European Parliament
2019-2024

TEXTS ADOPTED

P9_TA(2022)0275

Negotiations for a cooperation agreement between the EU and Interpol

European Parliament recommendation of 5 July 2022 to the Council and the Commission on the negotiations for a cooperation agreement between the European Union and the International Criminal Police Organization (ICPO-INTERPOL) (2022/2025(INI))

The European Parliament,

– having regard to Article 218 of the Treaty on the Functioning of the European Union (TFEU),

– having regard to the TFEU, and in particular Article 16, Article 82(1) and Article 87(2) thereof,

– having regard to the Charter of Fundamental Rights of the European Union (the 'Charter'), and in particular Articles 7, 8, 47 and 52 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] (Law Enforcement Directive),

– 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 Union institutions and bodies and on the free movement of such data[3] (EUDPR), and in particular Article 42(1) thereof,

---

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.

– having regard to 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 and2009/968/JHA[1],

– having regard to 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[2],

– having regard to Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office ('the EPPO')[3],

– having regard to 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)[4],

– having regard to Opinion 8/2021 of the European Data Protection Supervisor of 25 May 2021 on the Recommendation for a Council decision authorising the opening of negotiations for a cooperation agreement between the EU and Interpol,

– having regard the study of its Policy Department for Citizens' Rights and Constitutional Affairs of February 2022 entitled 'Ensuring the rights of EU citizens against politically motivated Red Notices',

– having regard to Interpol's Rules on the Processing of Data,

– having regard to the Parliamentary Assembly of the Council of Europe's resolutions 2161 (2017) on abusive recourse to the Interpol system: the need for more stringent legal safeguards and 2315 (2019) on Interpol reform and extradition proceedings: building trust by fighting abuse,

– having regard to 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[5],

– having regard to 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[6],

---

1 OJ L 135, 24.5.2016, p. 53.
2 OJ L 295, 14.11.2019, p. 1.
3 OJ L 283, 31.10.2017, p. 1.
4 OJ L 295, 21.11.2018, p. 138.
5 OJ L 135, 22.5.2019, p. 27.
6 OJ L 135, 22.5.2019, p. 85.

– having regard to Rules 114(4) and 54 of its Rules of Procedure,

– having regard to the opinion of the Committee on Foreign Affairs,

– having regard to the report of the Committee on Civil Liberties, Justice and Home Affairs (A9-0200/2022),

A. whereas present-day terrorism and serious and organised crime are dynamic, complex, innovative, globalised, mobile and often transnational phenomena, requiring a robust response and more effective, coordinated EU cooperation with international law enforcement authorities and bodies such as the International Criminal Police Organization (Interpol); whereas the Commission's 2020 EU Security Union strategy calls on the Member States to step up multilateral cooperation and coordination between the EU and Interpol, as this is essential to enhancing cooperation and information exchange; whereas Parliament's resolution of 17 December 2020 on the EU Security Union strategy[1] stresses the need for stronger cooperation between the Member States and for better coordination at EU level between all actors;

B. whereas effective international cooperation, in full respect of fundamental rights, is an important component of effective law enforcement and judicial cooperation, especially on types of crime involving the processing and sharing of personal data; whereas the legality of processing personal data is governed by the Union data protection *acquis*, and whereas that also applies to bilateral agreements with key partners who play an important role in obtaining information and potential evidence from beyond the EU;

C. whereas Interpol is the world's largest international criminal police organisation and has an important role to play all over the world; whereas Interpol is based on inter-governmental cooperation; whereas in December 2021, the Council adopted a negotiating mandate for the Commission to enter into negotiations, with the expectation of concluding by the end of 2022, on an international agreement on behalf of the EU seeking reinforced cooperation with Interpol, including access to Interpol's databases and the strengthening of operational cooperation; whereas it is paramount to ensure that the final agreement puts in place robust measures to guarantee compliance with the principles relating to the processing of personal data, as set out in the Union data protection *acquis*, as well as the correctness of the personal data received through such cooperation, and to ensure that all future cooperation and exchange of personal data respect fundamental rights, including the right to data protection and privacy;

