EUROPEAN
COMMISSION

Brussels, 13.5.2022
COM(2022) 208 final

ANNEX

ANNEX

to the

Proposal for a

COUNCIL DECISION

on the conclusion of the Agreement between the European Union, of the one part, and New Zealand, of the other part, on the exchange of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the authorities of New Zealand competent for fighting serious crime and terrorism

ANNEX

THE EUROPEAN UNION, hereinafter also referred to as ‘the Union’ or ‘EU’,

and

New Zealand,

hereinafter referred to as ‘the Contracting Parties’,

Whereas:

(1) By allowing the exchange of personal data between Europol and the New Zealand competent authorities, this agreement will create the framework for an enhanced operational cooperation between the European Union and New Zealand in the field of law enforcement, while safeguarding the human rights and fundamental freedoms of all individuals concerned, including privacy and data protection.

(2) This agreement is without prejudice to Mutual Legal Assistance arrangements between New Zealand and the EU Member States allowing for the exchange of personal data.

(3) This agreement does not impose any requirement on the competent authorities to transfer personal data. The sharing of any personal data requested under this agreement remains voluntary.

(4) The agreement recognises that the Parties apply comparable principles of proportionality and reasonableness. The common essence of these principles is the requirement of ensuring a fair balance between all the interests concerned, whether public or private, in the light of all the circumstances of the case at hand. Such balancing involves, on the one hand, the privacy rights of individuals together with other human rights and interests and, on the other hand, the countervailing legitimate objectives that may be pursued, such as the purposes of processing personal data reflected in this Agreement.

Have agreed as follows:

CHAPTER I – GENERAL PROVISIONS

Article 1
Objective

The objective of this Agreement is to allow the transfer of personal data between the European Union Agency for Law Enforcement Cooperation (Europol) and the competent authorities of New Zealand, in order to support and strengthen the action by the authorities of the Member States of the European Union and those of New Zealand, as well as their mutual cooperation in preventing and fighting criminal offences, including serious crime and terrorism, while ensuring appropriate safeguards with respect to the human rights and fundamental freedoms of individuals, including privacy and data protection.

Article 2
Definitions

For the purpose of this Agreement:

(a). 'Contracting Parties' means, on the one hand, the European Union, and, on the other hand, New Zealand;

(b). 'Europol' is the European Union Agency for Law Enforcement Cooperation, set up under Regulation (EU) 2016/794[1] or any amendment thereto" ('Europol Regulation')";

(c). 'Competent authority' means, for New Zealand, the domestic law enforcement authorities responsible under New Zealand national law for preventing and combatting criminal offences as listed in Annex II to this Agreement ('competent authorities of New Zealand'), and for the European Union, Europol;

(d). 'Union bodies' means institutions, bodies, missions, offices and agencies set up by, or on the basis of the Treaty on European Union and the Treaty on the Functioning of European Union, listed in Annex III;

(e). 'Criminal offences' are the types of crime listed in Annex I and related criminal offences. Criminal offences are considered related to the types of crime listed in Annex I if they are committed in order to procure the means of perpetrating, to facilitate or perpetrate, or to ensure the impunity of those committing such types of crime;

(f). 'Personal data' means any information relating to a data subject;

(g). 'Data subject' means an identified or identifiable natural person, an identifiable person being a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

[1] Regulation (EU) 2016/794 means 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; OJ L135, 24.5.2016, p. 53.

(h). 'Genetic data' means all personal data relating to the genetic characteristics of an individual that have been inherited or acquired, which give unique information about the physiology or the health of that individual, resulting in particular from an analysis of a biological sample from the individual in question;

(i). 'Processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(j). 'Information' means personal data;

(k). 'Personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

(l). 'Supervisory authority' means one or more domestic independent authorities that are, alone or cumulatively, responsible for data protection within the meaning of Article 16 of this Agreement, and which have been notified according to that Article; this may include authorities whose responsibility also covers other human rights.

(m). 'International organisation' means an organisation and its subordinate bodies governed by public international law, or any other body, which is set up by, or on the basis of, an agreement between two or more countries.

