EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

25 May 2021

Opinion 8/2021

on the Recommendation for a Council decision authorising the opening of negotiations for a cooperation agreement between the EU and INTERPOL

edps.europa.eu

The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 52(2) of Regulation (EU) No 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) thereof '…for advising Union institutions and bodies and data subjects on all matters concerning the processing of personal data'.

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

*Under **Article 42(1)** of Regulation (EU) No 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' and 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 relates to the EDPS' mission to advise the EU institutions on coherently and consistently applying the EU data protection principles, including when negotiating agreements in law enforcement cooperation. It builds on the general obligation that international agreements must comply with the provisions of TFEU and the respect for fundamental rights that stands at the core of EU law. In particular, compliance with Articles 7 and 8 of the Charter of Fundamental Rights of the EU and Article 16 TFEU must be ensured.

Executive Summary

On 14 April 2021, the Commission adopted a Recommendation for a Council Decision authorising the opening of negotiations for a cooperation agreement between the EU and the International Criminal Police Organization (Interpol).

Despite existing cooperation with Interpol, the Commission identified areas where cooperation could and should be stepped up, or even set up in new areas, to address a series of indispensable operational needs and to implement existing legal acts, with the aim of better supporting Member States in preventing and combating terrorism and organised crime. These operational needs require concluding a cooperation agreement with Interpol.

The EDPS wishes to highlight that the objective of supporting the (current and future) cooperation between the EU and Interpol across a wide range of activities in a single legal instrument renders the envisaged agreement highly heterogeneous in nature. He therefore underlines the need for **an in-depth impact assessment** and that the approach should not lead to a weakening of the fundamental rights and freedoms of natural persons, in particular of their rights to data protection and to privacy.

The EU data protection law regime provides, in principle, that data transfers to an international organisation can take place without additional requirements only when that international organisation ensures an adequate level of protection. When the international organisation has not been declared as adequate, exceptions apply for specific transfers, as long as appropriate safeguards are adduced. Therefore, the EDPS also makes three main recommendations to ensure that the envisaged agreement is capable of adducing appropriate safeguards:

- It should be made clear in the negotiating directives that it is necessary to ensure that the envisaged agreement generally complies with the Charter, with the relevant horizontal data protection legislation (Regulation (EU) 2018/1725, Regulation (EU) 2016/679 and Directive (EU) 2016/680 and with the specific data protection requirements and safeguards in the basic acts establishing the EU agencies or IT systems.
- The future agreement should explicitly clarify that there will be no reciprocal direct or indirect access by Interpol to the EU databases.
- In the context of onward transfers, it should be explicitly laid down that personal data transferred by the EU to Interpol will not be used to request, hand down or execute a death penalty or any form of cruel and inhuman treatment.

Finally, the EDPS recommends that the citations in the preamble of the Recommendation not only refer to the appropriate procedural legal basis but also to the relevant substantive legal basis, among which Article 16 TFEU considering the subject matter of the future agreement.

The EDPS also remains available to provide further advice during the negotiations and the formal consultation which has to take place on the proposal to Council for the signature and conclusion of the agreement pursuant to Article 218 TFEU, as per Article 42(1) Regulation (EU) 2018/1725.

Table of Contents

1. Introduction and background 4

2. The holistic approach 6

2.1. An in-depth fundamental rights impact assessment is missing 6

2.2. The envisaged agreement should not lower the level of protection 7

3. On the need to adduce appropriate data protection safeguards 8

4. On the legal basis of the future Council Decision 13

5. Conclusions 13

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 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[2],

Having regard to Regulation (EU) 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[3], and in particular Article 42(1) thereof,

HAS ADOPTED THE FOLLOWING OPINION:

1. Introduction and background

1. The International Criminal Police Organisation (Interpol)[4] is the largest global criminal police inter-governmental organisation, with 194 member countries. The EU and Interpol already have long-standing and deep cooperation in a range of law enforcement-related areas. Interpol is a key partner for the EU in the field of internal and external security, including countering terrorism and organised crime, as well as in integrated border management.

2. The 2020 EU Security Union strategy[5] calls on the Member States to step up cooperation between the EU and Interpol, as essential to enhance cooperation and information exchange. The strategy recognises that Interpol has an important role to play in this respect. In addition to the existing cooperation with Interpol, areas where cooperation could be stepped up or even set up to address a series of operational needs, and to implement existing legal acts, have been identified, with the aim of better supporting Member States in preventing and combating terrorism and organised crime.

3. Therefore, on 14 April 2021, the Commission adopted a Recommendation for a Council Decision authorising the opening of negotiations for a cooperation agreement between the EU and Interpol[6] (hereinafter, the 'Recommendation').