D. whereas the EU and Interpol already have long-standing cooperation in a range of law enforcement-related areas through the operational implementation of the EU policy cycle / EMPACT (European Multidisciplinary Platform Against Criminal Threats) and by supporting the activities of Member States in cooperation with EU agencies, such as the EU Agency for Law Enforcement Cooperation (Europol), the European Border and Coast Guard Agency (Frontex), the EU Agency for Law Enforcement Training , the European Monitoring Centre for Drugs and Drug Addiction, and the EU Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice, on the basis of agreements or working arrangements; whereas on 5 November 2001, Europol and Interpol signed an operational agreement followed by a memorandum of understanding allowing the transfer of personal data through their respective liaison

[1] OJ C 445, 29.10.2021, p. 140.

officers; whereas on 27 May 2009 Frontex signed a working agreement with Interpol establishing a framework for cooperation with the objective of facilitating the prevention, detection and combating of cross-border crime and improving border security to combat illegal immigration, people smuggling and trafficking in human beings;

E. whereas individual EU Member States, in their capacity as Interpol member countries, can directly access Interpol's 19 databases, which include potentially valuable information on individuals, stolen property, weapons and threats; whereas these databases contain millions of records with information that could directly help to combat serious and organised crime and terrorism; whereas Frontex, Eurojust and the EPPO currently do not have any access to these databases, in line with their mandates – either directly or on a 'hit/no hit' basis – due to the lack of an agreement with Interpol, which is required for this purpose under Interpol's rules on the processing of data;

F. whereas current cooperation between the EU and Interpol is already close in the area of counterterrorism; whereas it should be stepped up and extended to new areas; whereas procedures should be improved, accelerated and streamlined to address a series of indispensable operational needs in order to facilitate swift access to information related to serious and organised crime and terrorism and to implement existing Union legal acts;

G. whereas the EU is the largest donor of funds to Interpol, which are mainly assigned to information exchanges in the field of law enforcement, but also include border management cooperation and capacity building activities, and to projects and programmes targeting a range of terrorism and serious crime activities; whereas this gives the EU an important role to play in improving the functioning of Interpol, and in particular, its transparency and accountability;

H. whereas the new agreement should establish a modern and coherent framework for the cooperation of EU bodies and agencies with Interpol, based on the already existing modes of cooperation; whereas the agreement should be in compliance with the general requirements of the Charter, the applicable Union data protection *acquis*, namely the EUDPR and the Law Enforcement Directive, the specific data protection requirements and safeguards laid down in the basic acts establishing the EU bodies, agencies and IT systems and the relevant Court of Justice of the EU (CJEU) jurisprudence and fundamental rights standards;

I. whereas the agreement should respond to operational needs, taking into account the latest developments in combating terrorism and cross-border, transnational, serious and organised crime; whereas the agreement provides the legal basis for the exchange of operational information, including personal data, and access to relevant Interpol databases by Union bodies and agencies in line with their mandates, under the condition that the agreement is legally binding and enforceable against all parties and that it includes all the necessary data protection safeguards;

J. whereas no fundamental rights impact assessment on the Commission Recommendation has been carried out;

K. whereas the adoption of the Union legal framework for interoperability between EU information systems in the area of justice and home affairs in May 2019 led to exploratory talks between the EU and Interpol on the need to enter into a cooperation agreement; whereas an advanced and shared data infrastructure is currently in place in the EU for

police and judicial cooperation, asylum and migration, as well as borders and visas; whereas this infrastructure, and the IT systems and EU databases that constitute it, allows for limited and highly regulated information sharing with third countries or international organisations;

L. whereas the new agreement should govern cooperation between Interpol and Europol, the EPPO, Eurojust and Frontex and provide direct access by these bodies, agencies and Member States for purposes strictly linked to the performance of their tasks, as regulated in their respective basic acts to two of Interpol's databases – the Stolen and Lost Travel Document (SLTD) and Travel Document Associated With Notices (TDAWN) databases via the European Search Portal (ESP), in compliance with EU data protection requirements and in full respect of fundamental rights;

