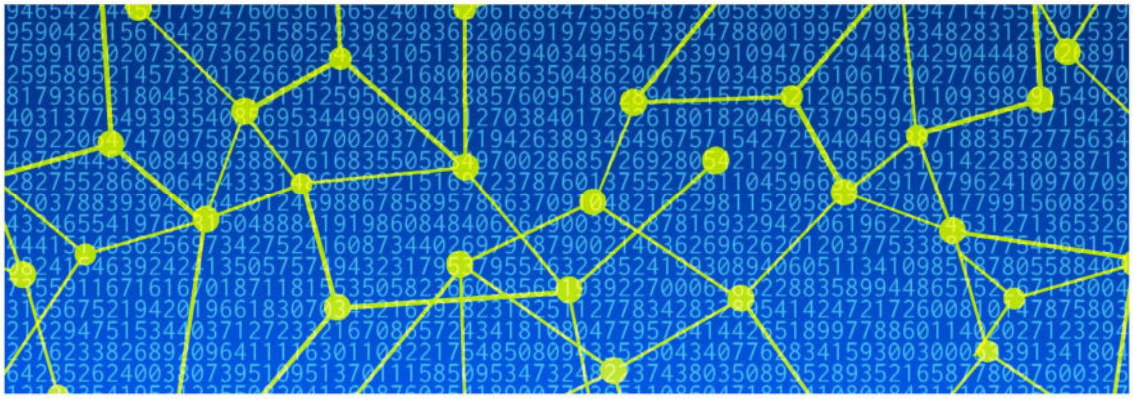

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion 2/2018

EDPS Opinion on eight negotiating mandates to conclude international agreements allowing the exchange of data between Europol and third countries

EDPS

14~~5~~ March 2018

The European Data Protection Supervisor (EDPS) is an independent institution of the EU, responsible under Article 41(2) of Regulation 45/2001 'With respect to the processing of personal data… for ensuring that the fundamental rights and freedoms of natural persons, and in particular their right to privacy, are respected by the Community institutions and bodies', and '…for advising Community institutions and bodies and data subjects on all matters concerning the processing of personal data'. Under Article 28(2) of Regulation 45/2001, the Commission is required, 'when adopting a legislative Proposal relating to the protection of individuals' rights and freedoms with regard to the processing of personal data...', to consult the EDPS.

He was appointed in December 2014 together with the Assistant Supervisor with the specific remit of being constructive and proactive. The EDPS published in March 2015 a five-year strategy setting out how he intends to implement this remit, and to be accountable for doing so.

This Opinion relates to the EDPS' mission to advise the EU institutions on coherently and consistently applying the EU data protection principles when negotiating agreements in the law enforcement sector, in line with Action 5 of the EDPS Strategy: 'Mainstreaming data protection into international agreements'.

Executive Summary

The Commission issued eight Recommendations suggesting to the Council to authorise the opening of negotiations between the European Union and respectively Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia and Turkey in order to conclude international agreements concerning the exchange of personal data between Europol and the authorities of these eight third countries competent to fight serious crimes and terrorism. Such international agreements would provide the required legal basis for Europol to transfer personal data to these third countries' authorities. Annexes to these Recommendations lay down the Council's directives to negotiate each one of the eight international agreements envisaged and set out the mandates given to the Commission.

International agreements allowing Europol and third countries to cooperate and exchange personal data should prove necessary and proportionate in accordance with Article 52(1) of the Charter of fundamental rights of the EU. They should strike a fair balance between the need to fight serious crimes and terrorism and the sound protection of personal data and other fundamental rights protected by the Charter. The EDPS provides recommendations to ensure the respect of these high-level requirements.

Moreover, the Europol Regulation lays down specific rules regarding transfers of data by Europol outside of the EU. Europol could regularly transfer data to a third country based on a binding international agreement between the EU and the third country in question on the condition that such agreement adduces adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals. In this Oopinion, the EDPS also makes general recommendations to ensure that the negotiated agreements will adduce appropriate safeguards within the meaning of the Europol Regulation.

Additionally, the EDPS express preliminary observations and specific recommendations relating to the Annexes to the Commission Recommendations and the directives laid down therein, which the Council will address to the Commission to negotiate the international agreements with third countries for which cooperation with Europol is envisaged.

Finally, the EDPS stands ready to give further advice during the negotiations and before the finalisation of these eight international agreements.

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 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1], and 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)[2],

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 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 Articles 28(2), 41(2) and 46(d) thereof,

Having regard to Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters[4], and 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[5],

HAS ADOPTED THE FOLLOWING OPINION:

1. INTRODUCTION AND BACKGROUND

The Europol Regulation[6] lays down specific rules regarding transfers of data by Europol outside of the EU. Article 25(1) thereof lists a number of legal grounds based on which Europol could lawfully transfer data to authorities of third countries. One possibility would be an adequacy decision of the Commission in accordance with Article 36 of Directive (EU) 2016/680[7] finding that the third country to which Europol transfers data ensures an adequate level of protection. Since there is no such adequacy decisions at the moment, the other alternative for Europol to regularly transfer data to a third country would be to use an appropriate framework resulting from the conclusion of a binding international agreement between the EU and the receiving third country.