4. According to the explanatory memorandum[7], the envisaged EU-Interpol cooperation agreement would pursue the following aims:

- Regulate cooperation between European Union Agency for Law Enforcement Cooperation (**Europol**)[8] and Interpol, taking into account the latest developments in combating terrorism, cross-border and transnational serious, organised crime, the current operational needs, Europol's mandate, and the EU's latest data protection regime.

- Provide the safeguards and guarantees needed to give controlled access to Interpol's Stolen and Lost Travel Document (SLTD) and Travel Document Associated With Notices (TDAWN) databases via the European Search Portal (ESP), **by EU Member States and EU agencies**, as necessary to carry out their tasks, in line with their access rights, with EU or national law covering such access and in full compliance with EU data protection requirements and with fundamental rights[9].

- Provide the necessary safeguards and guarantees to enable **EU Member States** and **Frontex**[10] (its European Travel Information and Authorisation System Central Unit ('ETIAS')) to access Interpol databases via the ESP in compliance with EU data protection requirements and with fundamental rights.

- Provide the necessary safeguards and guarantees to implement a **revised Visa Information System Regulation**[11] enabling **EU Member States** to access SLTD and TDAWN databases through the ESP when examining applications for visas or residence permits, in full compliance with EU data protection requirements and with fundamental rights.

- Set up and regulate cooperation between the European Public Prosecutor's Office ('the **EPPO**'), as established by Regulation (EU) 2017/1939 ('the EPPO Regulation')[12] and Interpol, in line with their mandates, and in full compliance with EU data protection requirements and with fundamental rights.

- Provide the legal basis to authorise **Europol, Frontex category 1 staff** (statutory staff of the standing corps[13]) and **EPPO** to **access relevant Interpol databases** to carry out their tasks, in full compliance with EU data protection requirements and with fundamental rights.

- Provide the legal basis to authorise **Eurojust**[14] **and EPPO** to exchange **operational information** with Interpol, in full compliance with EU data protection requirements and with fundamental rights.

5. Pursuant to Article 42(1) of Regulation (EU) 2018/1725, the Commission has to consult the EDPS following the adoption of a recommendation to the Council pursuant to Article 218 TFEU, where there is an impact on the protection of individuals' rights and freedoms with regard to the processing of personal data. The EDPS was also consulted informally during the process of preparation of the recommendation, and communicated his informal comments in August 2020. He welcomes the fact that his views have been sought (and implemented to some extent) at an early stage of the procedure and encourages the Commission to continue with this good practice.

6. The EDPS was formally consulted by the Commission on 14 April 2021 and expects that a reference to this Opinion will be included in the preamble of the Council Decision. The present Opinion is without prejudice to any future additional comments or recommendations by the EDPS, in particular if further issues are identified or new information becomes available and of the formal consultation which has to take place on the proposals to Council for the signature and conclusion of the agreement pursuant to Article 218 TFEU, as per Article 42(1) Regulation

(EU) 2018/1725. In this regard, the EDPS welcomes Recital 19 of the Recommendation according to which the Commission should consult him during the negotiation of the agreement or, in any event, before the agreement is concluded. Furthermore, this Opinion is without prejudice to any future action that may be taken by the EDPS in the exercise of his powers pursuant to Article 58 of Regulation (EU) 2018/1725.

2. The holistic approach

7. The EDPS highlights that the objective of underpinning a significant amount of the (current and future) cooperation between the EU and Interpol in a single legal instrument renders the envisaged agreement **highly heterogeneous** in nature, encompassing a wide range of activities, including police cooperation (Articles 87 and 88 TFEU), judicial cooperation in criminal matters (Articles 82 and 85 TFEU), border security as part of border management (Article 77 TFEU), visas and residence permits and the EPPO (Article 86 TFEU) - in which not all Member States participate[15].

8. Bearing in mind such a heterogenic approach, he underlines (1) the need for an in-depth impact assessment and (2) that the approach should not lead to a weakening of the fundamental rights and freedoms of natural persons, and in particular of their rights to data protection and to privacy.

2.1. An in-depth fundamental rights impact assessment is missing

9. The heterogeneity of the envisaged agreement, together with the potential impact of such an agreement on fundamental rights, in particular on privacy and data protection, call for an in-depth impact assessment. The EDPS regrets that the Commission Recommendation was not accompanied by a fundamental rights impact assessment and encourages the Council to undertake an in-depth fundamental rights and data protection impact assessment[16], including (a) the **necessity and proportionality of each envisaged measure as they limit** the rights to privacy and to the protection of personal data[17] and (b) the **legal feasibility** of regulating all of them under a **single** overarching agreement[18]. Special caution is warranted[19], due to the sensitivity of the data concerned and to the number of third countries members of Interpol, which are not party to an equivalent agreement with the EU or whose authorities to which it is intended personal data be transferred are not covered by a Commission adequacy Decision[20].

