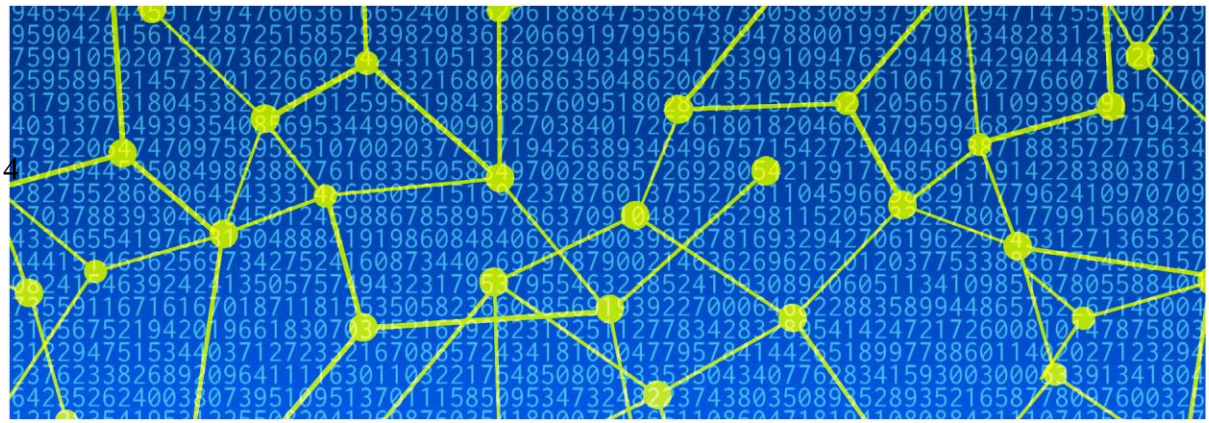
4



EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 4/2021

EDPS Opinion on the Proposal for Amendment of the Europol Regulation

EDPS

8 March 2021

The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 52(2) of Regulation 2018/1725 '[w]ith respect to the processing of personal data […] for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to data protection, are respected by Union institutions and bodies', and under Article 52(3)' […] for advising Union institutions and bodies and data subjects on all matters concerning the processing of personal data'.

Wojciech Wiewiorówski was appointed as Supervisor on 5 December 2019 for a term of five years.

Under Article 42(1) of Regulation 2018/1725, the Commission shall 'following the adoption of proposals for a legislative act, of recommendations or of proposals to the Council pursuant to Article 218 TFEU or when preparing delegated acts or implementing acts, consult the EDPS where there is an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data'. Furthermore, under article 57(1)(g), the EDPS shall 'advise on his or her own initiative or on request, all Union institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to the processing of personal data'.

This Opinion is issued by the EDPS, within the period of eight weeks from the receipt of the request for consultation laid down under Article 42(3) of Regulation (EU) 2018/1725, having regard to the impact on the protection of individuals' rights and freedoms with regard to the processing of personal data of the Commission Proposal for a Regulation of the European Parliament and of the Council on 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

Executive Summary

On 9 December 2020, the European Commission presented a Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation. The legislative proposal aims at strengthening and in certain cases extending the mandate of Europol, in response to the changes in the security landscape and the evolving and increasingly complex threats.

The EDPS understands the need for the law enforcement authorities to benefit from the best possible legal and technical tools to accomplish their tasks, which are to detect, investigate and prevent crimes and other threats to public security. Moreover, he is convinced that there is no inherent and irreconcilable conflict between security and fundamental rights, including the right to data protection. Therefore, the current Opinion aims at providing a fair and objective assessment of the necessity and proportionality of the proposed measures, accompanied by a number of specific recommendations for ensuring the right balance between the values and interests at stake.

Criminal investigations and criminal intelligence operations increasingly include the collection and processing of large and complex datasets by law enforcement authorities. While the EDPS positively notes the safeguards that accompany the proposed derogations in such cases, he is concerned that the exceptions from the current data protection rules, applicable to Europol, could become in reality the rule. Therefore, he recommends that the Europol Regulation should better define the situations and the conditions, in which Europol may resort to the proposed derogations. Furthermore, even in these cases, the processing of personal data by the Agency should be fully compliant with the general principles and obligations laid down in Chapter IX of Regulation (EC) No 2018/1725.

Regarding the extended legal possibilities for Europol to cooperate with private parties, in particular in the case of multi-jurisdictional or non-attributable datasets, the EDPS appreciates that they are counter-balanced with specific safeguards, such as the prohibition of systematic, massive or structural transfers of data. At the same time, the EDPS recommends this important restriction to be applied to all exchanges between Europol and private parties, irrespective of their location - within or outside the EU. The EDPS also considers that the exact legal role and responsibilities of Europol, when acting as service provider to national authorities and thus data processor, should be further clarified in a binding legal act. In addition, he sees a need for an assessment of the possible security risks created by the opening of Europol's communication infrastructure for use by private parties.