On 20 December 2017, the Commission adopted eight Recommendations[8] for Council Decisions to authorise the opening of negotiations for international agreements between the European Union (EU) and eight third countries of the Middle East and North African (MENA) regions, i.e. Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, Tunisia and Turkey. Such international agreements would provide the required legal basis for the exchange of personal data between Europol and the authorities of these third countries competent to fight serious crimes and terrorism.

The Commission considers that there is a need for closer cooperation between Europol and these eight countries in light of the EU political strategy outlined in the European Agenda on Security[9], Council Conclusions[10], and the Global Strategy of the EU's Foreign and Security Policy [11] as well as the operational needs of law enforcement authorities across the EU and of Europol. These eight third countries were also identified in the Eleventh Progress Report towards a genuine and effective Security Union[12]. Cooperation with MENA countries is envisaged as a whole[13]. The current instability in the region, especially the situation in Syria and Iraq, is identified as presenting a significant long-term security threat to the EU. This concerns both the effective fight against terrorism and related organised crime, and migration-related challenges such as the facilitation of irregular migration and trafficking in human beings. Cooperation with local law enforcement is also perceived as critical to address these challenges.

In accordance with the procedure laid down in Article 218 of the Treaty on the Functioning of the European Union (TFEU), the Commission will be responsible for negotiating these international agreements with third countries on behalf of the EU. With these eight Recommendations, the Commission seeks to obtain authorisation from the Council of the European Union (Council) to start the negotiations with the eight third countries identified. Once the negotiations are completed, in order to formally conclude these agreements, the European Parliament will have to give its consent to the texts of the agreements negotiated, while the Council will have to sign the agreements.

2. INVOLVEMENT OF THE EDPS

Recital 35 of the Europol Regulation provides that "where appropriate and in accordance with Regulation (EC) No 45/2001[14] the Commission should be able to consult the EDPS before and during the negotiation of an international agreement" between the EU and a third country to allow the exchange of data between Europol and the authorities of this third country. The EDPS note~~regret~~s that he has not been consulted by the Commission on the eight Recommendations and their Annexes prior to their adoption (but only after their adoption).

The Annexes to these Recommendations are of utmost importance since they lay down the Council's directives to negotiate each of these international agreements and set out the mandate given to the Commission. They notably aim at identifying the operational needs of Europol that would justify the conclusion of international agreements to exchange data with these eight third countries. They should also include all data protection requirements that such international agreements should comply with. Given that the EDPS has become the sole supervisor of Europol since 1 May 2017 and, pursuant to Regulation (EC) No 45/2001, the EDPS is also the advisor to the EU institutions on policies and legislations relating to data protection, international agreements on the exchange of data between Europol and third countries are particularly relevant both from the prospective of the supervisor of the agency and as advisor on data protection. For these reasons, i~~the EDPS considers that it would have been appropriate for him to be consulted by the Commission also prior to the adoption of these eight Recommendations.~~

~~I~~n line with Recital 35 of the Europol Regulation, the EDPS stands ready to give further advice to the Commission during the negotiations and before the finalisation of each one of these eight international agreements.

3. GENERAL RECOMMENDATIONS

3.1 Necessity and proportionality of transferring Europol data to third countries

The EDPS welcomes the attention paid to data protection in the Annexes to the eight Commission Recommendations.

The EDPS understands that Europol wishes to increase its cooperation with third countries for the purpose of fighting serious crimes and terrorism. Nonetheless, the necessity and proportionality of the international agreements envisaged to allow Europol to regularly transfer personal data to competent authorities of the eight third countries in question need to be assessed. As transfers of personal data to third countries constitute an interference with individuals' rights to privacy and data protection guaranteed by Articles 7 and 8 of the Charter of Fundamental Rights of the EU (Charter), requirements of necessity and proportionality of the envisaged processing need to be assessed in accordance with Article 52(1) of the Charter. Furthermore, each international agreement must strike a fair balance between the need to fight serious crimes and terrorism and the sound protection of personal data and other fundamental rights.

The EDPS welcomes that the Explanatory Memorandum to each one of the Recommendations specifies the political context in the third country in question, including its relations with the EU, and the operational needs supporting an enhanced cooperation between the third country and Europol. On this basis, the second sentence of directive 2 in each one of the Annexes specifies slightly the purposes of the transfer of personal data by Europol to the third country in question. However, **the EDPS considers that these purposes for transfer should be more specifically ~~are still too broadly~~ defined.** In order to allow for a full ~~proper~~ assessment of necessity and proportionality on a case-by-case basis, **we recommend to ~~the needs for transfers should be~~ further narrow~~ed~~ down and differentiat~~ed~~ the needs for transfers on the basis of the particular situation of each specific third country and the reality on the ground. The scope of each international agreement and the purposes for which Europol will transfer data to each third country should be further specified accordingly in the Annexes**.