M. whereas according to the Interpol constitution, Interpol is obliged not to assist or aid member countries that act in violation of international human rights law;

N. whereas governmental, international and non-governmental organisations continue to report abuses by some member countries of Interpol's notice and diffusion system in order to persecute political opponents, national human rights defenders, lawyers, civil society activists and journalists, in violation of international standards on human rights and Interpol's own rules; whereas according to reports by the Commission and civil society organisations, Interpol has reformed and strengthened its red notices review processes, as well as its support systems for National Central Bureaus in member countries, reformed the setup and functioning of the Commission for the Control of Files, which enforces its complaints mechanism, appointed a data protection officer and implemented a learning and knowledge-sharing programme; whereas despite those reforms, serious concerns remain related to possible abuses of the Interpol system that impact fundamental rights, as recent reports still emphasise the need for more legal safeguards, more transparency and better implementation of reforms; whereas there are significant challenges with the mechanisms to update information regarding red notices and diffusions, as they sometimes remain in effect in the national databases despite having been updated and removed by the General Secretariat of Interpol; whereas both written sources and interviews with governmental and non-governmental organisations suggest that Interpol's vetting process remains inconsistent;

O. whereas Article 3 of Interpol's constitution prohibits any intervention or activity of political, military, religious or racial character; whereas abuses in high profile cases in multiple member countries of Interpol have still been observed in recent years; whereas politically motivated extraditions are often triggered by the abusive issuing of a red notice or 'wanted person diffusion' through Interpol; whereas scarce information is made available by Interpol on the manner in which it reviews red notices, its administrative ability to do so and the outcomes of these reviews, leading to a lack of transparency as regards how Interpol works towards effectively countering politically motivated red notices; whereas member countries and other international organisations have little access to information about the overall handling of red notices and diffusions; whereas no information is available on the countries making the requests for such notices, how many requests are accepted and refused, the grounds for refusal, which countries perform better or worse in terms of acceptance or refusal of requests and the development of these practices over time; whereas this makes it impossible to evaluate the quality of the General Secretariat of Interpol's vetting process, the work of the National Central Bureaus or the quality of the requests submitted by countries;

P. whereas Parliament, in its resolution of 16 September 2021 on the case of human rights defender Ahmed Mansoor in the United Arab Emirates[1], expressed deep concern about the candidacy and appointment as Interpol's president of the General Inspector of the Ministry of Interior of the United Arab Emirates, Major General Ahmed Nasser Al Raisi, and called on the members of Interpol's General Assembly, and in particular the EU Member States, to duly examine the allegations of human rights abuses levelled against him; whereas on 11 May 2022, investigations into claims of torture were opened against Interpol's president in France;

Q. whereas cooperation between the European Union and Interpol is underpinned by trust in Interpol's system and internal processes; whereas trust in Interpol's system of red notices and diffusions relies on the prevention and swift tackling of misuse of Interpol notices by countries seeking to use Interpol systems for political and repressive ends; whereas, Interpol must ensure that the personal data processed internally through its systems complies with human rights and the rule of law;

R. whereas numerous authoritarian countries still remain member countries of Interpol; whereas in recent years authoritarian regimes have been successful in politically abusing the system of red notices and diffusions, persecuting individuals outside of their jurisdictions and subjecting them to real, practical, and invasive restrictions on their lives and fundamental rights;

S. whereas Russia's invasion of Ukraine is a direct threat to international law enforcement cooperation and its continued access to Interpol's databases is a threat to the integrity of the EU's cooperation with Interpol; whereas Russia is responsible for a very large number of red notices and diffusions worldwide and is responsible for circulating most politically motivated red notices, including against EU citizens – such as the Lithuanian judges, prosecutors and investigators looking into the events in Vilnius on 13 January 1991; whereas besides Russia, other countries have also used the system of red notices to politically target their citizens;

