



TEXTS ADOPTED

P9_TA(2020)0200

Conclusion of an EU - New Zealand agreement, under negotiation, on the exchange of personal data for fighting serious crime and terrorism

European Parliament resolution of 10 July 2020 on the European Parliament recommendation to the Council and the Commission concerning the conclusion of an agreement, under negotiation, between the European Union and New Zealand on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the New Zealand authorities competent for fighting serious crime and terrorism (COM(2019)0551 – 2020/2048(INI))

The European Parliament,

- having regard to the recommendation, by the Commission, for a Council decision authorising the opening of negotiations for an agreement between the European Union and New Zealand on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the New Zealand authorities competent for fighting serious crime and terrorism (COM(2019)0551),
- having regard to the Council Decision of 13 May 2020 authorising the opening of negotiations with New Zealand for an agreement between the European Union and New Zealand on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the New Zealand authorities competent for fighting serious crime and terrorism,
- having regard to the Charter of Fundamental Rights of the European Union (the Charter), and in particular Articles 2, 6, 7, 8 and 47 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/JHA¹,
- having regard to Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the

¹ OJ L 135, 24.5.2016, p. 53.

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/EC¹,

- 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/EC²,
 - 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 sector³,
 - 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/JHA⁴,
 - having regard to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) of 28 January 1981 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 trans-border data flows (ETS No. 181),
 - having regard to European Data Protection Supervisor (EDPS) Opinion 1/2020 on the negotiating mandate to conclude an international agreement on the exchange of personal data between Europol and New Zealand law enforcement authorities,
 - having regard to the Europol Terrorism Situation and Trend Report 2019,
 - having regard to the Christchurch Call to Action adopted by New Zealand, France, the Commission, technology companies and others to eliminate terrorist and violent extremist content online,
 - having regard to Rule 114(4) of its Rules of Procedure,
 - having regard to the report of the Committee on Civil Liberties, Justice and Home Affairs (A9-0131/2020),
- A. whereas Regulation (EU) 2016/794 enables the transfer of personal data to the competent authority of a third country or to an international organisation insofar as the 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 of the TFEU adducing adequate safeguards with respect to the protection of privacy and the fundamental rights and freedoms of

¹ OJ L 295, 21.11.2018, p. 39.

² OJ L 119, 4.5.2016, p. 1.

³ OJ L 201, 31.7.2002, p. 37.

⁴ OJ L 119, 4.5.2016, p. 89.

individuals, 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; stresses that the agreement needs to fully respect the fundamental rights and principles recognised in the Charter;

- B. whereas international agreements allowing Europol and third countries to cooperate and exchange personal data should respect the fundamental rights recognised in the Charter, in particular in Articles 2, 6, 7, 8 and 47 thereof, and in Article 16 of the TFEU, and hence respect the principle of purpose limitation and the rights of access and rectification; whereas those agreements should be subject to monitoring by an independent authority, as specifically stipulated in the Charter, and should be necessary for and proportionate to the fulfilment of Europol's tasks;
- C. whereas the Europol programming document 2020-2022¹ highlights that the full and successful implementation of the activities of the European multidisciplinary platform against criminal threats (EMPACT), in particular at the operational level, is not possible without close partnership with third countries and organisations; whereas the EU and New Zealand are close in their outlook on global security issues and pursue similar approaches in this regard;
- D. whereas Europol and the New Zealand police force have already established a framework of enhanced cooperation through a working arrangement and a memorandum of understanding, both signed in 2019, which allow the New Zealand police force to use the Secure Information Exchange Network Application (SIENA) and permanently deploy a liaison officer to Europol's headquarters in the Hague;
- E. whereas Europol has concluded multiple operational agreements on the exchange of personal data with third countries in the past; whereas in 2018, the Union launched negotiations on this matter with eight countries in the Middle East and North Africa (Turkey, Israel, Tunisia, Morocco, Lebanon, Egypt, Algeria and Jordan); and whereas Parliament has adopted resolutions on the negotiating mandates for those agreements²;
- F. whereas Europol has designated the threat level from Jihadi terrorists as high, and whereas in 2018, terrorism continued to constitute a major threat to security in the Member States; whereas although the number of arrests of right-wing terrorists remained at a comparatively low level, it did increase for the third year a row; whereas the Member States have reported to Europol that law enforcement agencies used data exchange tools to foil, disrupt or investigate 129 terrorist attacks in 2018;
- G. whereas the European Data Protection Supervisor (EDPS) has supervised Europol since 1 May 2017, and also advises the EU institutions on policies and legislation relating to data protection, including when negotiating agreements in the law enforcement sector;
- H. whereas in the light of the 2019 right-wing terrorist attack on two mosques in Christchurch, operational cooperation to be formalised under the agreement between

¹ Europol Programming Document 2020-2022 adopted by Europol's Management Board on 25 March 2020, EDOC# 1003783v20E.

² OJ C 118, 8.4.2020, p. 69.