Transfers of personal data to third countries for the purposes of preventing and combatting serious transnational crimes and terrorism could have a significant impact on the lives of the individuals concerned. The envisaged transfers relate to personal information gathered in the context of criminal investigations and further processed by Europol to produce criminal intelligence. Transfers of such information will potentially put the individuals concerned in the spotlight of law enforcement authorities of the receiving third countries and may be used in prosecution cases for serious crimes before the receiving countries' jurisdictions and under their national law. **The EDPS recommends further carrying out impact assessments in order to assess in depth the risks posed by transfers of personal data to each third country for individuals' rights to privacy and data protection, but also for other fundamental rights and freedoms protected by the Charter, so as to be able to define the precise safeguards necessary.**

Finally, the EDPS does not have information regarding the level of protection of personal data ensured in the third countries for which cooperation with Europol is envisaged. The EDPS welcomes that the Commission encourages[15] all remaining third countries that have not yet done so[16] and for which cooperation with Europol is envisaged to accede to the Council of

Europe Convention 108[17] in directive 3(8) of the Annexes. The EDPS invites the Commission to gather such information, which will be important to provide for international agreements tailor-made to each third country taking into consideration the state of their data protection legislation.

3.2 Adducing appropriate safeguards under the Europol Regulation

Since there is no adequacy decision of the Commission in accordance with Article 36 of Directive (EU) 2016/680 at the moment, Article 25(1)(a) of the Europol Regulation cannot be used as a basis for Europol to transfer data to the envisaged third countries[18]. The second alternative for Europol to regularly[19] transfer data to a third country is to use as a legal basis an appropriate framework resulting from the conclusion of a binding international agreement between the EU and the receiving third country "adducing adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals" (Article 25 (1)(b)). The Commission recommends adopting Council Decisions to authorise the opening of negotiations of such international agreements pursuant to Article 25(1)(b). The question remains what "adducing appropriate safeguards" exactly means under the Europol Regulation.

The EDPS first recalls one standard of EU law regarding international agreements concluded by the EU: the respect of fundamental rights. The CJEU found with respect to international agreements concluded by the EU that "the obligations imposed by an international agreement cannot have the effect of prejudicing the constitutional principles of the EC Treaty, which include the principle that all Community acts must respect fundamental rights, that respect constituting a condition of their lawfulness"[20]. The Charter not only guarantees the respect for private and family life (Article 7), but it has also raised data protection to the level of a fundamental right under EU law (Article 8). Consequently, the EDPS considers that adducing adequate safeguards with regard to the right to data protection requires in the first place **full consistency** ~~**compliance**~~ **with Article 8 of the Charter in the third countries to which Europol will transfer personal data, in particular with the purpose limitation principle, the right of access, the right to rectification and the control by an independent authority as specifically stipulated in the Charter.**

Furthermore, the CJEU recently set out the conditions under which an international agreement can provide a legal basis for transfers of personal data in its Opinion 1/15[21] on the international agreement regarding the transfer of Passenger Name Records (PNR) data to Canada delivered in July 2017. The CJEU found that "a transfer of personal data from the European Union to a non-member country may take place only if that country ensures a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union" and found that "[t]hat same requirement applies in the case of the disclosure of PNR data by Canada to third countries, [...] in order to prevent the level of protection provided for in that agreement from being circumvented by transfers of personal data to third countries and to ensure the continuity of the level of protection afforded by EU law"[22]. **Therefore, it follows from Opinion 1/15 that the level of protection resulting from the envisaged international agreements with third countries for the exchange of personal data between Europol and their national competent authorities should similarly** (to the agreement between the EU and Canada on the transfer of PNR data) **be essentially equivalent to the level of protection in EU law.**

Moreover, while the Europol Regulation provides for an autonomous data protection regime specific to Europol, its Recital 40 clearly says that it should at the same time remain "consistent

with other relevant data protection instruments applicable in the area of police cooperation in the Union", among which "in particular, Directive (EU) 2016/680 [...], as well as the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe and its Recommendation No R(87) 15". **The EDPS therefore considers that further requirements can be deduced from Directive (EU) 2016/680 to determine if an international agreement with a third country in fact adduces adequate safeguards.** Article 37 of Directive (EU) 2016/680 provides that, in cases where transfers are not based on an adequacy decision, they should be allowed only if "appropriate safeguards with regard to the protection of personal data are provided for in a legally binding instrument"[23] (similarly to the Europol Regulation), or if "the controller has assessed all the circumstances surrounding the data transfer and, on the basis of that assessment, considers that appropriate safeguards with regard to the protection of personal data exist". Recital 71 gives further guidance and specifies three criteria to take into account when assessing the existence of such appropriate safeguards in a law enforcement context:

- the fact that the transfer of personal data will be subject to confidentiality obligations;
- the principle of specificity, ensuring that the data will not be processed for other purposes than for the purposes of the transfer; 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.

The EDPS considers that these criteria should be applied *mutatis mutandis* to determine if international agreements allowing the exchange of data between Europol and the eight third countries envisaged adduce adequate safeguards. In relation to the third criteria in Recital 71, the EDPS points out that none of the third countries in question (with the exception of Israel) have abolished the death penalty and only some of them (i.e. Morocco, Algeria and Tunisia) have adopted a moratorium on the death penalty.