1. Recalls that EU values, fundamental rights and the Union data protection *acquis*, namely the EUDPR and the Law Enforcement Directive, must be the basis of Union policy in the area of law enforcement cooperation, ensuring compliance with the principles of necessity, proportionality, legality and the presumption of innocence, and guaranteeing accountability and judicial redress, while ensuring effective protection of individuals, particularly the most vulnerable; recalls, further, that compliance with these rights and principles, including the right to privacy and the protection of personal data, should be at the core of the development of digitalisation in the area of justice and security and the development of the interoperability framework; stresses that these principles should be at the core of the negotiations between the EU and Interpol on a cooperation agreement;

2. Underlines the absolute necessity of basing the agreement with Interpol on the full respect of the Charter, the Union data protection *acquis* and the specific data protection requirements and safeguards codified in the basic acts establishing the relevant EU agencies, bodies and large-scale IT systems and their respective mandates; stresses, therefore, that the Council Decision on the possible conclusion of this envisaged agreement should also be based on Article 16 TFEU;

---

[1] OJ C 117, 11.3.2022, p. 109.

3. Notes that prior to adopting the Recommendation for a Council Decision authorising the opening of negotiations for a cooperation agreement between the European Union and Interpol, the Commission did not perform a fundamental rights impact assessment on the necessity and proportionality of each envisaged measure or on the legal feasibility of all envisaged measures under a single overarching agreement;

4. Recommends that the Commission follow the Council's differentiation between the areas of law enforcement, judicial cooperation in criminal matters and border security as part of border management;

5. Recommends that the Commission ensure access to Interpol's different databases on the basis of the needs and according to the scope of competences laid down in the respective mandates of the different EU bodies and agencies; recalls that Interpol's databases contain millions of records with information that could potentially help to combat crime; recalls, however, that there are documented problems with the accuracy, reliability and origin of the data within those databases that should be addressed;

6. Stresses that the Commission should guarantee controlled access to Interpol's databases by EU Member States, and EU bodies and agencies, and should also ensure the necessary concrete, specific and effective safeguards for each type of cooperation included in the envisaged agreement in order to ensure full compliance with the Union data protection *acquis*, with the specific safeguards and data protection requirements stipulated by the legal bases of the Union bodies, agencies and the EU large-scale IT systems, and with, fundamental rights; stresses that regarding the controlled access to the databases, the agreement should at least comply with the safeguards already provided by the Interoperability Regulations[1], the European Travel Information and Authorisation System (ETIAS) Regulation[2] legal base and Regulation (EU) 2016/794;

7. Recommends that the Commission negotiate with Interpol on requirements relating to high standards for the quality and verifiability of information in Interpol's databases and the transparency of information sources;

8. Expects special vigilance during the negotiations due to the sensitivity of personal data included in the various databases and to the fact that most third country members of Interpol do not offer an adequate level of data protection and are not party to an international agreement pursuant to Article 218 TFEU allowing for the exchange of operational personal data with the EU;

9. Calls on the Commission to introduce the necessary robust safeguards and guarantees to ensure compliance with EU data protection requirements and fundamental rights in order to authorise the ETIAS Central Unit established within Frontex and the EU Member States to access Interpol's SLTD and TDAWN databases via the ESP, and as are needed to efficiently implement the Visa Information System (VIS) Regulation[3], as later revised,

---

1 Regulation (EU) 2019/817 and Regulation (EU) 2019/818.

2 Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 (OJ L 236, 19.9.2018, p. 1).

