



Brussels, 30.10.2019
COM(2019) 551 final

ANNEX

ANNEX

to the

Recommendation 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

ANNEX

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

- (1) The objective of the Agreement should be to provide the legal basis for the transfer of personal data between Europol and the competent authorities of New Zealand respectively, in order to support and strengthen the action by the competent authorities of this country and Member States as well as their mutual cooperation in preventing and combatting serious transnational crime and terrorism, while ensuring appropriate safeguards with respect to the protection of privacy, personal data and fundamental rights and freedoms of individuals;
- (2) To guarantee purpose limitation, cooperation and exchange of data under the Agreement should only relate to crimes and related criminal offences falling within Europol's competence in accordance with Article 3 of Regulation 2016/794 (together "criminal offences"). In particular, cooperation should be aimed at preventing and combating terrorism, disrupting organised crime and fighting cybercrime. The Agreement should specify its scope and the purposes for which Europol may transfer personal data to the competent authorities of New Zealand;
- (3) The Agreement should spell out clearly and precisely the necessary safeguards and controls with respect to the protection of personal data, fundamental rights and freedoms of individuals, irrespective of nationality and place of residence, in the exchange of personal data between Europol and the New Zealand competent authorities. In addition to the safeguards set out below, these should include requiring that the transfer of personal data will be subject to confidentiality obligations and 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, without prejudice to additional safeguards that may be required.

In particular:

- (a) The Agreement should contain definitions of key terms. In particular, the Agreement should contain a definition of personal data compliant with Article 3(1) of Directive (EU) 2016/680;
- (b) The Agreement should respect the principle of specificity, ensuring that the data will not be processed for other purposes than for the purposes of the transfer. To this end, the purposes of the processing of personal data by the Parties in the context of the Agreement should be spelt out clearly and precisely, and should 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;
- (c) Personal data transferred by Europol in accordance with the Agreement should be processed fairly, on a legitimate basis and only for the purposes for which they have been transferred. The Agreement should provide the obligation for Europol to indicate, at the moment of transferring the data, any restriction on access or use, including as regards its transfer, erasure, destruction or further processing. The Agreement should oblige competent authorities of New Zealand to respect these restrictions and specify how compliance with these restrictions will be enforced in practice. Personal data should be adequate, relevant and limited to what is necessary in relation to that purpose. It should be accurate and kept up to date. It should not be retained for longer than is necessary for the purposes for which they have been transferred. The Agreement should be accompanied by an annex containing an

exhaustive list of the competent authorities in New Zealand to which Europol may transfer personal data as well as a short description of their competences;

- (d) The transfer of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic data and data concerning a person's health and sex life by Europol should be prohibited, unless it is strictly necessary and proportionate in individual cases for preventing or combating criminal offences as referred to in the Agreement and subject to appropriate safeguards. The Agreement should also contain specific safeguards relating to the transfer of personal data on victims of criminal offences, witnesses or other persons who can provide information concerning criminal offences, as well as minors;
- (e) The Agreement should 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 Agreement should also ensure enforceable rights of administrative and judicial redress for any person whose data are processed under the agreement and guaranteeing effective remedies;
- (f) The Agreement should lay down the rules on storage, review, correction and deletion of personal data as well as on keeping records for the purposes of logging and documentation as well as on information to be made available to individuals. It should also provide for safeguards in respect to automated processing of personal data;
- (g) The Agreement should specify the criteria on the basis of which the reliability of the source and accuracy of the data should be assessed;
- (h) The Agreement should 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. The Agreement should also include the obligation of notification in the event of a personal data breach affecting data transferred under the Agreement;
- (i) Onward transfers of information from competent authorities of New Zealand 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 appropriate conditions and safeguards, including prior authorisation by Europol;
- (j) The same conditions as under (i) should apply to onward transfers of information from competent authorities of New Zealand to authorities in a third country, with the additional requirement that such onward transfers should be allowed only with respect to third countries to which Europol is entitled to transfer personal data on the basis of Article 25(1) of Regulation (EU) 2016/794;
- (k) The Agreement should 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 over those public authorities of New Zealand that use personal data/exchanged information, and to engage in legal proceedings. In particular, the independent authorities should have powers to hear complaints from individuals about the use of their personal data. Public authorities that use personal data should be accountable for complying with the rules on the protection of personal data under the Agreement;

- (4) The Agreement should provide for an effective dispute settlement mechanism with respect to its interpretation and application to ensure that the parties observe mutually agreed rules.;
- (5) The Agreement should include provisions on the monitoring and periodic evaluation of the Agreement;
- (6) The Agreement should include a provision on the entry into force and validity and a provision whereby a Party may terminate or suspend it, in particular where the third country no longer effectively ensures the level of protection of fundamental rights and freedoms required under this Agreement. The Agreement should also specify whether personal data falling within its scope and transferred prior to its suspension or termination may continue to be processed. Continued processing of personal data, if permitted, should in any case be in accordance with the provisions of the Agreement at the time of suspension or termination;
- (7) The Agreement may include a clause addressing its territorial application, if necessary;
- (8) The Agreement should be equally authentic in the Bulgarian, Czech, Croatian, Danish, Dutch, English, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Latvian, Lithuanian, Maltese, Polish, Portuguese, Romanian, Slovak, Slovenian, Spanish and Swedish languages and should include a language clause to that effect.