answers	Ratio
Any such regime should be voluntary for the private parties concerned (i.e. no obligation to share personal data with Europol).		21	29.58 %
Any such regime should be in full compliance with fundamental rights (including a fair trial) and applicable European legislation on data protection.		48	67.61 %
Any such regime should clarify that private parties should not expect to receive information related to operational activities, because they are not state actors.		39	54.93 %
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).		36	50.7 %
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.		42	59.15 %
Other		12	16.9 %
No Answer		6	8.45 %

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?

		Answers	Ratio
Yes		34	47.89 %
No		13	18.31 %
Other		12	16.9 %
No Answer		12	16.9 %

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?

		Answers	Ratio
Yes		41	57.75 %
No		9	12.68 %
Other		11	15.49 %
No Answer		10	14.08 %

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?

		Answers	Ratio
Yes		34	47.89 %
No		9	12.68 %
Other		19	26.76 %
No Answer		9	12.68 %

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?

		Answers	Ratio
Yes		45	63.38 %
No		7	9.86 %
Other		7	9.86 %
No Answer		12	16.9 %

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?

		Answers	Ratio
Yes		29	40.85 %
No		26	36.62 %
Other		9	12.68 %
No Answer		7	9.86 %

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

		Answers	Ratio
Yes		28	39.44 %
No		13	18.31 %
Other		18	25.35 %
No Answer		12	16.9 %

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?

		Answers	Ratio
Yes		37	52.11 %
No		13	18.31 %
Other		13	18.31 %
No Answer		8	11.27 %

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?

		Answers	Ratio
Yes		41	57.75 %
No		4	5.63 %
Other		11	15.49 %
No Answer		15	21.13 %

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

		Answers	Ratio
Yes		33	46.48 %
No		24	33.8 %
Other		7	9.86 %
No Answer		7	9.86 %

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

		Answers	Ratio
Yes		37	52.11 %
No		8	11.27 %
Other		15	21.13 %
No Answer		11	15.49 %

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

		Answers	Ratio
Yes		53	74.65 %
No		4	5.63 %
Other		5	7.04 %
No Answer		9	12.68 %