10. The assessment on the necessity and proportionality of the envisaged use-cases under each objective should address in particular **the purposes of the processing as well as the amount and categories of the concerned personal data**. It should notably evaluate which databases should be accessed - for instance, whether this should also include Interpol's Notices - and according to which modalities. The assessment should also demonstrate the necessity with reference to **each of the Interpol databases** it envisages to make accessible (compared to already available databases).

11. The impact assessment should also be carried out **having regard to the risks to the persons concerned**, bearing in mind that it could be vulnerable persons such as migrants and possibly asylum seekers.

2.2. The envisaged agreement should not lower the level of protection

12. The EDPS considers that **the Recommendation should be clarified to avoid the risk of lowering the level of protection for individuals, currently ensured under EU primary and secondary law**.

13. He notes that **the exchanges of personal data envisaged by the Recommendation might not always be consistent with the EU secondary law establishing or regulating the activities of the EU institutions, agencies, offices and bodies** that would cooperate with Interpol.

14. The lack of clarity on the specific purposes, the types of data to be exchanged, as well as the exact allocation of roles and responsibilities is detrimental to the requirement of the quality of the law, of paramount importance for **all measures limiting the rights** enshrined under Articles 7 and 8 of the Charter and Article 16 TFEU.

15. This concern is raised in particular by wording such as '*the agreement should provide the legal basis to authorise Europol, Frontex statutory staff of the standing corps (category 1 staff), and EPPO to* ***access relevant Interpol databases*** *for the performance of their tasks*'[21]. Having regard to the sensitive nature of the data concerned, the EDPS reiterates that **it is paramount that all the necessary specifications are included in the negotiating directives**.

16. More specifically, the EDPS considers that **each and every type of cooperation** with Interpol regulated under the envisaged overarching agreement, should:

    - clearly **specify the purpose(s) and the objectives of the cooperation between Interpol and each EU institution, body, office and agency concerned**. It is important that the specified purpose does not go beyond what is prescribed in the existing legal instruments, and notably is in line with the respective mandate of the EU institution, office, body or agency concerned. The envisaged agreement should not introduce new data processing operations that are not covered by existing legal bases. In this regard, we recommend clarifying that the envisaged agreement **will not provide for reciprocal direct or indirect access by Interpol to EU databases**.

    - duly take into account **the difference** between *judicial cooperation in criminal matters and police cooperation*, on the one hand and *border management* on the other hand;

    - be in **compliance with the rules provided under the EU legal acts** establishing the Union agencies, offices and bodies, regulating their activities or provided under the EU data protection framework.

17. In this regard, **point (2) in Annex** to the negotiating directives prescribes that the agreement should provide the safeguards and guarantees needed to authorise controlled access to SLTD and TDAWN databases via [ESP] for EU Member States and **EU agencies, as necessary to carry out their tasks, in line with their access rights**, with EU or national law covering such access and in full compliance with the EU data protection requirements and with fundamental rights' (emphasis added). The EDPS considers that this passage lacks clarity, since other negotiating directives already cover the access to these databases by Frontex (ETIAS and the Frontex category 1 staff), Europol and the EPPO[22]. **The EDPS is of the opinion that the necessity for other EU agencies to have such access has not been demonstrated**. Should it be demonstrated[23], **the negotiating directives should clearly set out which EU agencies should have access rights for which of their specific tasks**.

18. Also, with regard to Frontex, **Recital 13** of the Recommendation refers to Article 68(1) of the Frontex Regulation as the appropriate legal basis for Frontex to cooperate with Interpol and states that in accordance with Article 82(1) thereof, access to Interpol databases (in particular SLTD) should be granted to members of category 1 teams to perform tasks and exercise powers for border control provided for in Article 8(3)(a)(i), Article 8(3)(a)(ii) and Article 6(1) point (e) of Regulation (EU) 2016/399 of the European Parliament and of the Council[24] ('the Schengen Borders Code'). According to these provisions, such staff members of Frontex may check third country nationals against Interpol databases, in particular SLTD, at the external borders of the Member States and third countries associated with the implementation, application and development of the Schengen acquis in relation to control on persons at the external borders. The latter provision includes, among other entry conditions for third-country nationals, the condition that third-country nationals are not considered to be a threat to public policy, internal security, public health or the international relations of any of the Member States. However, the Recommendation seems to go beyond the scope of this provision when it indicates in its explanatory memorandum[25] that such access will not only serve the purpose of border checks, but also of preventing and investigating terrorist offences. Consequently, **the EDPS recommends clarifying in the Recommendation the purposes for which such access should be provided, ensuring consistency with Article 10(q) and Article 90 of the Frontex Regulation should such purposes include the prevention and investigation of terrorist offences. Also the mandate should clarify which databases should be accessed and for which purposes by the members of category 1 teams.** In any event, as per the legal basis mentioned in Recital 13, the EDPS notes that the envisaged agreement would cover only access to Interpol databases for checks of third country nationals.