The EDPS also pays special attention to the envisaged use of personal data by Europol for research and innovation purposes. At the same time, he is well aware that the alternative - Europol and the national law enforcement authorities to rely on tools and products developed by external vendors, often situated outside the EU, clearly poses much higher risks with regard to fundamental rights. Notwithstanding this, the EDPS considers that the new processing purpose is too broadly defined and recommends the scope of the research and innovation activities to be clarified in a binding document.

The EDPS welcomes and fully supports the proposed further strengthening of the data protection framework of Europol and in particular the direct application of the horizontal rules in Chapter IX of Regulation (EC) No 2018/1725 to the operational data processing by the

Agency. It is also an important step towards a comprehensive alignment of the data protection framework for all EU institutions, bodies and agencies, for which the EDPS has repeatedly called for.

With a stronger mandate of Europol should always come a stronger oversight. Therefore the EDPS calls for a full harmonisation of his supervisory powers vis-a-vis Europol with the general powers of the EDPS provided for in Regulation (EU) 2018/1725 and applicable to the other EU institutions, agencies and bodies, including the European Parliament, the Council and the Commission. Such alignment would be consistent with the will of the EU legislator and would also help avoiding a differentiated treatment of the Union bodies and placing them in a more or less privileged position.

TABLE OF CONTENTS

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)[1],

Having regard to Regulation (EC) No 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (hereinafter referred to as "EUDPR")[2], and in particular Article 42(1) thereof,

Having regard to Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA[3],

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION AND BACKGROUND

1. The European Union Agency for Law Enforcement Cooperation (Europol) was established by Regulation (EU) 2016/794 of the European Parliament and of the Council (the Europol Regulation) to support and strengthen action by the competent authorities of the Member States and their mutual cooperation in preventing and combating serious cross-border crime, terrorism and other criminal activities which affect the common interests of the Union. The Europol Regulation replaced the previous basic legal act - Council Decision 2009/371/JHA[4], and granted the EDPS the task of supervising the lawfulness of personal data processing by Europol as of 1 May 2017.

2. On 9 December 2020, the European Commission adopted a Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation[5].

3. The proposal has been included in the Commission Work Programme for 2020 as a legislative initiative to "strengthen the Europol mandate in order to reinforce operational police cooperation". It is also one of the key actions of the EU Security Union Strategy, presented in July 2020[6]. Furthermore, the legislative proposal is part of a package of measures, announced by the Commission on 9 December 2020, to reinforce the Union's response to the threat posed by terrorism[7].

4. The aim of the proposal is to strengthen and, where deemed necessary, extend the mandate of Europol within the mission and tasks of the Agency as laid down in Article 88 of the Treaty on the Functioning of the EU (TFEU). The three main areas, addressed by the proposal, are explicitly mentioned in the title of the draft Regulation, namely cooperation with private parties, operational support of criminal investigations, and research and innovation. However, there are a number of additional changes of other important aspects of the work of Europol, such as the legal regime on data protection, transfers of data to third countries, entering of alerts in the Schengen Information System, etc. The latter element is subject to a separate legislative proposal[8], on which the EDPS has also been consulted and has commented in a separate Opinion.

5. According to the Explanatory Memorandum, the legislative proposal is a response to the changes in the security landscape and the evolving and increasingly complex threats, including exploitation by criminal groups of the digital transformation, new technologies and the COVID-19 crisis. In this context, the Commission recalls several recent political statements by the Council and the European Parliament, which specifically address the need for further strengthening of Europol's mandate and capacity[9].

6. The EDPS was consulted informally by the Commission on several occasions throughout the process of preparation of the legislative proposal, lastly on 25 November 2020, and communicated his informal comments. He welcomes the fact that his views have been sought at an early stage of the procedure and encourages the Commission to continue with this good practice. In addition, on 9 October 2020 the EDPS organised an expert webinar "The Europol reform: the data protection perspective", with special focus on the alignment of the data protection provisions in the Europol Regulation with the general rules on the processing of operational personal data.

7. The EDPS was formally consulted by the Commission on 7 January 2021 on the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/794, and has adopted the current Opinion in accordance with Article 42(3) of Regulation (EC) No 2018/1725.

2. GENERAL COMMENTS

8. The consistent enforcement of the data protection rules in the Area of Freedom, Security and Justice, as well as identifying the discrepancies in the standards of processing of operational personal data within the EU are among the key objectives of the EDPS 2020-2024 Strategy "Shaping a Safer Digital Future: a new Strategy for a new decade"[10]. As an advisor to the Union institutions, offices, bodies and agencies and at the same time an enforcer of data protection and privacy rules, the EDPS is uniquely positioned to monitor whether their powers are designed and used in full respect of the legal framework and the fundamental rights of the individuals.