In addition, the Europol Regulation aims to provide a high level of data protection while taking into account the specificities of Europol's activities as "EU information hub" in the fight against terrorism and serious organised crime and support center for law enforcement operations. **Specific safeguards that are provided to this effect in the Europol Regulation should therefore be mirror~~replicat~~ed in international agreements with third countries in order to adduce adequate safeguards within the meaning of the Europol Regulation**. In this regard, the EDPS stresses that the Europol Regulation allocates different responsibilities in terms of data protection to information providers, such as Member States, and to Europol when processing the data provided for one of the legitimate purposes listed in the Europol Regulation (Article 18). Member States are responsible for the quality of the data provided (Article 38(1)), i.e. that they are accurate and kept up to date, as well as for the legality of the transfer (Article 38(5)(a)). This distribution of data protection responsibilities between Europol and information providers should be taken into account when devising the system of adequate safeguards in each of the international agreements. The Europol Regulation also attaches great importance to the respect of the purpose limitation principle. Furthermore, information providers are also given the possibility to add further restrictions to the use of the data by Europol and other recipients (Article 19(2)). In that sense, Article 25 of the Europol Regulation makes an explicit reference to the obligation to comply with such specific restrictions on further use of the data. Future international agreements between the EU and third countries for the exchange of Europol data should thus ensure the effective application of these restrictions.

Finally, the international agreements in question should adduce adequate safeguards not only with respect to data protection but also with respect to other fundamental rights and freedoms of individuals. The international agreements will allow transfers of personal data collected in

the context of criminal investigations. These data will be used in the receiving country to order specific measures of surveillance, to conduct arrests, to provide evidence for criminal prosecution and ultimately to impose criminal penalties. The envisaged transfers of personal data to third countries might thus have implications for other fundamental rights recognised by the Charter in Chapter I "Dignity" of the Charter (i.e. the right to human dignity, the right to life, the right to the integrity of the person, the prohibition of torture and inhuman or degrading treatment or punishment) and Chapter VI "Justice" (i.e. the right to an effective remedy and to a fair trial, the right to the presumption of innocence and the right of defence, principles of legality and proportionality of criminal offences and penalties, the right not to be tried or punished twice in criminal proceedings for the same offence). In this regard, the EDPS notes that some of the third countries for which cooperation with Europol is envisaged have been found in breach of such fundamental rights. The United Nations Committee Against Torture has pointed to grave deficiencies in some of these countries in relation to reported cases of acts of torture and ill-treatment, the conditions of places of detention, the use of coerced evidence, the lack of basic safeguards for detainees and the living conditions in refugee camps[24]. Given the EU ongoing commitment to actively promote and defend human rights when engaging in relations with non-EU countries, the **EDPS insists that essential guarantees also apply in the context of criminal investigations and that the safeguards put in place in the future international agreements with Europol address, on a case-by-case basis, the foreseeable risks that such transfers could pose**.

4. SPECIFIC RECOMMENDATIONS

The EPDS wishes to express the following general~~preliminary~~ observations and specific recommendations on the negotiation directives included in the Annexes to the Recommendations. These comments are without prejudice to any additional recommendations that the EDPS could make on the basis of further available information and the provisions of the draft agreements during the negotiations.

Most of the data protection principle and safeguards to ensure the protection of individuals' personal data that the EDPS will address below are mentioned in general terms in the negotiation directives. Nonetheless, the EDPS would like to insist on the importance of providing concrete and specific safeguards, as well as safeguards with teeth. Given the law enforcement context and the potential risks that such transfers of data could pose to data subjects, **the safeguards included in these international agreements with third countries should satisfactorily address and mitigate these risks**. Moreover, **these safeguards should be clear and effective in order to fully comply with EU primary law and be in line with the recent Opinion 1/15 of the CJEU**[25] .

4.1. Purpose limitation and purpose specification of data transfers by Europol

Purpose limitation is a cornerstone principle of the EU data protection frameworks. The Europol Regulation states in this respect that "it contributes to transparency, legal certainty and predictability and is particularly of high importance in the area of law enforcement cooperation, where data subjects are usually unaware when their personal data are being collected and processed and where the use of personal data may have a very significant impact on the lives and freedoms of individuals"[26]. More specifically, purpose limitation requires on the one hand that personal data are collected for specified, explicit and legitimate purposes and, on the other

hand, that personal data are not further processed in a manner that is incompatible with those purposes.

a) Specification of the purposes of the data transfers

Article 18 of the Europol Regulation provides a list of purposes for data processing activities by Europol that are considered legitimate[27]. For operational analyses, the purposes of data processing activities have to be further specified in the opening decisions of Operational Analysis Projects (Article 18(3))[28].

Directive 2 of each of the Annexes limits the cooperation of Europol and third countries' authorities under the future international agreements to crimes and related criminal offences that fall within the mandate of the agency. Directive 2 then specifies the purposes of such cooperation by listing different crime areas for each of the agreements. Directive 3(a) further states that "[t]he purposes of the processing of personal data by the Parties in the context of the Agreement shall be spelt out clearly and precisely, and shall be no wider than what is necessary in individual cases for the purpose of preventing and combating terrorism and criminal offences referred to in the Agreement".