19. More generally, the EDPS considers that the envisaged agreement should not create an obligation for the EU agencies to cooperate with Interpol beyond what is already set out in the relevant Union law.

20. Finally, it should be clarified whether the concept of '**operational information**' under **point (7) of the Annex** to the Recommendation, refers to any information collected and analysed during operations, including for an administrative purpose (such as interviews or administrative handling of incoming persons etc.) or is meant to refer to 'operational personal data' within the meaning of Regulation (EU) 2018/1725, i.e. personal data processed by Union bodies, offices or agencies when carrying out activities falling within the scope of judicial cooperation in criminal matters and police cooperation as defined under the TFEU to meet the objectives and tasks laid down in the legal acts establishing them. **In this regard, the wording used under point (7) of the Annex is still very broad so that it could be read as giving a mandate for establishing cooperation beyond what is already provided for under EU secondary law.**

3. On the need to adduce appropriate data protection safeguards

21. The EU data protection *acquis*, which is to be read in the light of Article 8 of the Charter and Article 16 TFEU, provides, in principle, that international data transfers can take place to an international organisation without additional requirements only when that international organisation ensures an adequate level of protection. When the international organisation has not been declared as adequate, exceptions apply for specific transfers, as long as appropriate safeguards are adduced.

22. Therefore, in the absence of an adequacy decision concerning Interpol, the envisaged agreement could provide for a legal basis allowing the transfer of personal data to Interpol **on the condition that** it would be **legally binding and enforceable against all parties to the agreement and that it would include appropriate data protection safeguards.** According to Article 46 of Regulation (EU) 2018/1725, any transfer of personal data by EU institutions, agencies, offices to international organisations must also meet the conditions of the other provisions of the Regulation. Therefore, each transfer must comply with the data protection principles provided in Article 4 and have a legal basis from the ones provided in Articles 5 and 10 (regarding special categories of data). Hence, a two-step approach must be applied: first, the data processing should be legal according to all relevant provisions of the Regulation and as a second step, the provisions of Chapter V must be complied with. Article 46 provides that a data transfer to an international organisation shall not undermine the level of protection guaranteed by this Regulation and in particular, **data subjects must be ensured enforceable and effective rights**[26].

23. The EDPS welcomes that several negotiating directives in the Annex refer to ensuring cooperation in full respect of the EU data protection and fundamental rights requirements. It should however be made clear in the mandate that this expression '*in full compliance with EU data protection requirements and with fundamental rights*' includes the following three levels of compliance:

    – generally with the Charter, including in particular Articles 7, 8 and 52;

    – with the relevant horizontal data protection legislation: Regulation (EU) 2018/1725, Directive (EU) 2016/680 and the Regulation (EU) 2016/679;

    – with the specific data protection requirements and safeguards in the basic acts establishing the EU agencies or IT systems.

24. In this regard, the EDPS underlines that Article 94 of Regulation (EU) 2018/1725 applies to transfer of operational data for law enforcement purposes, except for the EPPO and Europol, for which their respective Regulations apply[27]. Therefore, **Recital 16** dedicated to transfers of operational data is welcome, but appears **to be incomplete,** as it does not refer to the specific provisions relating to the transfers of operational data by Europol and EPPO, which are not covered under Regulation (EU) 2018/1725 but by the Europol and EPPO Regulations. Also, **reference to Eurojust Regulation** should be added as the general rules of the distinct Chapter of Regulation (EU) 2018/1725 on the processing of operational data apply without prejudice to the specific data protection rules contained in the Eurojust Regulation[28].

25. At the same time, the EDPS welcomes that point (c) of the Annex provides that the agreement shall '*[s]pell out clearly and precisely the safeguards and controls needed on the protection of personal data, fundamental rights and freedoms of individuals, irrespective of nationality and place of residence, in the exchange of personal data with Interpol*' and mentions under letters (i) to (xi) some principles and safeguards. He insists, however, on the importance of **providing concrete, specific and effective safeguards for each type of cooperation included in the Agreement**. Given the law enforcement context and the potential risks that such transfers of data could pose to data subjects, the safeguards included in this future agreement with Interpol should satisfactorily address and mitigate these risks.

26. The holistic approach entails particular risks for fundamental rights: first, the risk of lowering the level of protection provided under the current EU legal framework and second, of creating legal uncertainty. **The negotiating directives, notably under point (c) on the necessary**

safeguards and controls, do not clearly differentiate between the different kinds of activities and data processing, even though they are regulated under different legal instruments[29], and therefore require appropriate sets of safeguards and requirements adapted to each 'scenario' as necessary. In this regard, the EDPS wishes to draw attention to the fact that the European Commission followed a different approach as far as EU secondary law is concerned, regarding the access to the SLTD and TDAWN Interpol databases through the ESP for borders and visa on the one hand, and for police cooperation on the other hand. This access has been established under two separate Regulations (Regulations (EU) 2019/817 and 2019/818), as explained by the European Commission in the proposals for these instruments, to 'respect the distinction between the matters which constitute a development of the Schengen *acquis* regarding borders and visa on the one hand and other systems which concern the Schengen *acquis* on police cooperation or are not related to the Schengen acquis on the other (...)'.