9. The EDPS understands the need for the law enforcement bodies to benefit from the best possible legal and technical tools to accomplish their tasks that are to detect, investigate and prevent crimes and other threats to public security. The right to data protection is not an absolute right and interferences with it may be justified, provided that they remain limited to what is necessary and proportionate in a democratic society, in line with Article 52(1) of the Charter of Fundamental Rights.

10. The EDPS is convinced that there is no inherent and irreconcilable conflict between security and fundamental rights, including the right to data protection. Instead of looking at the problem through the lenses of an abstract and rather false dichotomy, he considers that the best approach is to conduct a fair and objective assessment of the necessity and proportionality of the proposed measures. In this regard, the EDPS welcomes the use by the Commission of the Necessity Toolkit and Guidelines on proportionality, developed by the EDPS[11], when conducting the impact assessment accompanying the legislative proposal[12].

11. The strengthening of Europol's mandate should also be viewed in a wider political context. On the one hand, a more prominent and proactive role of Europol in prevention and investigation of serious crimes will fit into the strategic trend for a more assertive protection of the common interests of the Union, which has led to the establishment of the European Public Prosecutor Office (EPPO), transformation of Frontex into a European Border and Coast Guard, and of EASO into a European Union Agency for Asylum. On the other hand, it raises the question whether the legal framework for oversight of Europol and the existing legal avenues for judicial redress are sufficient and adequate for the new role of the Agency.

12. The EDPS stresses that any legislative change should take into account the need for consequential arrangements to achieve the right balance between the values and interests at stake. In particular, with a stronger mandate should always come stronger oversight of the Europol**.** The EDPS also encourages the EU legislator to look for future-proof solutions in a rapidly changing world.

13. The EDPS notes that one of the key elements of the system of safeguards, designed to counter-balance the strengthened powers of Europol, is the extended role of the EDPS, in, *inter alia*, assessing the proportionality and lawfulness of the personal data received from third countries (Article 18a(4)), approving the extension of the maximum period of pre-analysis of big datasets (Article 18(5a)), or following the research and innovation projects (Article 33a(1)(b)). While the EDPS does not shy away from additional responsibility, he wishes to insist on the fact that **the effective implementation of the new tasks requires the availability of the necessary resources - both human and technical**[13]. Even more crucial than the number of available staff, are the skills of the experts, who should cover a very broad range of issues - from criminal investigations and police cooperation to big data analytics and AI. The same fully applies for the national supervisory authorities, which, pursuant to Article 44(2), would carry out joint inspections of the Agency together with the EDPS.

14. This Opinion also contains specific recommendations to ensure that the limitations to the fundamental rights and freedoms of the individuals concerned, in particular to the rights to privacy and data protection, in relation to the fight against serious crimes and terrorism, are limited to what is strictly necessary[14].

3. SPECIFIC RECOMMENDATIONS

3.1. Cooperation with private parties

15. Currently, Europol is allowed to exchange personal data with private parties, subject to specific conditions, pursuant to Article 26 of Regulation (EU) 2016/794. The proposed amendments extend the legal possibilities for such exchange, in particular in the case of multi-jurisdictional or non-attributable datasets.

16. A new element in the proposal is the support of Europol to Member States in preventing the large scale dissemination, via online platforms, of terrorist content related to on-going or recent real-world events depicting harm to life or physical integrity, or calling for imminent harm to life or physical integrity. To this end, Europol would serve as a channel for the exchange of personal data with private parties, including hashes, IP addresses or URLs related to such content (new Article 26a).

17. The EDPS welcomes the choice of the Commission to discard as not proportionate the other policy options, which would have allowed Europol to query databases managed by private parties, or to request directly personal data held by them on its own initiative. Moreover, such powers would not have been compatible with the restriction in Article 88(3) TFEU, which excludes the application of coercive measures by Europol.

18. The EDPS also positively notes that, in order to counter-balance the new powers of Europol, the proposal maintains the existing specific safeguards, e.g. the requirement for "absolute" or "strict" necessity (Article 26(5)), as well as introduces new ones, such as the **prohibition of systematic, massive or structural transfers** (Article 26(6), last subparagraph). However, as the latter relates only to cases of international transfers to private parties established outside the EU, **the EDPS recommends this safeguard to apply also to transmissions to private parties within the Union**.

