Wednesday 4 July 2018

P8_TA(2018)0298

Opening of negotiations for an EU-Tunisia Agreement on the exchange of personal data for fighting serious crime and terrorism

European Parliament resolution of 4 July 2018 on the Commission 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)0807 — 2018/2063(INI))

(2020/C 118/12)

The European Parliament,

— having regard to the Commission 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)0807),

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

— having regard to the Treaty on European Union, in particular Article 6 thereof, and to the Treaty on the Functioning of the European Union (TFEU), in particular Articles 16 and 218 thereof,

— 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 and 2009/968/JHA ([1]),

— 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) ([2]),

— having regard to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) ([3]),

— 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]),

— 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 ([5]),

([1]) OJ L 135, 24.5.2016, p. 53.
([2]) OJ L 119, 4.5.2016, p. 1.
([3]) OJ L 201, 31.7.2002, p. 37.
([4]) OJ L 350, 30.12.2008, p. 60.
([5]) OJ L 119, 4.5.2016, p. 89.

— having regard to the Council of Europe Convention on Data Protection (ETS No 108) and the Additional Protocol of 8 November 2001 to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows (ETS No 181),

— having regard to European Data Protection Supervisor (EDPS) Opinion 2/2018 on eight negotiating mandates to conclude international agreements allowing the exchange of data between Europol and third countries,

— having regard to its resolution of 3 October 2017 on the fight against cybercrime [1],

— having regard to the agreement reached by the European Parliament and the Council on the proposal for a regulation on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (COM(2017)0008), and in particular to the chapter on the processing of operational personal data which applies to Union bodies, offices or agencies when carrying out activities which fall within the scope of Chapters 4 and 5 of Title V of Part Three of the TFEU,

— having regard to Rule 108(1) of its Rules of Procedure,

— having regard to the report of the Committee on Civil Liberties, Justice and Home Affairs (A8-0237/2018),

A. whereas Regulation (EU) 2016/794 on the European Union Agency for Law Enforcement Cooperation (Europol) enables the transfer of personal data to an authority of a third country or to an international organisation insofar as such transfer is necessary for the performance of Europol's tasks, on the basis of an adequacy decision of the Commission pursuant to Directive (EU) 2016/680, an international agreement pursuant to Article 218 TFEU adducing adequate safeguards, or cooperation agreements allowing for the exchange of personal data concluded before 1 May 2017, and, in exceptional situations, on a case-by-case basis under strict conditions laid down in Article 25(5) of Regulation (EU) 2016/794 and provided that adequate safeguards are ensured;

B. whereas international agreements allowing Europol and third countries to cooperate and exchange personal data should respect Articles 7 and 8 of the Charter of Fundamental Rights and Article 16 TFEU, and hence respect the principle of purpose limitation and the rights of access and rectification and be subject to monitoring by an independent authority, as specifically stipulated by the Charter, and prove necessary and proportionate for the fulfilment of Europol's tasks;

C. whereas such a transfer is to be based on an international agreement concluded between the Union and that third country pursuant to Article 218 TFEU adducing adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals;

D. whereas the Europol programming document 2018-2020 [2] highlights the increasing relevance of an enhanced multi-disciplinary approach, including the pooling of necessary expertise and information from an expanding range of partners, for the delivery of Europol's mission;

E. whereas Parliament underlined in its resolution of 3 October 2017 on the fight against cybercrime that strategic and operational cooperation agreements between Europol and third countries facilitate both the exchange of information and practical cooperation in the fight against cybercrime;

---

[1] Texts adopted, P8_TA(2017)0366.

[2] Europol Programming Document 2018-2020 adopted by Europol's Management Board on 30 November 2017, EDOC# 856927v18.

Wednesday 4 July 2018

F. whereas Europol has already set up multiple agreements on data exchange with third countries in the past, such as Albania, Australia, Bosnia and Herzegovina, Canada, Colombia, the former Yugoslav Republic of Macedonia, Georgia, Iceland, Liechtenstein, Moldova, Monaco, Montenegro, Norway, Serbia, Switzerland, Ukraine and the United States of America;

G. whereas the EDPS has been the supervisor of Europol since 1 May 2017, and is also the advisor to the EU institutions on policies and legislation relating to data protection;

1. Considers that the necessity of the cooperation with Tunisia in the field of law enforcement for the European Union's security interests, as well as its proportionality, need to be properly assessed; calls on the Commission, in this context, to conduct a thorough impact assessment; highlights that due caution is needed while defining the negotiating mandate 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;

2. Considers that full consistency with Articles 7 and 8 of the Charter, as well as other fundamental rights and freedoms protected by the Charter, should be ensured in the receiving third countries; calls, in this regard, on the Council to complete the negotiating guidelines proposed by the Commission with the conditions set out in this resolution;

3. Takes note that to date no appropriate impact assessment has been conducted in order to assess in depth the risks posed by transfers of personal data to Tunisia as regards individuals' rights to privacy and data protection, but also for other fundamental rights and freedoms protected by the Charter; asks the Commission to carry out an appropriate impact assessment so as to define the necessary safeguards to be integrated in the agreement;