27. Against this background, the EDPS recommends that **Recital 17** of the Recommendation **also refer to the data protection provisions of the instruments establishing the Union agencies and offices concerned by the envisaged agreement**. The EU legal framework for data protection is indeed composed of several different legal sources among which a series of EU secondary legislation which applies to specific transfers of data, prohibiting as a rule transfers to international organisations and allowing them only as a way of derogation under strict conditions[30].

28. Concerning **Europol**, the EDPS invites the Council to ensure that the envisaged agreement does not go below the level of data protection safeguards provided under the Europol Regulation - which explicitly refers to the cooperation and exchange of information, including personal data, between Interpol and Europol - and the current bilateral agreement. For instance, the Annex, **point (c), letter (ii)** provides that *'[t]he Agreement must provide scope to indicate, when the data is transferred, any restriction on access or use, including a restriction on data transfer, erasure or destruction*'. Article 19(2) of the Europol Regulation in relation to such restrictions also states that '*[w]here the need for such restrictions becomes apparent after the information has been provided, [international organisations] shall inform Europol accordingly. Europol shall comply with such restrictions*'. **Such obligation of information should be included in the envisaged agreement as well**. Letter (iv) of the Annex lays down that '[*t]he Agreement shall specify the criteria on the basis of which the reliability of the source and accuracy of the data shall be indicated*'. However, the Europol Regulation already contains a specific provision on reliability and accuracy of the source of information originating from a Member State (Article 29), specifying under paragraph 5 that '*[t]his Article shall apply mutatis mutandis where Europol receives data or information from [...] [an] international organisation [...]*'. **The negotiating directives should be amended to clarify that the envisaged agreement should not undermine the criteria set out in the Europol Regulation with regard to the reliability and accuracy of the source of information[31]. In the same vein, regarding other agencies and bodies included in the recommendation, further amendments will be needed to ensure that relevant provisions regarding the responsibility for accuracy of the information provided in their relevant mandates are not undermined by the future EU-Interpol agreement**.

29. Concerning **Eurojust**, Articles 47 and 56 (General principles for transfers of operational personal data to third countries and international organisations) also lay down specific, mandatory requirements for cooperation entailing transfers of personal data to an international organisation, including strict rules on onward transfers.

30. Concerning **the EPPO**, according to Article 80 (General principles for transfers of operational personal data) of the EPPO Regulation, '*[t]he EPPO may transfer operational personal data to a*

third country or international organisation, subject to compliance with the other provisions of this Regulation, in particular Article 53, only where the conditions laid down in the Articles 80 to 83 are met'.

31. **Further,** the EDPS underlines the importance of including sufficient safeguards to ensure that information transmitted by Interpol is **correct and complete** as it will be used to make decisions about individuals (e.g. in the context of ETIAS, individuals could be refused entry onto EU territory).

32. Also, **the EDPS recommends including** in the Annex at least the following safeguards:

- the envisaged agreement should spell out **when and under what circumstances automated individual decisions** are allowed (or not) (**letter (viii), point (c)**);

- **more details on the obligation of Interpol to notify in the event of a personal data breach** (**letter (ix), point (c)**). The current text does not specify who needs to inform who, and who informs data subjects. According to the nature of the personal data breach, it should be clarified when and if Interpol should notify competent authorities (e.g. the EU agency that provided the information, its oversight body) and, wherever necessary, data subjects. Also, the agreement should include a description of the minimum information to be provided when notifying the breach (to the oversight body and the data subject); and

- **more operational details on technical and organisational measures for the security** of personal data should be provided, including on e.g. how confidentiality of electronic communications would be ensured.

33. As regards the '**exchange of operational information**' with Interpol, the Recommendation does not sufficiently specify the modalities, conditions, limits, scope of the data transferred to Interpol, including personal data. This issue is made more critical by the possibility of **onward transfers** from Interpol to other international organisations or third countries, including for which no adequacy decision has been issued, pursuant to **letter (x) of point (c)** of the Annex. Indeed, as far as personal data transferred by EU agencies and bodies are concerned, according to Article 46 of Regulation (EU) 2018/1725 any transfer of personal data which are undergoing processing or intended for processing after transfer to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in Chapter V thereof are complied with by the controller and the processor, including for onward transfers of personal data from an international organisation to another third country or to another international organisation, so as to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

34. In particular, **the EDPS recommends including the following safeguards regarding onward transfers in the negotiating directives**:

- the fact that the transfer of personal data will be subject to **confidentiality obligations**; and

- the fact that the personal data will not be used to request, **hand down or execute a death penalty or any form of cruel and inhuman treatment**[32].