19. The EDPS considers that the exact legal role and responsibilities of Europol, when acting as service provider to national authorities by offering its infrastructure for exchanges of data between Member States and private parties, are not sufficiently clear. In fact, the only guidance on this aspect is provided in a footnote to the Impact Assessment, accompanying the proposal, where the Commission considers that "[i]n these cases, Europol acts as data processor rather than as data controller."[15] However, currently the Europol Regulation does not define the notion of "data processor". Once Article 3 and Chapter IX of EUDPR become directly applicable to Europol (see point 3.1. of this Opinion), the Agency will have to comply with the conditions and the obligations of a data processor under Article 87 of EUDPR. Therefore, in view also of the principle of accountability, **the EDPS reminds that pursuant to paragraph 3 of Article 87 of EUDPR, there are a number of mandatory elements, which should be provided for in a binding legal act under the Union or Member State law[16].**

20. The EDPS is also concerned about the possible practical implications of the new paragraph 6b of Article 26. In view of the Commission's commitment that "[f]or 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."[17] (emphasis added), **the EDPS recommends that Europol should carry out an assessment of the possible security risks posed from the opening of its infrastructure for use by private parties and, where necessary, implement appropriate preventive and mitigating measures.**

3.2. Processing of large and complex datasets

21. Nowadays, criminal investigations and criminal intelligence operations increasingly include the collection of large and complex datasets by national law enforcement authorities. The processing of large datasets has thus become an important part of the work

performed by Europol to produce criminal intelligence. However, while the processing of such information might be lawful under national law, the Europol Regulation is currently more restrictive. In particular, Europol can only process information about certain categories of individuals, namely suspects, contacts and associates, victims, witnesses or informants, and certain categories of data (Article 18(5) and Annex II B of the Europol Regulation).

22. As a result of the inconsistency between the Europol's practices relating to large datasets and the legal framework in force, in September 2020 the EDPS decided to issue an admonishment to Europol[18]. The decision focused specifically on the legal issues resulting from the processing of large datasets, i.e. the lack of the necessary legal ground, as well as the application of the principle of data minimisation. At the same time, it should be borne in mind that big data analytics raises a number of other challenges to the protection of personal data, related, *inter alia*, to purpose limitation, data minimisation, data quality, storage limitation, transparency, etc[19].

23. The EDPS notes that the proposal tries to addresses the identified structural legal problem with the introduction of a "pre-analysis" of the received large and complex datasets for the sole purpose of determining whether such data falls into the categories of data subjects categories of personal data and categories of data subjects, laid down in Article 18(5) and Annex II B of the Europol Regulation (new paragraph 5a of Article 18). Furthermore, the prior processing of data is limited to a maximum period of one year, which can be extended in justified cases with the prior authorisation of the EDPS.

24. The EDPS welcomes the safeguards that accompany the proposed "pre-analysis", which are generally in line with the data protection principles of purpose limitation and storage limitation, as well as the fact that this new type of processing is construed as a derogation from the general rules. However, the EDPS considers that it has to be further limited to cases where the transfer by Member States to Europol and the subsequent processing of big datasets by the Agency is actually an objective necessity. In other words, **the derogation under paragraph 5a of Article 18 should not become the rule**.

25. The EDPS has also doubts how the legal possibility to extend the maximum period of pre-analysis under paragraph 5a will work in practice. Given the lack of specific criteria or at least general indication what should be considered as "justified cases", the prior authorisation of the prolongation by the EDPS could actually turn into "rubber-stamping" of the requests by the Agency. Furthermore, it is not entirely clear what is the relationship between the new derogation under paragraph 5a of Article 18 and the existing derogation under paragraph 6 of the same Article. Both provisions envisage "temporarily processing of data" (pre-analyses) for similar, though not identical purposes. Therefore, **the EDPS recommends that the Regulation should further define the cases when Europol could resort to the derogation under paragraph 5a, respectively when the Agency may request extension of the maximum period of 1 year. In addition, the interaction between paragraphs 5a and 6 of Article 18 should be clarified.**

3.3. Data processing in support of a specific criminal investigation

26. The proposed information processing by Europol in support of specific criminal investigations under the new Article 18a is another response to the so-called "big data challenge", which has led to the admonishment of Europol by the EDPS. It is also the

change of the legal framework with probably the most substantial impact on the protection of personal data, as it would allow extensive data processing outside the list of categories of personal data in Annex II and beyond the current storage periods in the Europol Regulation.

27. The EDPS is aware that some Member States might not have the necessary IT tools, expertise and resources to analyse large and complex datasets, as part of a criminal investigation, and therefore might turn to Europol for support. While pooling of expertise and capabilities at Union level, when dealing with complex investigations like cybercrime or terrorism, should be generally encouraged and supported, the EDPS is concerned that the broad derogation from the existing data minimisation and storage limitation safeguards in the Europol Regulation might in practice upend the existing system of checks and balances with regard to personal data processing by the Agency.