Article 3
Purposes of processing personal data

1. Personal data requested and received by under the Agreement shall be processed only for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, within the limits of Article 4(5) and the respective mandates of the competent authorities.

2. The competent authorities shall clearly indicate, at the latest at the moment of transferring personal data, the specific purpose or purposes for which the data are being transferred. For transfers to Europol, the purpose or purposes for such transfer shall be specified in line with the specific purposes of processing set out in Europol's mandate.

CHAPTER II - INFORMATION EXCHANGE AND DATA PROTECTION

Article 4
General data protection principles

1. Each Contracting Party shall provide for personal data exchanged under this Agreement to be:

   (a) Processed fairly, lawfully and only for the purpose for which they have been transferred in accordance with Article 3;

(b) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(c) Accurate and kept up to date; each Contracting Party shall provide that its competent authorities take every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without undue delay;

(d) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

(e) Processed in a manner that ensures appropriate security of the personal data.

2. The transferring competent authority may indicate, at the moment of transferring personal data, any restriction on access thereto or the use to be made thereof, in general or specific terms, including as regards its onward transfer, erasure or destruction after a certain period of time, or the further processing of it. Where the need for such restrictions becomes apparent after the information has been provided, the transferring competent authority shall inform the receiving authority accordingly.

3. Each Contracting Party shall ensure that the receiving competent authority complies with any restriction on access or further use of the personal data indicated by the transferring competent authority as described in paragraph 2.

4. Each Contracting Party shall provide that its competent authorities implement appropriate technical and organisational measures in such a way as to be able to demonstrate that the data processing will comply with this Agreement and the rights of the data subjects concerned are protected.

5. Each Contracting Party shall ensure that its competent authorities do not transfer personal data which have been obtained in a manifest violation of human rights recognised by the norms of international law binding on the Contracting Parties. Each Contracting Party shall ensure that the personal data received are not used to request, hand down or execute a death penalty or any form of cruel or inhuman treatment.

6. Each Contracting Party shall ensure that a record is kept of all transfers of personal data under this Agreement and of the purpose or purposes for such transfers.

Article 5
Special categories of personal data and different categories of data subjects

1. The transfer of personal data in respect of victims of a criminal offence, witnesses or other persons who can provide information concerning criminal offences, or in respect of persons under the age of 18, shall be prohibited unless such transfer is strictly necessary as well as reasonable and proportionate in individual cases for preventing or fighting a criminal offence.

2. The transfer of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, or data concerning health, or data concerning a natural person's sex life or sexual orientation shall be

allowed only where strictly necessary as well as reasonable and proportionate in individual cases for preventing or fighting a criminal offence, and if those data, except biometric data, supplement other personal data.

3. The Contracting Parties shall ensure that the processing of personal data under paragraphs 1 and 2 is subject to appropriate safeguards guarding against the specific risks involved, including restrictions on access, additional security measures within the meaning of Article 15 and limitations on onward transfers under Article 7.

Article 6
Automated processing of personal data

Decisions based solely on automated processing of the personal data exchanged, including profiling, without human intervention, which may produce an adverse legal effect on the data subject or significantly affect him or her, shall be prohibited, unless authorised in law for preventing or fighting a criminal offence and with appropriate safeguards for the rights and freedoms of the data subject, including at least the right to obtain human intervention.

Article 7
Onward transfer of the personal data received

1. New Zealand shall ensure that its competent authorities only transfer personal data received under this Agreement to other authorities in New Zealand if:

   (a) Europol has given its prior explicit authorisation;

   (b) The purpose of the onward transfer is the same as the original purpose of the transfer by Europol, or, within the limits of Article 3(1), is directly related to that original purpose; and

   (c) The onward transfer is subject to the same conditions and safeguards as those applying to the original transfer.

2. Without prejudice to Article 4(2), no prior authorisation is required when the receiving authority is itself a competent authority of New Zealand. The same applies to the ability for Europol to share personal data with authorities responsible in the Member States of the European Union for preventing and fighting criminal offences and Union bodies as listed in Annex III.