Given the strong emphasis placed on purpose limitation in the Europol Regulation, **the EDPS recommends specifying more narrowly the purposes of the transfers for each agreement in directive 2 of each one of the Annexes. To that end, the EDPS recommends more specifically that:**

- the lists of offences regarding which personal data will be exchanged should be clearly defined in the international agreements. In particular, the agreements should define in a clear and precise manner the activities covered by those crimes, and the persons, groups and organisations likely to be affected by the transfer;
- the list of Europol's Operational Analysis Projects in which the third counties in question will participate, as well as the conditions for such participation, should be made available in advance to the authorities in charge of supervising the implementation of the agreement;
- the terms "individual cases" should be clearly defined in the international agreements, as this will form the yardstick against which the necessity and proportionality of the transfers will be assessed. It is not clear whether these terms refer to criminal investigations or criminal intelligence operations targeting specific individuals considered as suspects, if it also includes individuals who are victims, witnesses or contacts and if this could justify mass data transfers (for instance, in relation to a list of young persons travelling to a third country in question who are suspected to be radicalised).

b) Limitation of further processing of the transferred data by the receiving authority

Directive 3(b) of the Annexes limits the processing of personal data "only [to] the purposes for which they have been transferred". The EDPS stresses that compliance with this principle is closely linked to the scope of competences of recipients in the receiving third countries. To ensure respect of the purpose limitation principle, the scope of competence of the specific authorities in the receiving third countries to which Europol will transfer data and which will process these data should be clearly defined in order to ensure that they are also competent for the purposes of the transfer. In that sense, Article 4(2) of Directive (EU) 2016/680 limits the further processing by the same or another controller for purposes of prevention, investigation, detection or prosecution of criminal offences, including the safeguarding and the prevention of threats to public security, other than that for which the personal data are collected to cases

where the processing is necessary and proportionate to that other purpose and *where the recipient is authorised to process such personal data for such a purpose* in accordance with the legal framework regulating its activities. Therefore, the EDPS **recommends that international agreements be accompanied by an exhaustive list of the competent authorities in the receiving third countries to which Europol will transfer data as well as a short description of their competences. This should also be reflected in one of the directives of the Annexes.**

4.2. Onward transfers

The EDPS points out that there is a discrepancy between directive 3(b) of the Annexes ("personal data transferred by Europol in accordance with the Agreement shall be processed [...] only for the purposes for which they have been transferred") and directive 3(h) ("onward transfers of information from competent authorities of [the third country] to other authorities in [the same country] shall only be allowed for the purposes of the Agreement and shall be made subject to appropriate conditions and safeguards"). **Directive 3(h) of the Annexes should be more restrictive than "the purposes of the Agreement" and limit onward transfers from competent authorities of the third country to other authorities of the same country to the original purposes of the transfer by Europol.**

4.3. Specific restrictions on the processing of information transferred by Europol

Article 19(2) and (3) of the Europol Regulation gives to Member States and other providers of information to Europol, as well as to Europol itself, the possibility to indicate any restrictions regarding the access, use, transfer, erasure or destruction of the data, and oblige Europol to comply with these restrictions. Future international agreements concluded between the EU and third countries for the exchange of data between Europol and their national competent authorities cannot ignore the restrictions that Member States and other providers have imposed regarding the use and access to the data they have shared with Europol. International agreements with third countries should thus ensure the effective application of these restrictions[29]. For now, directive 3(b) of the Annexes only requires "the possibility for Europol to indicate, at the moment of transferring the data, any restriction on access or use, including as regards its transfer, erasure or destruction". **The EDPS recommends strengthening the language of this directive to state that Europol shall indicate, at the moment of transferring the data, any existing restrictions regarding further processing of these data. The international agreements should oblige competent authorities of the third countries in question to respect these restrictions and specify how compliance with these restrictions will be enforced in practice.**

4.4. Independent oversight

While the EDPS is the independent authority in charge of supervising the data processing activities of Europol, including the transfer of data to third countries, there is also a need for an effective independent oversight once the data have been transferred in the receiving third countries. The EDPS recalls that both Article 16 of the TFEU and Article 8(3) of the Charter include as essential guarantee of the right to data protection: the control by an independent authority. The EDPS thus welcomes that directive 3(j) of the Annexes require that future international agreements ensure "a system of oversight by one or more independent public authorities responsible for data protection with effective powers of investigation and intervention to exercise oversight[,] to engage in legal proceedings [and which] have powers

to hear complaints from individuals". Moreover, the public authorities entrusted with such independent oversight should be granted these powers over all authorities to which Europol will transfer data on the basis of the international agreements.
The EDPS recalls that, pursuant to the CJEU[30] case-law, an independent supervisory authority within the meaning of Article 8(3) of the Charter is an authority able to make decisions independently from any direct or indirect external influence. Such a supervisory authority must not only be independent from the parties it supervises, but it should also not be "subordinate to a further supervisory authority, from which it may receive instructions" as this would imply that it is "not free from any external influence liable to have an effect on its decisions"[31].

4.5. Rights of data subjects

The EDPS welcomes that directive 3(d) of the Annexes require that the future international agreements ensure "enforceable rights of individuals whose personal data are processed by laying down rules on the right of access, rectification and erasure, including the specific grounds which may allow any necessary and proportionate restrictions".