28. The potential impact of the proposed measure is recognised in the Impact Assessment accompanying the legislative proposal, including the need to "take full account of Fundamental Rights and notably the right to the protection of personal data". The chosen policy option (option 4) is presented as "narrow and justified exception", which would be applied "on an exceptional basis"[20]. In the same vein, recital 18 of the legislative proposal foresees two parallel assessments of the necessity and proportionality of the processing of the investigative case file by Europol, carried out by the respective Member State and by the Agency. However, these important safeguards remain only in the above-mentioned non-binding texts and are not reflected in the provisions of Article 18a.

29. In the light of the above, the **EDPS recommends the introduction of efficient safeguards in Article 18a, in order to ensure that this derogation is applied on an exceptional basis and thus prevent the risk of the exception becoming the rule. To that end, the amended Regulation should lay down certain conditions and/or thresholds, such as scale, complexity, type or importance of the investigations.** These legal safeguards should be then further particularised and specified by the Management Board of Europol, in accordance with the second subparagraph of paragraph 2 of Article 18a.

30. In addition, **the EDPS stresses that the processing of personal data under the derogation in Article 18a should in all cases be compliant with the general principles and obligations laid down in Chapter IX of EUDPR**.

3.4. Use of data for research and innovation

31. Another area, where the legislative proposal aims at further extending the mandate and the role of Europol, is research and innovation for law enforcement purposes. In view of the evolving security threats and exploitation of the digital transformation and new technologies by criminals, the objective of proposed amendment is to support the effective response at EU level, by providing the law enforcement authorities with the necessary tools to counter such threats.

32. The EDPS takes note of the various arguments in support of the policy choice to assign to Europol a leading role in the area of research and innovation. In this regard, the EDPS would like to highlight the high common standards, increased transparency, as well as technological sovereignty and strategic autonomy of the EU in the area of internal security. The alternative - Europol and the national law enforcement authorities relying on tools and

products developed by external vendors, very often situated outside the EU - clearly poses much higher risks, also with regard to the fundamental rights to privacy and data protection[21].

33. Taking into account that development of new technologies very often involves extensive processing of personal data, e.g. for training of algorithms, the key challenge is how to ensure the strict necessity and proportionality of such processing[22]. In this regard EDPS appreciates the introduction of a number of specific safeguards in the new Article 33a, including the obligation to carry out "data protection impact assessment of the risks to *all rights and freedoms* of data subjects, *including of any bias*" (emphasis added). The list of safeguards in Article 33a, however, should not be considered as exhaustive but only the minimum, and all other relevant data protection principles should also be fully taken into account, including data minimisation, privacy by design and by default, etc. At the same time, the EDPS considers the scope of the new processing purpose, set out in Article 18(2)(e), as too broadly defined. Therefore, **the EDPS recommends that the scope of the research and innovation activities should be better defined in the Europol Regulation, e.g. by clearly linking those activities to the tasks of Europol, and further clarified in a binding document, for instance adopted by the Management Board of Europol, which could be subsequently updated, if necessary**.

34. In addition, the Impact Assessment accompanying the legislative proposals stipulates the participation of Europol in the roll-out of the European Strategy for Data**,** as a major stakeholder in the establishment and use of the European Security Data Space, taking also into account the Commission's White Paper on Artificial Intelligence – A European approach to excellence and trust. Having in mind the higher risks stemming from large-scale processing of data and use of algorithms in the field of law enforcement, **the EDPS considers that his comments and recommendations, made in his Opinions on the European Strategy for Data[23] and the AI White Paper[24], are fully valid also for the research and innovation by Europol**, in particular on the application of the data protection principles, the prohibitions on the use of sensitive personal data for other purposes, the accountability and enforcement in the context of AI, Remote Biometric Identification, etc.

3.5. Strengthening Europol's cooperation with third countries

35. The EDPS notes that, unlike the initial intentions[25], the changes in the Europol Regulation with regard to international transfers of data are rather limited. In fact, the only new element is the legal possibility under paragraph 5 of Article 25 for the Executive Director of Europol to authorise *categories* of transfers of personal data to third countries in specific situations and on a case-by-case basis.

