EUROPEAN
COMMISSION

Brussels, 14.4.2021
COM(2021) 177 final

ANNEX

ANNEX

to the

Recommendation for a Council Decision

authorising the opening of negotiations for a cooperation agreement between the European Union and the International Criminal Police Organisation (ICPO-INTERPOL)

ANNEX

In the course of the negotiations, the Commission should aim to achieve the objectives set out in detail below.

(1) To regulate cooperation between Europol and Interpol, taking into account the latest developments in combating terrorism, cross-border and transnational serious, organised crime, current operational needs, Europol's mandate, in full respect of the EU data protection and fundamental rights requirements;

(2) To provide the safeguards and guarantees needed to authorise 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) 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;

(3) To provide the safeguards and guarantees needed to authorise EU Member States and Frontex (its European Travel Information and Authorisation System (ETIAS) Central Unit) to access Interpol's Stolen and Lost Travel Document and Travel Document Associated With Notices databases via the European Search Portal, in compliance with EU data protection requirements and with fundamental rights;

(4) To provide the safeguards and guarantees needed to implement a revised Visa Information System Regulation that authorises EU Member States to access Interpol's Stolen and Lost Travel Document and Travel Document Associated With Notices databases via the European Search Portal when examining applications for visas or residence permits, in full compliance with EU data protection requirements and with fundamental rights;

(5) To set up and regulate cooperation between the European Public Prosecutor's Office (EPPO) as established under Regulation (EU) 2017/1939 and Interpol, in line with their mandates, and in full compliance with EU data protection requirements and with fundamental rights;

(6) To provide the legal basis to authorise Europol, Frontex category 1 staff (statutory staff of the standing corps) and the European Public Prosecutor's Office to access relevant Interpol databases to carry out their tasks, in full compliance with EU data protection requirements and with fundamental rights;

(7) To provide the legal basis to authorise Eurojust and the European Public Prosecutor's Office to exchange operational information with Interpol, in full compliance with EU data protection requirements and with fundamental rights;

Specifically, the cooperation Agreement should:

(a) Establish agreed definitions of key terms, including on personal data, compliant with Regulations (EU) 2016/679 and 2018/1725, and Article 3(1) of Directive (EU) 2016/680;

(b) Provide that any automated queries of Interpol's Stolen and Lost Travel Document and Travel Document Associated With Notices databases in the context of European Travel Information and Authorisation System, interoperability and a revised Visa Information System Regulations must be carried out in such a way that no information is revealed to the State owner of the Interpol alert;

(c) Spell 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. In particular:

(i) The purposes of processing personal data in the context of the Agreement must be spelt out clearly and precisely by the Parties, and be no wider than what is necessary in individual cases for the purposes of the Agreement;

(ii) Personal data transferred to Interpol by EU Justice and Home Affairs agencies and bodies in line with their mandates under the Agreement must be processed fairly, on a legitimate basis and only for the purposes for which they have been transferred. Any further data processing incompatible with the initial data processing must be prohibited (purpose limitation). The 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;

(iii) Transferred personal data must be adequate, relevant and limited to what is necessary for the purpose for which it has been transferred. It must be accurate and kept up to date. It must not be retained for longer than is necessary for the purpose for which it has been transferred. The Agreement must lay down rules on storage, including storage limitation, on review, correction and deletion of personal data;

(iv) The Agreement must specify the criteria on the basis of which the reliability of the source and accuracy of the data shall be indicated;

(v) The transfer of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, and data concerning a person's health and sex life or sexual orientation, must be allowed only where necessary and proportionate in individual cases for preventing or combating criminal offences as referred to in the Agreement, and subject to appropriate safeguards addressing the specific risks of processing. The Agreement should contain specific safeguards governing the transfer of personal data on minors and on victims of criminal offences, witnesses or other persons who can provide information concerning criminal offences;

(vi) The Agreement must lay down rules on the information to be made available to individuals and must ensure enforceable rights of individuals whose personal data are processed, in the form of rules on the right of information, access, rectification and erasure, including the specific grounds that may allow any necessary and proportionate restrictions. The Agreement must also ensure enforceable rights of administrative and judicial redress for any person whose data are processed under the Agreement and guaranteeing effective remedies;

(vii) The Agreement must lay down the rules on keeping records for the purposes of logging and documentation;

(viii) The Agreement must provide for safeguards in respect to automated processing of personal data including on profiling, and to prohibit decisions based solely on the automated processing of personal information without human involvement.

(ix) The Agreement must include the obligation to ensure security of personal data through appropriate technical and organisational measures, including by

allowing only authorised persons to have access to personal data. It must also include the obligation to notify the competent authorities and, wherever necessary, data subjects, in the event of a personal data breach affecting data transferred under the Agreement. The Agreement must also include the obligation to implement data protection by default and by design measures designed to implement data protection principles in an effective manner;

(x) Onward 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 and must be allowed only with respect to third countries or international organisations ensuring an essentially equivalent level of protection of personal data as ensured under this Agreement, unless the onward transfer is necessary for the prevention and investigation of a serious and imminent threat to public security or to protect the vital interests of any natural person. In particular, such onward transfers may be allowed in case the international organisation or third country is covered by an adequacy decision of the Commission under Article 36 of Directive (EU) 2016/680 or by appropriate safeguards for the protection of personal data ensured by an international Agreement pursuant to Article 218 TFEU concluded between the Union and that international organisation or third country or by a cooperation Agreement allowing for the exchange of operational personal data between the Agency and the third country or international organisation in question that cover onward transfers and concluded before the date of application of the legal act establishing the Agency concerned.

(xi) The Agreement must ensure a system of oversight over the use by Interpol of that personal data by one or more independent bodies responsible for data protection with effective powers of investigation and intervention. In particular, the body or bodies shall have powers to hear complaints from individuals about the use of their personal data. The Agreement must provide for the duty of cooperation between the oversight bodies for Interpol, on the one hand, and the relevant EU agency or Member States authority, on the other hand.

(d) The cooperation Agreement must provide for an effective dispute settlement mechanism with respect to its interpretation and application to ensure that the parties observe mutually agreed rules.

(e) The cooperation Agreement must include a provision on the entry into force and validity and a provision whereby a party may terminate or suspend it.

(f) The cooperation Agreement must include provisions on the monitoring and periodic evaluation of the Agreement.

(g) The cooperation Agreement must be equally authentic in the Bulgarian, Czech, Croatian, Danish, Dutch, English, Estonian, Finnish, French, German, Greek, Hungarian, Irish, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish and Swedish languages and should include a language clause to that effect.