3. New Zealand shall ensure that onward transfers of personal data received by its competent authorities under this Agreement to the authorities of a third country or to an international organisation are prohibited, unless the following conditions are fulfilled:

   (a) The transfer concerns personal data other than that covered by Article 5 of the agreement;

   (b) Europol has given its prior explicit authorisation;

   (c) The purpose of the onward transfer is the same as the original purpose of the transfer by Europol, and;

(d) The onward transfer is subject to the same conditions and safeguards as those applying to the original transfer.

4. Europol may only grant its authorisation under subparagraph 3b for an onward transfer to the authority of a third country or to an international organisation if and insofar as an adequacy decision, an international agreement providing appropriate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals, a cooperation agreement or any other future legal ground for transfers of personal data within the meaning of the Europol Regulation covering the onward transfer is in place.

5. The European Union shall ensure that onward transfers of personal data received by Europol under this Agreement to the European Union bodies not listed in Annex III, to the authorities of third countries or to an international organisation are prohibited, unless:

(a) The transfer concerns personal data other than that covered by Article 5 of the agreement;

(b) New Zealand has given its prior explicit authorisation;

(c) The purpose of the onward transfer is the same as the original purpose of the transfer by New Zealand, and;

(d) An adequacy decision, an international agreement providing appropriate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals or a cooperation agreement within the meaning of the Europol Regulation is in place with that third country or international organisation.

Article 8
Assessment of reliability of the source and accuracy of information

1. The competent authorities shall indicate as far as possible, at latest at the moment of transferring the information, the reliability of the source of the information on the basis of one or more of the following criteria:

(1) Where there is no doubt of the authenticity, trustworthiness and competence of the source, or if the information is supplied by a source who, in the past, has proved to be reliable in all instances;

(2) Where the information is provided by a source from whom information received has in most instances proved to be reliable;

(3) Where the information is provided by a source from whom information received has in most instances proved to be unreliable;

(4) Where the reliability of the source cannot be assessed.

2. The competent authorities shall indicate as far as possible, at the latest at the moment of transferring the information, the accuracy of the information on the basis of one or more of the following criteria:

(1) Information of which the accuracy is not in doubt at the time of transfer;

(2) Information known personally to the source but not known personally to the official passing it on;

(3) Information not known personally to the source but corroborated by other information already recorded;

(4) Information which is not known personally to the source and cannot be corroborated.

3. Where the receiving competent authority, on the basis of information already in its possession, comes to the conclusion that the assessment of information or of its source supplied by the transferring competent authority in accordance with paragraphs 1 and 2 needs correction, it shall inform that authority and shall attempt to agree on an amendment to the assessment. The receiving competent authority shall not change the assessment of information received or of its source without such agreement.

4. If a competent authority receives information without an assessment, it shall attempt as far as possible and where possible in agreement with the transferring competent authority to assess the reliability of the source or the accuracy of the information on the basis of information already in its possession.

5. If no reliable assessment can be made, the information shall be evaluated in accordance with paragraph 1(4) and paragraph 2(4) above.

DATA SUBJECT RIGHTS

Article 9
Right of access

1. The Contracting Parties shall ensure the data subject has the right, at reasonable intervals, to obtain information on whether personal data relating to him or her are processed under this Agreement, and when that is the case, access to at least the following information:

(a) Confirmation as to whether or not data related to him or her have been processed;

(b) Information on at least the purposes of the processing operation, the categories of data concerned, and where applicable the recipients or categories of recipients to whom the data are disclosed;

(c) The existence of the right to request from the competent authority rectification/correction or erasure/deletion of personal data or restriction of processing of personal data concerning the data subject;

(d) An indication of the legal ground for processing the data;

(e) Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(f) Communication in an intelligible form of the personal data undergoing processing and of any available information as to its sources.

2. In cases where the right of access is exercised, the transferring Party will be consulted on a non-binding base before a final decision on the request is taken.

3. The Contracting Parties may provide for the provision of information in response to any request under paragraph 1 to be delayed, refused or restricted if and as long as such delay, refusal or restriction constitutes a measure that is necessary as well as reasonable and proportionate taking into account the fundamental rights and interests of the data subject, in order to:

(a) Ensure that any criminal investigation and prosecution will not be jeopardised; or

(b) Protect the rights and freedoms of third parties, or

(c) Protect national security and public order or prevent crime.