36. The EDPS understands that the proposed change aims to bring additional flexibility in the international cooperation, e.g. in the context of a criminal investigation. However, it is not entirely clear what exactly is meant by "*categories* of transfers" in paragraph 5 of Article 25 and how they differ from the "*sets* of transfers" in the following paragraph 6. Moreover, in the Impact Assessment accompanying the legislative proposal the Commission admits that there is "under-use" of the legal grounds for transfers already available in the Europol Regulation[26].
37. The EDPS points out that the lack of sufficient clarity what could be included into "a category of transfers" creates potential risks for the protection of the personal data of the affected individuals, especially if in practice a broad interpretation of the notion is applied

by the Agency. The Impact Assessment indeed states that "]t]his allows for transfers [...] that are *related to the specific crime* where this is *necessary for the investigation*"[27] (emphasis added). However, as already explained before in this Opinion, the Impact Assessment is a non-binding document and thus insufficient to ensure the necessary legal clarity and certainty. Therefore, **the EDPS recommends that the meaning of "categories of transfers", as well as the distinction from "sets of transfers", should be further defined and clarified in the Europol Regulation.**

38. In addition, the legislative proposal stipulates that in paragraph 8 of Article 25, the following sentence is "*deleted"*: "Where a transfer is based on paragraph 5, such a transfer shall be documented and the documentation shall be made available to the EDPS on request. The documentation shall include a record of the date and time of the transfer, and information about the receiving competent authority, about the justification for the transfer and about the operational personal data transferred." However, the current provision of paragraph 8 does not include such text. Moreover, apparently the aim of the sentence is to introduce an additional safeguard. Therefore, **the EDPS considers this is a technical mistake and recommends replacing the word "deleted" with "added".**

3.6. Strengthening of the data protection framework

39. The Europol Regulation, adopted in 2016, provides for an autonomous data protection regime, specific to Europol. The subsequently adopted EUDPR introduced a distinct Chapter with general rules applicable to the processing of operational personal data by Union bodies, offices or agencies when carrying out activities in the fields of judicial cooperation in criminal matters and police cooperation. However, Europol and EPPO have retained their stand-alone data protection regimes, subject to a legal review by the Commission by 30 April 2022[28].

40. The EDPS welcomes and fully supports the proposed further strengthening of the data protection framework of Europol and in particular the direct application of Chapter IX and Article 3 of EUDPR to the operational data processing by the Agency. It is also an important step towards a comprehensive alignment of the data protection framework for all EU institutions, bodies and agencies, for which the EDPS has repeatedly called for[29] and which drove the Commission's data protection reform proposals since 2009[30].

41. At the same time, the EDPS notes that there is an important element, which is still missing – the harmonisation of the EDPS powers vis-a-vis Europol with the general powers of the EDPS provided for in Article 58 of EUDPR. For instance, currently the EDPS does not have the legal power to order Europol to bring processing operations into compliance with the provisions of EUDPR, to impose an administrative fine pursuant to Article 66 EUDPR in the case of non-compliance, or to order the suspension of data flows to a recipient in a Member State, a third country or to an international organisation[31].

42. The fact that Chapter IX of EUDPR does not contain any *sui generis* provisions on supervision clearly indicates that the EU legislator did not intend to establish a separate supervisory regime for operational personal data. This policy choice is explicitly confirmed in Recital 11 of EUDPR, which provides that "[i]n order to reduce legal fragmentation, specific data protection rules applicable to the processing of operational personal data by Union bodies, offices or agencies when carrying out activities falling within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU **should be consistent with [...] the**

provisions of this Regulation relating to independent supervision, remedies, liability and penalties" (emphasis added). In the same context, Article 98(1)(c) of EUDPR specifically calls upon the Commission to "identify any divergences that may create legal fragmentation of the data protection legislation in the Union", when conducting the review of the legal acts which regulate the processing of operational personal data by Union bodies, offices or agencies.

43. In addition to the above-mentioned legal arguments, it should be added that it is only fair if all EU institutions, agencies and bodies are subject to the same supervisory powers of the EDPS, as any differentiation will put some of them in a more or less privileged position. Therefore, in line with the clear will of the EU legislator, **the EDPS calls for harmonisation of his supervisory powers vis-a-vis Europol with the general powers of the EDPS provided in Article 58 of EUDPR. To that end, the current paragraphs 3 and 4 of Article 43 "Supervision by the EDPS" of Regulation (EU) 2016/794 should be deleted, so that the provisions of Article 58 of EUDPR would directly apply**.

44. The EDPS also observes that the proposed new Article 37a "Right to restriction of processing" is not sufficiently clear and precise with regard to the legal possibilities to process personal data under a restriction. In addition to the two purposes laid down in Article 82(3) of Regulation (EU) 2018/1725, to which Article 37a explicitly refers, namely to ascertain the accuracy of the personal data, and the use of the data as evidence, the legislative proposal introduces a new one: "protection of the rights of the data subject or another natural or *legal* person" (emphasis added). The EDPS considers that such formulation is too broad and could in practice deprive the restriction of personal data processing of its intended effect. Moreover, it would create additional legal fragmentation of the data protection legislation in the Union. Therefore, **the EDPS recommends that the proposed new purpose in Article 37a is deleted and thus the restriction of processing of personal data by Europol is regulated directly by the provision of Article 82 of Regulation (EU) 2018/1725**.