3 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 (OJ L 218, 13.8.2008, p. 60).

authorising EU Member States to access Interpol's SLTD and TDAWN databases via the ESP when examining applications for visas or residence permits; insists that, when hits occur, no information be shared with Interpol or the owner of the data in Interpol's databases and recalls that, as provided for in the ETIAS and VIS Regulations, until this is agreed upon and practically guaranteed, the two systems will not be checking against the Interpol databases;

10. Recommends that the envisaged agreement clearly set out which EU bodies and agencies should have access rights to which specific Interpol databases, and for which of their specific tasks and purposes; considers that the envisaged agreement should not create an obligation for EU agencies to cooperate with Interpol beyond what is already set out in relevant Union law;

Data protection, processing and storage of personal data, judicial redress

11. Calls on the Commission to ensure that the agreement complies with the EU data protection *acquis* and protects individuals' fundamental rights and freedoms by ensuring a level of protection for personal data processed under this agreement that is essentially equivalent to that of EU primary and secondary law; stresses that the envisaged cooperation agreement 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, and should provide effective remedy to any violation of these rights;

12. Stresses that the agreement should guarantee that the transfer of personal data is adequate, relevant and limited to what is necessary for and proportionate to the purpose for which it is to be transferred, in line with the Union data protection *acquis*; highlights further that it should provide for the possibility to introduce any restriction on access or use, including a restriction on further transfers, or erasure at the time of transfer; stresses as well that data subjects must have their enforceable and effective rights ensured;

13. Considers it is necessary to require that the purposes for which data may be transferred should be clearly indicated in the agreement and that any further data processing incompatible with the initial purpose should be prohibited; considers that the agreement has to clearly indicate that decisions based solely on the automated processing of personal information without human involvement are not allowed;

14. Stresses that the envisaged agreement should clearly outline the procedures regarding Interpol's obligation to notify in the event of a personal data breach, and the description of the minimum information to be provided with the notification of the breach; calls on the Commission to ensure in the agreement that Interpol notifies the relevant EU agencies and Member State authorities, including national data protection authorities, in the event of a personal data breach, without undue delay and, where feasible, within 72 hours;

15. Recommends that oversight of the data consulted be done by one or more independent bodies responsible for data protection with effective powers of investigation and intervention and with the power to hear complaints from individuals about the use of their personal data;

16. Recommends that the Commission guarantee that Interpol does not retain data for longer than is necessary for the purpose for which it was transferred; expects, in this context, the

agreement to provide clear and specific rules on storage, including on storage limitation, review, rectification and deletion of personal data;

17. Calls on the Commission to ensure effective and enforceable rights to administrative and judicial redress, and effective remedy for all data subjects, meaning any person whose data is processed under this agreement;

18. Underlines that the agreement explicitly clarifies that Interpol will not have reciprocal direct or indirect access to EU databases;

Interoperability

19. Stresses that law enforcement cooperation and information sharing are important tools to combat crime and terrorism and pursue justice, but they need to be targeted and subject to appropriate and predefined safeguards and oversight; underscores that they should address fundamental rights challenges, in particular by enhancing data quality, mitigating bias, detecting errors and avoiding any form of discrimination in the decision-making process;

20. Recommends that particular attention be paid to fundamental rights challenges and the necessity of adequate mitigating measures and non-discrimination mechanisms, as well as improved data quality and protection with a view to the establishment of frameworks for future development of an enhanced connection between the EU's and Interpol's information systems in the fields of police and judicial cooperation, asylum and migration, as well as integrated borders management and visas, providing a pivotal legislative framework for current and future developments in the EU's digital infrastructure;

21. Recommends that in view of the rules governing access to personal data and information sharing in the different EU systems and databases, the terms of the future cooperation agreement with Interpol should provide the safeguards and guarantees needed to give Member States and relevant EU agencies controlled access to Interpol's databases via the ESP as required to carry out their tasks, in line with their access rights and EU or national law covering such access and in full compliance with EU data protection requirements and fundamental rights;

22. Recalls that Interpol's databases contain a large volume of data on third country nationals' travel documents, and that using these databases could minimise information gaps, increase positive matches and subsequently improve the operational results of the ETIAS and revised VIS Regulation; highlights that the cooperation agreement with Interpol should provide the required legal basis, including data protection safeguards and guarantees, and authorise the ESP to connect directly with Interpol databases; highlights that the cooperation agreement should therefore also provide scope for establishing secure ESP and the ETIAS connections with Interpol's IT infrastructure, so as to allow access to Interpol's databases;