4. The Contracting Parties shall ensure the competent authority informs the data subject in writing of any delay, refusal or restriction of access and of the reasons therefor. Such reasons may be omitted if and as long as this would undermine the purpose of the delay, refusal or restriction under paragraph 3. The competent authority shall inform the data subject of the possibility of lodging a complaint with the respective supervisory authorities and of other available redress provided for in their respective legal frameworks.

Article 10
Right to rectification/correction, erasure/deletion and restriction

1. The Contracting Parties shall ensure the data subject has the right to request the competent authorities to correct/rectify inaccurate personal data concerning the data subject transferred under this Agreement. Taking into account the purposes of the processing, this includes the right to have incomplete personal data transferred under the Agreement completed.

2. Rectification/correction shall include erasure/deletion of personal data that are no longer required for the purpose(s) for which they are processed.

3. The Contracting Parties may provide for the restriction of processing rather than the erasure/deletion of personal data as referred to in paragraph 2 if there are reasonable grounds to believe that erasure/deletion could affect the legitimate interests of the data subject.

4. The competent authorities shall inform each other of measures taken pursuant to paragraphs 1, 2 and 3. The receiving competent authority shall rectify/correct, erase or restrict the processing of such data in accordance with the action taken by the transferring competent authority.

5. The Contracting Parties shall provide for the competent authority having received the request to inform the data subject in writing without undue delay, and in any case within three months of receipt of a request in accordance with paragraph 1 or 2, that

data concerning the data subject have been rectified/corrected, erased/deleted or processing restricted.

6. The Contracting Parties shall ensure for the competent authority having received the request to inform the data subject in writing, without undue delay and in any case within three months of receipt of a request of any refusal of rectification/correction, erasure/deletion or restriction of processing, of the reasons for such a refusal and of the possibility of lodging a complaint with the respective supervisory authorities and other available redress provided for in their respective legal frameworks.

Article 11
Notification of a personal data breach to the authorities concerned

1. The Contracting Parties shall ensure, in the event of a personal data breach affecting personal data transferred under this Agreement, that the respective competent authorities notify each other as well as their respective supervisory authority of that breach without delay, and to take measures to mitigate its possible adverse effects.

2. The notification shall at least:

   (a) Describe the nature of the personal data breach including, where possible, the categories and number of data subjects concerned and the categories and number of personal data records concerned;

   (b) Describe the likely consequences of the personal data breach;

   (c) Describe the measures taken or proposed to be taken by the competent authority to address the personal data breach, including the measures taken to mitigate its possible adverse effects.

3. To the extent that it is not possible to provide all the required information at the same time, it may be provided in phases. Outstanding information shall be provided without undue further delay.

4. The Contracting Parties shall ensure their respective competent authorities document any personal data breaches affecting personal data transferred under this Agreement, including the facts surrounding the breach, its effects and the remedial action taken, thereby enabling their respective supervisory authority to verify compliance with applicable legal requirements.

Article 12
Communication of a personal data breach to the data subject

1. The Contracting Parties shall, where a personal data breach as referred to in Article 11 is likely to have a serious adverse effect upon the rights and freedoms of the data subject, provide for their respective competent authorities to communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject pursuant to paragraph 1 shall describe, where possible, the nature of the personal data breach, recommend measures to mitigate the possible adverse effects of the personal data breach, and provide the name and contact details of the contact point where more information can be obtained.

3. The communication to the data subject referred to in paragraph 1 shall not be required if:

(a) The personal data concerned by the breach were subject to appropriate technological protection measures that render the data unintelligible to any person who is not authorised to have access;

(b) Subsequent measures have been taken which ensure that the data subject's rights and freedoms are no longer likely to be severely affected; or

(c) Such communication would involve disproportionate effort, in particular owing to the number of cases involved. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. The communication to the data subject may be delayed, restricted or omitted where such communication would be likely to:

(a) Obstruct official or legal inquiries, investigations or procedures;

(b) Prejudice the prevention, detection, investigation and prosecution of criminal offences or the execution of criminal penalties, public order or national security;

(c) Affect the rights and freedoms of third parties;

where this constitutes a necessary as well as reasonable and proportionate measure with due regard for the legitimate interests of the data subject concerned.