The EDPS first recalls that the right of access and the right to rectification are essential elements of the right to data protection under Article 8(2) of the Charter. If the exercise of data subjects' rights are usually limited in the law enforcement context in order to avoid jeopardising ongoing investigations, the possibility for data subjects to exercise their rights should exist in practice and not remain purely theoretical, even if limited or performed by a trusted third party in situations where the exercise of these rights is denied to protect sensitive law enforcement information (as it is the case in the Europol Regulation).

Moreover, the EDPS takes note of the fact that the Annexes do not include any directive regarding the right to information. The right to information is also of utmost importance as it allows the exercise of other data protection rights, including the right to remedies, and ensures fair processing of the data[32]. Data subjects usually have no knowledge of the fact that their data are processed (or transferred) for law enforcement purposes. In the case of Europol, the Europol Regulation does not include any obligation for Europol to proactively inform data subjects of the fact that the agency is processing personal information regarding them. Data subjects have to exercise their right of access to find out if Europol is processing data about them. Nonetheless, in its recent Opinion 1/15, the CJEU found that "air passengers must be notified of the transfer of their PNR data to Canada and of its use as soon as that information is no longer liable to jeopardise the investigations being carried out by the government authorities" considering that "[t]hat information is, in fact, necessary to enable the air passengers to exercise their rights to request access to PNR data concerning them and, if appropriate, rectification of that data, and, in accordance with the first paragraph of Article 47 of the Charter, to an effective remedy before a tribunal"[33]. **The EDPS therefore recommends to include the right to information in the Annexes requiring the future international agreements to provide for obligations of transparency upon third countries' authorities to which Europol will transfer data.**

4.6. Transfer of special categories of data

Directive 3(c) of the Annexes provide that transfer of special categories of data should be prohibited "unless it is strictly necessary and proportionate in individual cases for preventing or combating criminal offences [...] and subject to appropriate safeguards", and that transfer of data relating to specific categories of data subjects should also be accompanied by specific

safeguards. The EDPS considers that, if the future international agreements concluded with countries provide that special categories of data may be transferred to third countries, they should contain specific provisions to ensure that they receive a level of data protection comparable to the specific provisions imposed on Europol. The Europol Regulation subjects the processing of special categories of data and the processing of data relating to specific categories of data subjects (i.e. victims, witnesses, contacts, informants and persons under the age of 18) to the principles of strict necessity and proportionality (Article 30(1) and (2))[34].

Moreover, the EDPS points out that, to the extent the future international agreements would provide that special categories of data may be transferred to third countries, the Court of Justice held in Opinion 1/15 that any transfer of such sensitive data would require "**a precise and particularly solid justification**, **based on grounds other than the protection of public security against terrorism and serious transnational crime**"[35]. Without such justification, the Court held as regards Canada that the provisions of the agreement on the transfer of sensitive data and on the processing and retention of that data are incompatible with fundamental rights[36].

4.7. Data retention

Directive 3(b) of the Annexes provide that personal data transferred "shall not be retained for longer than is necessary for the purposes for which they have been transferred". Directive 3(e) further requires that the agreements lay down rules on storage, review, correction and deletion of personal data. In that regard, the EDPS would like to point out that the Europol Regulation contains an elaborated regime for data retention that relies both on detailed rules for data retention and on technical[37] and procedural safeguards, which ensure that data retention obligations are complied with in practice[38]. Article 31 requires Europol to conduct reviews of the necessity and proportionality of storing the data every three years. This is without prejudice to different retention periods communicated by data providers when sending the data to Europol, which are binding for Europol. Any decision to store the data after the first three years must be duly justified and the motivation must be recorded. In addition, Article 31(6) of the Europol Regulation provides a list of exceptions to the obligation to delete the data. Europol is also bound to delete the data that have been deleted in the systems of the data provider as soon as it is informed thereof. Europol should likewise be able to inform third parties to whom data have been communicated or transferred that the data will be erased from its systems.

4.8. Suspension or termination of the international agreements in cases of breaches

The EDPS notes that the directive 3(5) of the Annexes to the Recommendations provide for the possibility to suspend or terminate the international agreements in question. Similarly to existing adequacy decisions based on Article 25 of the current Directive 95/46/EC, and to Article 36(5) of Directive 2016/680 regarding adequacy decisions for law enforcement purposes, the EDPS considers it is of utmost importance to include the possibility to suspend or terminate these international agreements with third countries in cases of breaches of their provisions by the law enforcement authorities of the receiving third countries. In this respect, the EDPS also stresses the paramount role of independent supervision of the application of future international agreements in order to allow the identification of breaches. Furthermore, **the EDPS recommends specifying 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.**

5. CONCLUSION

The EDPS welcomes the attention paid to data protection in the Annexes to the Commission Recommendations of 20 December 2017 that will constitute the mandate of the Commission to negotiate on behalf of the EU the respective international agreements with each one of the eight MENA countries for which cooperation with Europol is envisaged.