45. The EDPS notes that the proposal replaces the current model of coordinated supervision of Europol, carried out through a Cooperation Board comprising of the Member States' supervisory authorities, with the single model of coordinated supervision laid down in Article 62 of EUDPR and, respectively, the Coordination Supervisory Committee to the European Data Protection Board. The EDPS is convinced that this change, aimed at bringing additional coherence and harmonisation of the supervision of EU agencies and large-scale IT systems, will provide even further possibilities to take advantage of the expertise and experience of the national supervisory authorities.

3.7. Other elements

3.7.1. Transmission of operational personal data to Union institutions, bodies, offices and agencies

46. The legislative proposals updates the current rules in Article 24 on the transmission of operational personal data by Europol to Union institutions, bodies, offices and agencies. The EDPS welcomes the fact that the new provision further specifies the conditions for such transmissions, in particular the requirements for lawfulness and necessity. At the same time, the EDPS notes that the general rule in Article 71(2) of Regulation (EU) 2018/1725, applicable to processing by the same or another EU controller for purposes other than that

for which the operational personal data are collected, lays down an additional requirement for proportionality, which is missing in the proposal. Therefore, **the EDPS invites the legislator to align the conditions for transmission of data to other Union bodies in Article 24 of the Europol Regulation with the general rules in Article 71(2) of Regulation (EU) 2018/1725, in particular with the requirement for proportionality.**

3.7.2. Joint operational analysis between Europol and Member States

47. Another legal change, which aims to regulate processing activities that emerged in practice and have not been initially envisaged in the Europol Regulation, concerns the joint operational analyses between Europol and Member States (Article 20(2a) and Recital 20). As already stated in this Opinion, the EDPS supports pooling of resources and expertise at Union level in the fight against serious crimes and terrorism. At the same time, he considers that the relevant legal provisions could be further improved, for the sake of legal clarity and certainty.

48. In this context, the EDPS notes that the notion of "joint operational analyses" is only mentioned in Recital 20 and is not defined in the legal provisions of the Europol Regulation. Furthermore, there is ambiguity about the legal rules applicable to the processing of personal data in the framework of such joint operational analyses. Recital 20, the last sentence, states that "[a]ny processing of personal data by Member States in joint operational analysis should take place in accordance with the rules and safeguards set out in this Regulation", which also corresponds to Article 18(4) of the Europol Regulation. At the same time paragraph 3 of Article 20 provides that the information could be accessed and further processed by Member States in accordance with national law. Therefore the **EDPS recommends that the notion of "joint operational analysis" as well as the legal rules applicable to the processing of personal data are clearly defined in the Europol Regulation, and not just in the preamble**.

4. CONCLUSIONS

49. In light of the above, the EDPS makes the following recommendations:

Concerning cooperation with private parties

- the prohibition of systematic, massive or structural transfers (Article 26(6), last subparagraph) should apply to all exchanges with private parties, including within the EU;
- the obligations of Europol when acting as data processor / service provider, in particular the mandatory elements provided for in paragraph 3 of Article 87 of Regulation (EU) 2018/1725, should be stipulated in a binding legal act under the Union or Member State law;
- Europol should carry out an assessment of the possible security risks posed from the opening of its infrastructure for use by private parties and, where necessary, implement appropriate preventive and mitigating measures.

Concerning processing of large and complex datasets, including in support of specific criminal investigations

- the Europol Regulation should provide sufficient safeguards to ensure that the derogations under Article 18(5a) and Article 18a would not in reality become the rule;

- the Europol Regulation should further define the cases when Europol could resort to the derogation under Article 18(5a), respectively when the Agency may request extension of the maximum period of 1 year. In addition, the interaction between paragraphs 5a and 6 of Article 18 should be clarified;
- Article 18a should lay down further conditions and thresholds for the processing by Europol of data outside the categories of data subjects listed in Annex II in support of a specific criminal investigation, such as scale, complexity, type or importance of the investigation;
- the processing of personal data under the derogations in Article 18(5a) and Article 18a should in all cases be compliant with the general principles and obligations laid down in Chapter IX of Regulation (EU) 2018/1725.

Concerning use of data for research and innovation

- the scope of the research and innovation activities should be better defined in the Europol Regulation and further clarified in a binding document, which could be subsequently updated.

Concerning Europol's cooperation with third countries

- the meaning of "categories of transfers" in paragraph 5 of Article 25, as well as the distinction from "sets of transfers" in paragraph 6 of the same Article, should be further defined and clarified in the Europol Regulation.

Concerning data protection framework applicable to Europol

- the supervisory powers of the EDPS vis-a-vis Europol should be full aligned with the general powers of the EDPS provided for in Article 58 of Regulation (EU) 2018/1725;
- the proposed new purpose in Article 37a should be deleted and thus the restriction of processing of personal data by Europol should be regulated directly by the provision of Article 82 of Regulation (EU) 2018/1725.