35. Also, **derogations** are provided for under Article 50 of Regulation (EU) 2018/1725 allowing for a transfer to take place despite the absence of adequacy or of appropriate safeguards, if it is necessary in order to protect the vital interests of a person. However, only where the data

subject is physically or legally incapable of giving consent and it does not provide for a derogation for the prevention of an immediate and serious threat to public security. Furthermore, no derogation is foreseen when it comes to the transfer of operational data under Article 94 of Regulation (EU) 2018/1725. It is only in the context of the Directive (EU) 2016/680 that a derogation based on public security of a Member State or a third country is foreseen (paragraph 1 c) of Article 38). **The EDPS recommends therefore limiting the application of derogations for onward transfers to the cases already allowed for EU agencies and bodies concerned when transferring the personal data.** In this regard, the EDPS recalls once more the necessity to ensure that the **specific requirements set up under the Regulations establishing the concerned EU agency or office are respected**.

36. The negotiating directives merely state, **point (c) letter (x)** of the Annex, that *'[o]nward transfers of information from Interpol to other international organisations or third countries must only be allowed for the purposes of the Agreement, must be made subject to appropriate conditions*' while for instance, Article 23(7) of the **Europol Regulation** states that *'[o]nward transfers of personal data held by Europol by (...) international organisations shall be prohibited,* ***unless Europol has given its prior explicit authorisation***' (emphasis added). Article 47 of the **Eurojust** Regulation includes safeguards on onward transfers, with which the envisaged agreement shall be aligned. In particular, Article 47(6) of the Eurojust Regulation clearly provides that *'[w]here [...] international organisations have received personal data from Eurojust,* ***onward transfers of such data to third parties shall be prohibited unless all of the following conditions have been met****:*

(a) Eurojust has obtained prior consent from the Member State that provided the data;

(b) Eurojust has given its explicit consent after considering the circumstances of the case at hand;

(c) the onward transfer is only for a specific purpose that is not incompatible with the purpose for which the data were transmitted' (emphasis added).

37. In addition, Article 80(1)(e) of the **EPPO Regulation** provides that '*in the case of an onward transfer to another third country or international organisation by a third country or international organisation, the EPPO shall require the third country or international organisation to seek its* ***prior authorisation for that onward transfer****, which the EPPO may provide only after taking into due account all relevant factors, including the seriousness of the criminal offence, the purpose for which the operational personal data was originally transferred and the level of personal data protection in the third country or an international organisation to which operational personal data are onward transferred*'.

38. The EDPS finally notes that **point (e) of the Annex** to the Recommendation provides for the possibility to suspend or terminate the agreement in question. **The EDPS recommends specifying in the mandate that the agreement should provide for such possibility in cases of breaches, of its provisions on personal data, by one of the parties and that personal data falling within the scope of the agreement transferred prior to its suspension or termination may continue to be processed in accordance with the agreement.**

4. On the legal basis of the future Council Decision

39. It stems from the explanatory memorandum of the Recommendation[33] that the subject matter of the future agreement would fall in particular in the field of instruments on data protection (Article 16 TFEU). The citations in the preamble of the Recommendation, however, do not refer to the substantive legal basis of the legal act.

40. In accordance with Article 296(2) TFEU and the settled case law of the CJEU[34], the EPDS questions the fact that the citations in the preamble of the Recommendation only refer to the appropriate procedural legal basis and do not equally refer to the relevant substantive legal basis.

41. **The EDPS recommends that the citations in the preamble of the Recommendation not only refer to the appropriate procedural legal basis but also to the relevant substantive legal basis, among which Article 16 TFEU.** It follows from the Annex on the negotiating directives that the Commission should simultaneously pursue several objectives during the negotiations of the envisaged agreement, among which ensuring respect for the fundamental rights enshrined in the Charter, including the rights to privacy and the protection of personal data so as to allow for the lawful transfer of personal data. The envisaged agreement would thus indeed relate directly to the objective pursued by Article 16 TFEU.

42. The EDPS recalls that, in a similar law enforcement context, the CJEU found that '*the Council Decision on the conclusion of the envisaged Agreement [between Canada and the European Union on the transfer and processing of Passenger Name Record data] must be based jointly on Article 16(2) and Article 87(2)(a) TFEU*'[35].

5. Conclusions

43. The EDPS welcomes that the agreement should fully respect the fundamental rights and observe the principles recognised by the Charter, in particular the right to a private and family life, enshrined in Article 7 of the Charter, the right to the protection of personal data, enshrined in Article 8 of the Charter and the right to effective remedy and fair trial enshrined by Article 47 of the Charter.