4. Insists that the level of protection resulting from the agreement should be essentially equivalent to the level of protection in EU law; stresses that if such level cannot be guaranteed both in law and in practice, the agreement cannot be concluded;

5. Requests that, in order to fully respect Article 8 of the Charter and Article 16 TFEU and to avoid any potential liability from Europol as regards a violation of Union data protection law resulting from a transfer of personal data without the necessary and appropriate safeguards, the agreement contain strict and specific provisions imposing respect for the principle of purpose limitation with clear conditions for the processing of personal data transmitted;

6. Calls for Guideline B to be completed to expressly indicate the agreement that Europol, pursuant to Article 19 of the Europol Regulation, is to respect any restriction imposed on personal data transmitted to Europol by Member States or other providers regarding the use and access to data to be transferred to Tunisia;

7. Requests that the agreement clearly provide that any further processing should always require prior written authorisation from Europol; stresses that these authorisations should be documented by Europol and made available to the EDPS at its request; calls for the agreement also to contain a provision obliging the competent authorities of Tunisia to respect these restrictions and specify how compliance with these restrictions would be enforced;

8. Insists that the agreement contain a clear and precise provision setting out the data retention period of personal data that have been transferred and requiring the erasure of the personal data transferred at the end of the data retention period; requests that procedural measures be set out in the agreement to ensure compliance; insists that, in exceptional cases, where there are duly justified reasons to store the data for an extended period, past the expiry of the data retention period, these reasons and the accompanying documentation be communicated to Europol and the EDPS;

9. Expects the criteria included in Recital 71 of Directive (EU) 2016/680 to be applied, i.e. transfers of personal data are to be subject to confidentiality obligations by the competent Tunisian authorities receiving personal data from Europol, the principle of specificity, and that the personal data will not be used in any case to request, hand down or execute a death penalty or any form of cruel and inhuman treatment;

10. Considers that the categories of offences for which personal data will be exchanged need to be clearly defined and listed in the international agreement itself, in line with EU criminal offences definitions when available; stresses that this list should define in a clear and precise manner the activities covered by such crimes, and the persons, groups and organisations likely to be affected by the transfer;

11. Urges the Council and the Commission to define, pursuant to Court of Justice of the European Union (CJEU) case-law and within the meaning of Article 8(3) of the Charter, with the Government of Tunisia, which independent supervisory authority is to be in charge of supervising the implementation of the international agreement; urges that such an authority should be agreed and established before the international agreement can enter into force; insists that the name of this authority be expressly included in an annex to the agreement;

12. Considers it should be possible for either of the contracting parties to suspend or revoke the international agreement should there be a breach thereof, and that the independent supervisory body should also be empowered to suggest suspending or terminating the agreement in the event of a breach thereof; considers that any 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; considers that a periodic evaluation of the agreement should be established in order to evaluate the partners' compliance with the agreement;

13. Is of the opinion that a clear definition of the concept of individual cases is needed as this concept is needed to assess the necessity and proportionality of data transfers; highlights that this definition should refer to actual criminal investigations;

14. Is of the opinion that the concept of reasonable grounds needs to be defined in order to assess the necessity and proportionality of data transfers; highlights that this definition should refer to actual criminal investigations;

15. Stresses that data transferred to a receiving authority can never be further processed by other authorities and that, to this end, an exhaustive list of the competent authorities in Tunisia to which Europol can transfer data should be drawn up, including a description of the authorities' competences; considers that any modification to such a list that would replace or add a new competent authority would require a review of the international agreement;

16. Insists on the need to expressly indicate that onward transfers of information from the competent authorities of Tunisia to other authorities in Tunisia can only be allowed to fulfil the original purpose of the transfer by Europol and should always be communicated to the independent authority, the EDPS and Europol;

17. Stresses the need to expressly indicate that onward transfers of information from the competent authorities of Tunisia to other countries are prohibited and would result in the immediate ending of the international agreement;

18. Considers that the international agreement with Tunisia should include data subjects' right to information, rectification and erasure as provided for in other Union legislation on data protection;

19. Points out that the transfer of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data or data concerning a person's health and sex life is extremely sensitive and gives rise to profound concerns given the different legal framework, societal characteristics and cultural background of Tunisia compared with the European Union; highlights the fact that criminal acts are defined differently in the Union from in Tunisia; is of the opinion that such a transfer of data should therefore only take place in very exceptional cases and with clear safeguards for the data subject and persons linked to the data subject; considers it necessary to define specific safeguards that would need to be respected by Tunisia as regards fundamental rights and freedoms, including respect for freedom of expression, freedom of religion and human dignity;

20. Believes that a monitoring mechanism should be included in the agreement and that the agreement should be subject to periodic assessments to evaluate its functioning in relation to the operational needs of Europol as well as its compliance with European data protection rights and principles;

21. Calls on the Commission to seek the advice of the EDPS before the finalisation of the international agreement in accordance with Regulation (EU) 2016/794 and Regulation (EC) No 45/2001;

22. Stresses that the Parliament's consent to the conclusion of the agreement will be conditional upon satisfactory involvement of the Parliament at all stages of the procedure in accordance with Article 218 TFEU;

23. Instructs its President to forward this resolution to the Council, the Commission and the Government of Tunisia.