The necessity and proportionality of the international agreements envisaged to allow Europol to regularly transfer data to the competent authorities of the eight third countries in question need to be fully assessed to ensure compliance with Article 52(1) of the Charter. To allow such an in depth assessment on a case-by-case basis, the EDPS recommends to ~~considers that the needs for transfers should be~~ further narrow~~ed~~ down and differentiate~~d~~ the needs for transfers based on the particular situation of each third country and the reality on the ground. The scope of each international agreement and the purposes for transfers to each third country should be further specified accordingly in the Annexes. The EDPS recommends further carrying out impact assessments to better assess the risks posed by transfers of data to these third countries for individuals' rights to privacy and data protection, but also for other fundamental rights and freedoms protected by the Charter, in order to define the precise safeguards necessary.

The EDPS notes that, pursuant to Article 25(1)(b) of the Europol Regulation, Europol could regularly transfer data to a third country through the conclusion of a binding international agreement between the EU and the receiving third country on the condition that such agreement adduce appropriate safeguards. The EDPS considers that "adducing appropriate safeguards" within the meaning of the Europol Regulation implies that the international agreements concluded with third countries should:

- ensure full consistency ~~compliance~~ with Article 8 of the Charter in the receiving third countries, in particular with the purpose limitation principle, the right of access, the right to rectification and the control by an independent authority specifically stipulated by the Charter;
- follow Opinion 1/15 of the CJEU by ensuring that the level of protection resulting from these agreements be essentially equivalent to the level of protection in EU law;
- apply mutatis mutandis the criteria included in Recital 71 of Directive (EU) 2016/680, i.e. transfers of personal data are subject to confidentiality obligations, the principle of specificity 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;
- mirror~~replicate~~ specific safeguards included in the Europol Regulation, such as restrictions specified by information providers; and
- apply essential guarantees in the context of criminal investigations and include safeguards that address on a case-by-case basis the foreseeable risks that transfers to these third countries could pose with respect to other fundamental rights and freedoms.

In addition to these general recommendations, the recommendations and comments of the EDPS in the present O~~o~~pinion relate to the following specific aspects of the future international agreements to be negotiated with MENA countries in the negotiating mandates:

- the purpose limitation -and purpose specification principles regarding data transferred by Europol;
- onward transfers by competent authorities of the third countries in question;
- restrictions on the processing of information transferred by Europol to the competent authorities of the third countries;
- independent oversight ensured in the third countries;

- the rights of data subjects;
- transfer of special categories of data to the competent authorities of the third countries;
- data retention of the data transferred by Europol; and
- the possibility to suspend and terminate the international agreements in cases of breaches of their provisions.

Brussels, 14~~5~~ March 2018

Giovanni BUTTARELLI
European Data Protection Supervisor

NOTES

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 119, 4.5.2016, p. 1.
[3] OJ L 8, 12.1.2001, p. 1.
[4] OJ L 350, 30.12.2008, p. 60.
[5] OJ L 119, 4.5.2016, p. 89.
[6] 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, hereinafter "the Europol Regulation".
[7] 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, OJ L 119, 4.5.2016, p. 89.
[8] Recommendation for a Council Decision authorising the opening of negotiations for an agreement between the European Union and the Hashemite Kingdom of Jordan on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the Jordanian competent authorities for fighting serious crime and terrorism, COM(2017) 798 final; Recommendation for a Council Decision authorising the opening of negotiations for an agreement between the European Union and the Republic of Turkey on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the Turkish competent authorities for fighting serious crime and terrorism, COM(2017) 799 final; Recommendation for a Council Decision authorising the opening of negotiations for an agreement between the European Union and the Lebanese Republic on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the Lebanese competent authorities for fighting serious crime and terrorism, COM(2017) 805 final; Recommendation for a Council Decision authorising the opening of negotiations for an agreement between the European Union and the State of Israel on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the Israeli competent authorities for fighting serious crime and terrorism, COM(2017) 806 final; Recommendation for a Council Decision authorising the opening of negotiations for an agreement between the European Union and Tunisia on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the Tunisian competent authorities for fighting serious crime and terrorism, COM(2017) 807 final; Recommendation for a Council Decision authorising the opening of negotiations for an agreement between the European Union and the Kingdom of Morocco on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the Moroccan competent authorities for fighting serious crime and terrorism, COM(2017) 808 final; Recommendation for a Council Decision authorising the opening of negotiations for an agreement between the European Union and the Arab Republic of Egypt on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the Egyptian competent authorities for fighting serious crime and terrorism, COM(2017) 809 final; Recommendation for a Council Decision authorising the opening of negotiations for an agreement between the European Union and the People's Democratic Republic of Algeria on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the Algerian competent authorities for fighting serious crime and terrorism, COM(2017) 811 final.
[9] Communication from the Commission of 28 April 2015 to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - The European Agenda On Security, COM(2015) 185 final.
[10] Conclusions from the Council of 19 June 2017 on EU External Action on Counter-terrorism, Document 10384/17.
[11] Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union's Foreign and Security Policy, available at: http://europa.eu/globalstrategy/en.
[12] Communication from the Commission of 18 October 2017 to the European Parliament, the European Council and the Council – Eleventh progress report towards an effective and genuine Security Union, COM(2017) 608 final.
[13] See the Memorandum of Understanding of all Commission Recommendations for Council Decisions tabled on 20 December 2017, except for the one concerning Israel.