44. However, it should be made clear in the mandate that the agreement should include the following three levels of compliance:

- generally with the Charter;
- with the relevant horizontal data protection legislation: Regulation (EU) 2018/1725, Directive (EU) 2016/680 and Regulation (EU) 2016/679;
- with the specific data protection requirements and safeguards in the basic acts establishing the EU agencies or IT systems.

45. Also, the objective of underpinning a significant amount of the (current and future) cooperation between the EU and Interpol in a single legal instrument renders the envisaged agreement highly heterogeneous in nature, encompassing a wide range of activities. The EDPS therefore underlines the need for an in-depth impact assessment and that the approach should not lead

to a weakening of the fundamental rights and freedoms of natural persons, and in particular of their rights to data protection and to privacy.

46. In the absence of an adequacy decision concerning Interpol, the envisaged agreement could be a legal basis allowing the transfer of personal data to Interpol provided that it would be legally binding and enforceable against all parties to the agreement and that it would include appropriate data protection safeguards.

47. The EDPS considers that adducing appropriate safeguards implies that the international agreement concluded with Interpol should:

- ensure safeguards introduced in existing EU legislation with regard to the transfer by the concerned EU agencies and bodies and the onward transfers of personal data are respected, including the specific provisions relating to the transfers of operational data by Europol and EPPO. In particular, in the context of onward transfers, it should be explicitly laid down that personal data transferred by the EU to Interpol will not be used to request, hand down or execute a death penalty or any form of cruel and inhuman treatment;

- explicitly clarify that there will be no reciprocal direct or indirect access by Interpol to the EU databases;

- spell out when and under what circumstances automated individual decisions are allowed (or not);

- contain more details on the obligation of Interpol to notify in the event of a personal data breach;

- contain more operational details on technical and organisational measures for the security of personal data should be provided.

48. Also, the EDPS recommends specifying in the mandate the possibility to suspend or terminate the agreement in cases of breaches of its provisions on personal data by one of the parties and that personal data falling within the scope of the agreement transferred prior to its suspension or termination may continue to be processed in accordance with the agreement.

49. Finally, the EDPS recommends that the citations in the preamble of the Recommendation not only refer to the appropriate procedural legal basis but also to the relevant substantive legal basis, among which Article 16 TFEU.

Brussels, 25 May 2021

Wojciech Rafał WIEWIÓROWSKI

[e-signed]

Notes

[1] OJ L 119, 4.5.2016, p. 1.
[2] OJ L 119, 4.5.2016, p. 89.
[3] OJ L 295, 21.11.2018, p. 39.
[4] Constitution of the ICPO-Interpol [I/CONS/GA/1956 (2017)].
[5] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and social Committee and the Committee of the Regions on the EU Security Union Strategy, Brussels, 24.7.2020, COM(2020) 605 final.
[6] COM(2021)177 final.
[7] Page 8.
[8] 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, OJ L 135, 24.5.2016, p. 53 ('the Europol Regulation'). According to the explanatory memorandum, there is already a cooperation agreement with Interpol that provides for the exchange of personal data, concluded in 2001, well before the Europol Regulation. However, this agreement does not give direct or indirect access by Europol to information and Interpol's databases, in particular its Notices containing information on terrorists. In addition, the Agency only exchanges information with Interpol and accesses Interpol's databases for the performance of the Agency's tasks through Interpol's Liaison Officer at Europol or the Agency's Liaison Officer at Interpol. The agreement was supplemented later by several cooperation-related documents agreed or concluded between the organisations, for instance on cooperation through Liaison Officers and the establishment, implementation and operation of a secure communication line for the exchange of information.
[9] Following the adoption of regulations on interoperability between EU information systems in the fields of borders and visa i.e. Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA (OJ L 135, 22.5.2019, p. 27) and Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816 (OJ L 135, 22.5.2019, p. 85).
[10] Frontex refers to the European Border and Coast Guard Agency. Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624,OJ L 295, 14.11.2019, p. 1 ('the Frontex Regulation').
[11] Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), OJ L 218, 13.8.2008, p. 60; proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA (COM/2018/302 final) and see political agreement: https://data.consilium.europa.eu/doc/document/ST-5537-2021-INIT/en/pdf
[12] Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO'), OJ L 283, 31.10.2017, p.1 ('the EPPO Regulation').
[13] According to Article 54 of the Frontex Regulation, the European Border and Coast Guard standing corps must be composed of four categories of operational staff. Category 1 includes statutory staff deployed as members of the teams in operational areas in accordance with Article 55 of this Regulation. The Agency must contribute members of its statutory staff (category 1) to the standing corps to be deployed in operational areas as members of the teams with the tasks and powers provided for in Article 82 of this Regulation. Their tasks include countering cross-border crime and terrorism.
[14] Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA, OJ L 295, 21.11.2018, p. 138 ('the Eurojust Regulation').
[15] There are currently 22 Member States, who participate in enhanced cooperation on the establishment of the EPPO.
[16] See for example, in the context of the Commission proposals for amendments to the legal instruments of the EU information systems following the adoption of Regulation 2018/1240 on the establishment of a European Travel Information and Authorisation System (ETIAS), the targeted substitute impact assessment study requested by the European Parliament, LIBE Committee:
https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2019)642808.