Europol and New Zealand, by enabling the exchange of personal data, could be essential for preventing and prosecuting other serious crimes and terrorist attacks that could be planned or perpetrated within the EU or worldwide;

- I. whereas transfers of personal data gathered in the context of criminal investigations and further processed by Europol under the agreement could have a significant impact on the lives of the individuals concerned;
 1. Considers that cooperation with New Zealand in the field of law enforcement will help the European Union to further protect its security interests, especially in the areas of preventing and combating terrorism, disrupting organised crime and fighting cybercrime; encourages the Commission to expeditiously launch negotiations with New Zealand on the exchange of personal data between Europol and the New Zealand authorities competent for fighting serious crime and terrorism in full respect of the negotiating guidelines adopted by the Council; calls on the Commission to follow the additional recommendations set out in this resolution;
 2. Insists that the level of data protection provided for in the agreement should be essentially equivalent to the level of protection provided for in EU law, both in law and in practice; insists, furthermore, that if such a level of protection is not guaranteed, the agreement cannot be concluded; highlights, in this context, the formal recognition of New Zealand by the Commission in 2012 as a country providing an adequate level of data protection; whereas this decision does, however, only apply to matters falling within the scope of Regulation (EU) 2016/679 and consequently does not apply to law enforcement matters;
 3. Believes that cross-border information exchange between all relevant law enforcement agencies, within the EU and with global partners, should be prioritised in order to fight serious crime and terrorism more effectively;
 4. Requires the agreement to contain all the necessary safeguards and controls with respect to the protection of personal data set out in the negotiating directives; notes that the transfer of sensitive personal data should only be permitted in exceptional cases where such transfers are strictly necessary and proportionate for preventing and combating criminal offences covered by the agreement; stresses that clear safeguards for the data subject, persons linked to the data subject and persons linked to the criminal offence such as witnesses and victims should be defined to guarantee respect for fundamental rights;
 5. Is of the opinion that, in line with the principle of purpose limitation, the future agreement should explicitly lay down a list of criminal offences in relation to which personal data can be exchanged, in line with EU criminal offences definitions when available; considers that this list should include the activities covered by such crimes and the likely effects of the transfer of personal data;
 6. Stresses that transferred personal data should relate to individual criminal cases; points out that a clear definition of the concept of individual criminal cases should be included in the agreement, as this concept is needed to assess the necessity and proportionality of data transfers;
 7. Insists that the agreement contain a clear and precise provision setting out the retention

period for personal data that have been transferred to New Zealand and requiring the data to be erased at the end of that period; requests that procedural measures be set out in the agreement to ensure compliance; requests, in this regard, that the agreement specifically provide for periodic reviews of the retention periods and any further need to store personal data, and that it provide for other appropriate measures to ensure that the time limits are observed; insists that, in exceptional cases, where there are duly justified reasons to store data for an extended period, past the end of the data retention period, these reasons and the accompanying documentation be communicated to Europol and the EDPS;

8. Urges the Council and the Commission to work with the Government of New Zealand to define, pursuant to Court of Justice case law and within the meaning of Article 8(3) of the Charter, which independent supervisory authority vested with effective powers of investigation and intervention is to be in charge of supervising the implementation of the international agreement; requests that such an authority be agreed on and established before the international agreement can enter into force; insists that the name of this authority be expressly included in the agreement;
9. Considers that the international agreement should include a provision allowing the EU to suspend or revoke the agreement in the event of a breach; considers it important that the independent supervisory body should also have the power to decide to suspend or terminate personal data transfers in the event of a breach; considers that under the agreement, authorities should be allowed to continue to process any personal data falling within the scope of the agreement transferred prior to its suspension or termination; considers that a mechanism for monitoring and periodically evaluating the agreement should be established in order to evaluate the partners' compliance with the agreement and the functioning of the agreement in relation to the operational needs of Europol, and with the EU data protection law;
10. Considers that onward transfers of Europol information from competent New Zealand authorities to other authorities in New Zealand, including for use in judicial proceedings, should only be allowed for the original purposes of the transfer by Europol and should be made subject to prior authorisation by Europol; points out that onward transfers of Europol information from competent New Zealand authorities to third country authorities should not be allowed;
11. Calls on the Council and the Commission to consult the EDPS on the provisions of the draft agreement before its finalisation and throughout the negotiations;
12. Considers that the international agreement with New Zealand should enshrine the right of data subjects to information, rectification and erasure as provided for in other EU legislation on data protection; requests, in this regard, that the agreement include clear and detailed rules regarding information that should be provided to the data subjects;
13. Stresses that its consent for the conclusion of the agreement will be conditional on its satisfactory involvement at all stages of the procedure; expects to be kept fully and proactively informed about the progress of the negotiations in accordance with Article 218 of the TFEU and expects to receive the documents at the same time as the Council so that it can carry out its scrutiny role;
14. Stresses that it will give its consent to the conclusion of the agreement only if such an

agreement does not pose risks to the rights to privacy and data protection, nor to other fundamental rights and freedoms protected by the Charter; indicates, in this regard, that pursuant to Article 218(11) of the TFEU, it may obtain the opinion of the Court of Justice as to whether the agreement envisaged is compatible with the Treaties;

15. Instructs its President to forward this resolution to the Council and the Commission and the Government of New Zealand.