[14] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data, OJ L 8, 12.1.2001, p. 1.
[15] Directive 3(8) of the Annexes to the Recommendations concerning Algeria, Egypt, Israel, Jordan and Lebanon; see also Communication from the Commission of 10 January 2017 to the European Parliament and the Council on Exchanging and Protecting Personal Data in a Globalised World, COM(2017) 7 final, p. 11 where the Commission promotes accession by third countries to Council of Europe Convention 108 and its additional Protocol.
[16] For now, Turkey as a member State of the Council of Europe has signed Convention 108, Tunisia as a non-member State has acceded to Convention 108 and Morocco as a non-member State has been invited to accede. Algeria, Egypt, Israel, Jordan and Lebanon have not entered such process.
[17] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, ETS No. 108.
[18] The EDPS is not aware of any short-term plan of the Commission to engage with these third countries and perform comprehensive assessments of their legal systems in view of adopting such adequacy decisions.
[19] Article 25(5) of the Europol Regulation provides for derogations that can be used on a case by case basis for individual transfers; they cannot apply to systematic, massive or structural transfers. Article 25(6) also provides for derogations for set of transfers that must be duly justified and documented and carried out in agreement with the EDPS.
[20] Joined cases C-402/05 P and C-415/05 P, Kadi v. Council, ECLI:EU:C:2008:461, para. 285.
[21] Opinion 1/15, EU-Canada PNR Agreement, ECLI:EU:C:2017:592.
[22] Opinion 1/15, EU-Canada PNR Agreement, ECLI:EU:C:2017:592, para. 214; see also para. 93 of Opinion 1/15.
[23] In the case of Article 37 of Directive (EU) 2016/680, the legally binding instruments are those concluded between Member States and third countries.
[24] See the latest reports of the United Nations Committee Against Torture available at: http://www.ohchr.org/EN/Countries/MENARegion/Pages/LBIndex.aspx.
[25] Opinion 1/15, EU-Canada PNR Agreement, ECLI:EU:C:2017:592, specifically para. 134, where the Court found that "[e]ven though the means intended to ensure such a level of protection may differ from those employed within the European Union [...], those means must nevertheless prove, in practice, effective in order to ensure protection essentially equivalent to that guaranteed within the European Union".
[26] Recital 26 of the Europol Regulation.
[27] Namely cross-checking, strategic or thematic analysis, operational analysis, and facilitation of exchanges of information between Member States, Europol, other Union bodies, third countries and international organisations.
[28] Operational Analysis Projects are platforms in which operational analysis can be conducted to support international criminal investigations and criminal intelligence operations against specific targets. They are defined by Europol on the basis of operational needs of Member States in the context of the cross-border fight of serious crimes falling within the scope of competences of Europol. The scope of such platforms can in particular be a crime area covering one or more types of crime; it can relate to a geographical dimension, or it can focus on particular crime structures, phenomena or incidents that due to their size, complexity or impact require a dedicated approach.
[29] Under the current Europol Analysis System, this is regulated through the use of handling codes, which are binding for all Member States and other information providers.
[30] See Case C-518/07, Commission v Germany, ECLI:EU:C:2010:125, para. 25; Case C-614/10, Commission v Austria, ECLI:EU:C:2012:631, para. 36 and 37; Case C-288/12, Commission v Hungary, para. 48; Case C-362/14, Maximillian Schrems v Data Protection Commissioner, ECLI:EU:C:2015:650, para. 41.
[31] Opinion 1/15, EU-Canada PNR Agreement, ECLI:EU:C:2017:592, para. 230.
[32] Case C-201/14, Smaranda Bara and Others v Președintele Casei Naționale de Asigurări de Sănătate, Casa Națională de Asigurări de Sănătate, Agenția Națională de Administrare Fiscală, ECLI:EU:C:2015:638, in particular para. 32 and 33 where the Court found that "the requirement to inform the data subjects about the processing of their personal data is all the more important since it affects the exercise by the data subjects of their right of access to, and right to rectify, the data being processed, and their right to object to the processing of those data" and that "That information concerns the identity of the data controller, the purposes of the processing and any further information necessary to guarantee fair processing of the data".
[33] Opinion 1/15, EU-Canada PNR Agreement, ECLI:EU:C:2017:592, para. 220.
[34] In practice, these provisions are implemented through a specific assessment made in the Opening Decision of each Operational Analysis Project. All participants to the Operational Analysis Project have access to this information in accordance with the rules defined in Article 20 of the Europol Regulation.
[35] Opinion 1/15, EU-Canada PNR Agreement, ECLI:EU:C:2017:592, para. 165.
[36] Opinion 1/15, EU-Canada PNR Agreement, ECLI:EU:C:2017:592, para. 167.

[37] For instance, the obligation for Europol to store the data in a way that ensures that their source can be established (Article 38(1)) or the obligation to log all data operations performed over the data (Article 40)(1)).
[38] For instance, the obligation for Europol to communicate logs upon request to the EDPS, Europol's Data Protection Officer or the national unit in the context of a specific investigation (Article 40(2)).