23. Stresses that in line with the current EU framework, the new agreement should guarantee that any automated queries of Interpol's SLTD and TDAWN databases via the ESP using interoperability should be performed in such a way that no information is revealed to the state that is owner of the Interpol alert;

Transfer of data and onwards transfers

24. Recalls that according to the Union data protection *acquis*, the transfer of personal data from the EU to third countries and international organisations is allowed only if the recipients of this information are able to guarantee an essentially equivalent level of personal data protection to that of the Union; underlines, in this context, that in the absence of an adequacy decision on Interpol, the agreement should constitute the legal basis allowing the transfer of personal data to Interpol, provided that it is legally binding and enforceable against all parties to the agreement and that it includes appropriate data protection safeguards;

25. Stresses that the transfer of personal data revealing racial or ethnic origins, 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, should only be allowed in exceptional circumstances and where such transfer is necessary and proportionate in the individual case for preventing or combating criminal offences that fall within the scope of the agreement; emphasises that the agreement must provide appropriate safeguards to address the specific risks of processing special categories of data, especially for minors and victims of offences;

26. Recommends limiting the application of derogations for onward transfers of personal data to the cases provided for in Chapter V of the EUDPR; stresses that the specific requirements under the regulations establishing the concerned EU agencies or bodies must be fully respected, including the specific provisions related to the transfers of operational data by Europol and the EPPO;

27. Recommends that the agreement ensure that transfers of personal data must be subject to confidentiality obligations, and necessary and proportionate for the purposes specified in the agreement, namely prevention, investigation, detection or prosecution of criminal offences, safeguarding against threats to public security and protecting external borders;

28. Recommends that the agreement explicitly lay 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, and that personal data will not be transferred if there is any risk that the data will be used for this purpose;

Red notices and diffusions

29. Stresses, with a view to future cooperation, that despite recent reforms, transparency and accountability remain a challenge both at the individual and the organisational level in Interpol, as does a lack of available statistical information on the operation of its notices and diffusions system; calls, therefore, on the Commission, to ensure commitment and guarantees from Interpol that it will further develop the necessary structures and rules, as well as substantive tools allowing consistent and transparent processing of requests, reviews, challenges, corrections and deletions;

30. Calls on the Commission to negotiate a firm requirement that Interpol improve the transparency of its red notices and diffusions review system, in particular of the role and work of its Notices and Diffusions Task Force; calls on the Commission to use the negotiations with Interpol to request that the organisation produce, update and make available procedural and substantive tools on the legal handling of red notices and

diffusions, ensuring the consistent and transparent processing of requests, reviews, challenges, corrections and deletions;

31. Recommends, in order to improve efficiency and increase transparency, an annual publication of statistical data on the processing of red notices and diffusions, including information on the number of submissions, the country of origin, the criminal offence category, the reasons or justifications for the denials and the use of sanctions in cases of abuse; calls on the Commission to ensure that statistical data on EU Member States' handling of requests for red notice arrests and diffusions are collected for all Member States;

32. Stresses that, in the context of this agreement, Interpol should develop public risk profiles of red notices and diffusions, based on the annual statistical publication referred to in the paragraph above, which would allow for the evaluation of the risk of abuse by the requesting countries, and would contribute to evaluating the effectiveness of Interpol's enforcement mechanisms;

33. Calls on the Commission, in the context of this agreement, to explore possible ways that the ESP could address the problem of politically motivated red notices and diffusions, which in practice would be one of the tools that could prove effective against politically motivated red notice requests in some situations;

34. Recalls the Council's statement on Interpol's red notices as regards the adoption of Regulation (EU) 2022/991 of the European Parliament and of the Council[1], supporting efforts undertaken at Interpol to prevent the abuse of red notices and diffusions for political reasons or violations of human rights and calling for a continued and regular exchange on the matter between Interpol and its National Central Bureaus in order to raise further awareness of the actions that Member States should take in cooperation with Interpol;