[17] See EDPS toolkit on assessing the necessity of measures that limit the fundamental rights to the protection of personal data, available at: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en.pdf and EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, available at: https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf

[18] In this regard, see Opinion 1/15 of the Court of justice of the European Union (hereinafter, 'the CJEU') (Grand Chamber) of 26 July 2017, EU-Canada PNR Agreement, ECLI:EU:C:2017:592, para. 77 and 78: '77 If an examination of a European Union act reveals that it pursues a twofold purpose or that it comprises two components and if one of these is identifiable as the main one, whereas the other is merely incidental, the act must be based on a single legal basis, namely that required by the main or predominant purpose or component. Exceptionally, if it is established, however, that the act simultaneously pursues a number of objectives, or has several components, which are inextricably linked without one being incidental to the other, such that various provisions of the Treaties are applicable, such a measure will have to be founded on the various corresponding legal bases (judgment of 14 June 2016, Parliament v Council, C-263/14, EU:C:2016:435, paragraph 44 and the case-law cited).
78 Nonetheless, recourse to a dual legal basis is not possible where the procedures laid down for each legal basis are incompatible with each other (judgment of 6 November 2008, Parliament v Council, C-155/07, EU:C:2008:605, paragraph 37 and the case-law cited)'.

[19] See Study requested by the European Parliament, DROI Committee, 'Misuse of Interpol's red notices and impact on human rights, recent developments', January 2019, available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/603472/EXPO_STU(2019)603472_EN.pdf

[20] See CJEU Opinion 1/15 of 26 July 2017, EU-Canada PNR Agreement, ECLI:EU:C:2017:592.

[21] Emphasis added. See Recital 7 of the Recommendation.

[22] Points (3) and (6) of the Annex to the Recommendation.

[23] E.g. as a result of the substitute fundamental rights impact assessment, supra, note 16.

[24] Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code),OJ L 77, 23.3.2016, p. 1.

[25] Page 5.

[26] They are available at: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_en

[27] See Article 2 of Regulation (EU) 2018/1725.

[28] Recital 29 of the Eurojust Regulation.

[29] As far as data protection is concerned: Directive (EU) 2016/680 in case of exchange of personal data by Member States authorities competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties with Interpol; Regulation (EU) 2016/679 in case of exchange of personal data by other Member States' public authorities with Interpol, Regulation (EU) 2018/1725 in case of exchange of personal data by EU Institutions, offices, agencies and bodies with Interpol, and in particular its Chapter IX, Article 94 in case of transfer of operational personal data to Interpol by Union bodies, offices and agencies carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three TFEU (Judicial cooperation in criminal matters or police cooperation), as well as specific data protection provisions included in separate instruments such as the Europol and EPPO Regulations).

[30] See for instance Article 31 of Regulation 767/2008/EC of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (OJ, 13.8.2008, p. 60).

[31] Paragraphs 1 and 2 of Article 29 Assessment of reliability of the source and accuracy of information of the Europol Regulation
provide:
'*1. The reliability of the source of information originating from a Member State shall be assessed as far as possible by the providing Member State using the following source evaluation codes:*
(A): where there is no doubt as to the authenticity, trustworthiness and competence of the source, or if the information is provided by a source which has proved to be reliable in all instances;
(B): where the information is provided by a source which has in most instances proved to be reliable;
(C): where the information is provided by a source which has in most instances proved to be unreliable;
(X): where the reliability of the source cannot be assessed.
2. The accuracy of information originating from a Member State shall be assessed as far as possible by the providing Member State using the following information evaluation codes:
(1): information the accuracy of which is not in doubt;
(2): information known personally to the source but not known personally to the official passing it on;
(3): information not known personally to the source but corroborated by other information already recorded;
(4): information not known personally to the source and which cannot be corroborated'.

[32] See Recital 71 of Directive (EU) 2016/680 with regard to criteria to take into account when assessing the existence of appropriate safeguards in a law enforcement context in the absence of an adequacy decision.

[33] See section 3, p. 9 of the Recommendation.

[34] See Judgment of 25 October 2017, European Commission v Council of the EU, Case C-687/15, ECLI:EU:C:2017:803, par. 48 and following.
[35] Opinion 1/15 of 26 July 2017, EU-Canada PNR Agreement, ECLI:EU:C:2017:592, par. 232.