Concerning other elements of the proposal

- the conditions for transmission of data to other Union bodies in Article 24 of the Europol Regulation should be aligned with the general rules in Article 71(2) of Regulation (EU) 2018/1725, in particular with the requirement for proportionality;
- the notion of "joint operational analysis" as well as the legal rules applicable to the processing of personal data within it, should be clearly defined in the Europol Regulation.

Brussels, 8 March 2021

Wojciech Rafał WIEWIÓROWSKI

(e-signed)

Notes

[1] OJ L 119, 4.5.2016, p. 1.
[2] OJ L 295, 21.11.2018, p. 39.
[3] OJ L 119, 4.5.2016, p. 89.
[4] Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol) (OJ L 121, 15.5.2009, p. 37).
[5] COM(2020) 796 final
[6] COM(2020) 605 final (24.7.2020).
[7] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2326
[8] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters as regards the entry of alerts by Europol, COM(2020) 791 final
[9] See in particular the European Parliament resolution of 10 July 2020 on a comprehensive Union policy on preventing money laundering and terrorist financing (2020/2686(RSP), Council conclusions on Europol's cooperation with Private Parties of 2 December 2019 or the Declaration of the Home Affairs Ministers of the EU ('Ten points on the Future of Europol') of 21 October 2020.
[10] https://edps.europa.eu/data-protection/our-work/publications/strategy/edps-strategy-2020-2024-shaping-safer-digital-future_en
[11] 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).
[12] See Impact Assessment Report, Part 2, SWD(2020) 543 final
[13] The Commission estimates in point 4 "Budgetary Implications" of the legislative proposal that Europol will need an additional budget of around EUR 180 million and around 160 additional posts for the overall MFF period to enforce its revised mandate. However, no such estimate is made for the EDPS.
[14] See Judgments in Joined Cases C-293/12 and C-594/12 DRI, paragraph 52; Case C-73/07 Satakunnan Markkinapörssi and Satamedia, paragraph 56; Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke and Eifert, paragraphs 77 and 86.
[15] Footnote 69, Impact Assessment Report, Part 1, page 13, SWD(2020) 543 final
[16] For more information see EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725.
[17] Impact Assessment Report, Part 1, page 9, SWD(2020) 543 final
[18] https://edps.europa.eu/data-protection/our-work/publications/investigations/edps-decision-own-initiative-inquiry-europols_en
[19] See also the EDPS Preliminary Opinion "Privacy and competitiveness in the age of big data" of March 2014,
[20] See Impact Assessment Report, Part 1, page 51, SWD(2020) 543 final
[21] The use of the Clearview AI application by some of the law enforcement authorities in the EU is a clear illustration of this risk.
[22] A possible parallel could be made with the finding of the Court of Justice of the EU in its Opinion 1/2015 on the EU-Canada PNR Agreement , where the Court has found that "the systematic use of [PNR] data for the purpose of verifying the reliability and topicality of the pre-established models and criteria [...] or of defining new models and criteria [...] [do] not exceed the limits of what is strictly necessary". Similarly, the use of operational personal data, lawfully collected and stored by Europol, to develop tools and provide solutions to facilitate the fight against serious crimes and terrorism, could be justified, if accompanied by efficient and appropriate safeguards.
[23] https://edps.europa.eu/sites/edp/files/publication/20-06-16_opinion_data_strategy_en.pdf
[24] https://edps.europa.eu/sites/edp/files/publication/20-06-19_opinion_ai_white_paper_en.pdf
[25] See the Inception impact assessment, Ares(2020)2555219.
[26] See Impact Assessment Report, Part 2, Annex 7, page 109-110, SWD(2020) 543 final.
[27] Idem.
[28] See Article 2(3) and Article 98 of Regulation (EU) 2018/1725
[29] See in particular the EDPS Opinion of 14 January 2011 on the Communication "A comprehensive approach on personal data in the European Union", as well as the EDPS Opinion 5/2017 of 15 March 2017 on upgrading data protection rules for EU institutions and bodies.
[30] In its Communication on "A comprehensive approach on personal data protection in the European Union" (COM(2010)609 final), the Commission concluded that the EU needs a more comprehensive and coherent policy

on the fundamental right to personal data protection. In the area of law enforcement, the Commission underlined again in 2012 that the EU's new reformed data protection framework therefore aims to ensure a consistent, high level of data protection to enhance mutual trust between police and judicial authorities of different Member States (and Union institutions, offices, bodies and agencies), thus contributing further to a free flow of data, and effective cooperation between police and judicial authorities (Commission Communication 'Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century', COM/2012/09 final).

[31] See Article 58(2)(e), (i) and (j) of Regulation (EU) 2018/1725.