35. Expects the Council to deliver on its commitment to continue to support Interpol in the promotion of its existing standards and procedures for data quality and compliance;

36. Calls on the Commission to also work internally, making use of existing technical tools available under the EU security framework, to establish a verification mechanism for EU Member States to exchange information on the identification and removal of politically motivated red notices and diffusions, on best practices in this field and on risk profiles of third countries creating red notices;

37. Calls on the Commission to recognise the risk of authoritarian regimes systematically undermining the trust-based international law enforcement cooperation by abusing the tools provided by Interpol; calls on the Commission to encourage Interpol to increase its efforts in effectively countering this misconduct;

38. Calls on the Commission to include provisions regarding support to Interpol in the agreement to increase the currently small number of staff dealing with the review of red notices and diffusions within the Commission for the Control of Files and to improve the

---

[1] Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation (OJ L 169, 27.6.2022, p. 1).

statistical information on the operation of red notices and diffusions; calls on the Commission to use the EU's role and influence to support improvements that will strengthen protection of notices and diffusions from misuse;

Russia

39. Notes the announcement by Interpol's Secretary-General that it would implement enhanced monitoring measures to identify and prevent any further abuse of Interpol's systems by Russia; remains concerned, however, that monitoring alone will not fully mitigate the risks of Russian abuse; stresses, therefore, that given the current special circumstances, including Russia's blatant breaches of international law and disregard for the rules-based international system, Interpol's Executive Committee and General Secretariat should take immediate and firm measures to revoke the access rights of the Russian Federation and Belarus to Interpol's systems, as their actions are a direct threat to international law enforcement cooperation and constitute a serious breach of fundamental rights; urges Interpol's Executive Committee to prepare and propose to the General Assembly the necessary amendments to the Interpol constitution to enable the suspension of member countries from Interpol and calls on the EU Member States to support this initiative with a view to suspending Russia and other countries that consistently abuse Interpol for political reasons from the organisation; urges Interpol's General Secretariat to put forward a proposal to the Executive Committee for corrective measures for the Russian Federation according to Article 131(3) of Interpol's Rules on the Processing of Data, including suspension of the access rights of the Russian National Central Bureau;

40. Strongly recommends that the Commission put forward enhanced monitoring measures, in the context of this agreement, regarding notices and diffusions issued before the war in Ukraine by Russian authorities; calls on the Commission to advise Member States on specific measures to apply as regards notices and diffusions issued by Russian authorities before the war and in the current context;

Final remarks

41. Demands that the agreement provide for the possibility of its suspension or termination in case of any breach of its provisions, notably those on personal data by one of the parties, 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 terms of the agreement;

42. Considers that the envisaged agreement should contain a clause on a review report by the Commission three years after its entry into force, and every three years thereafter, assessing the effective implementation of the agreement and its respect of fundamental rights; considers it important that the agreement provide for a monitoring mechanism and periodic reviews to evaluate its functioning in relation to the operational needs of the relevant Union agencies, including statistics on the number of criminals arrested and convicted with the help of Interpol data, as well as its compliance with data protection and other fundamental rights;

43. Recommends, as was confirmed by the CJEU, in its opinion of 8 September 2016 on the draft agreement between Canada and the European Union on the Transfer of Passenger Name Record data from the European Union to Canada, that the citations of the agreement include all the relevant substantive legal bases, including Article 16 TFEU;

44. Recommends that any dispute settlement to be negotiated fall under the ultimate jurisdiction of the CJEU;

45. Calls on the Commission to report to Parliament on the conduct and the outcome of the negotiations, both on a regular basis and whenever requested; recalls that Parliament has consenting power on the conclusion of the envisaged cooperation agreement and that it should thus be closely involved in the negotiating process; calls on the Commission to ensure that reporting to Parliament is a part of the monitoring and evaluation mechanisms foreseen in the cooperation agreement;

°

° °

46. Instructs its President to forward this recommendation to the Council, the Commission and the International Criminal Police Organization (ICPO-INTERPOL).