Article 13
Storage, review, correction and deletion of personal data

1. The Contracting Parties shall provide for appropriate time limits to be established for the storage of personal data received under this Agreement or for a periodic review of the need for the storage of such data, so that data are stored only as long as is necessary for the purpose for which they are transferred.

2. In any case, the need for continued storage shall be reviewed no later than three years after the personal data has been transferred, and if no justified and documented decision is taken on the continued storage of personal data, that data shall be erased automatically after three years.

3. Where a competent authority has reason to believe that personal data previously transferred by it are incorrect, inaccurate, no longer up to date or should not have been transferred, it shall inform the receiving competent authority, which shall correct or delete the personal data, and provide notification thereof to the transferring authority.

4. Where a competent authority has reason to believe that personal data previously received by it are incorrect, inaccurate, no longer up to date or should not have been transferred, it shall inform the transferring competent authority, which shall provide its position on the matter. Where the transferring competent authority concludes that

the personal data are incorrect, inaccurate, no longer up to date or should not have been transferred, it shall inform the receiving competent authority, which shall correct or delete the personal data, and provide notification thereof to the transferring authority.

Article 14
Logging and Documentation

The Contracting Parties shall provide for the keeping of logs of the collection, alteration, access, disclosure including onward transfers, combination and erasure of personal data.

Such logs or documentation shall be made available to the respective supervisory authority upon request for the purpose of verification of the lawfulness of data processing, self-monitoring and ensuring proper data integrity and security.

Article 15
Data security

The Contracting Parties shall ensure the implementation of technical and organisational measures to protect personal data exchanged under this Agreement.

In respect of automated data processing, the Contracting Parties shall ensure the implementation of measures designed to:

(a). Deny unauthorised persons access to data processing equipment used for processing personal data (equipment access control);

(b). Prevent the unauthorised reading, copying, modification or removal of data media (data media control);

(c). Prevent the unauthorised input of personal data and the unauthorised inspection, modification or deletion of stored personal data (storage control);

(d). Prevent the use of automated data processing systems by unauthorised persons using data- communication equipment (user control);

(e). Ensure that persons authorised to use an automated data processing system have access only to the personal data covered by their access authorisation (data access control);

(f). Ensure that it is possible to verify and establish to which bodies personal data may be or have been transmitted using data communication equipment (communication control);

(g). Ensure that it is possible to verify and establish which personal data have been input into automated data processing systems and when and by whom the personal data were input (input control);

(h). Ensure that it is possible to verify and establish what data have been accessed by which member of personnel and at what time (access log);

(i). Prevent the unauthorised reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media (transport control);

(j). Ensure that installed systems may, in the event of interruption, be restored immediately (recovery);

(k). Ensure that the functions of the system perform without fault, that the appearance of faults in the functions is immediately reported (reliability) and that stored personal data cannot be corrupted by system malfunctions (integrity).

Article 16
Supervisory authority

1. Each Contracting Party shall ensure that there is an independent public authority responsible for data protection (supervisory authority) to oversee matters affecting the privacy of individuals, including the domestic rules relevant under this Agreement, in order to protect the fundamental rights and freedoms of natural persons in relation to the processing of personal data. The Contracting Parties will notify each other of the authority that each of them considers as the supervisory authority within the meaning of this Article.

2. The Contracting Parties shall ensure that the supervisory authority acts with complete independence in performing its tasks and exercising its powers. It shall act free from external influence and neither seek nor accept instructions. Its members shall have a secure term of office, including safeguards against arbitrary removal.

3. The Contracting Parties shall ensure that each supervisory authority has the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers.

4. The Contracting Parties shall ensure that each supervisory authority has effective powers of investigation and intervention to exercise oversight over the bodies it supervises, and to engage in legal proceedings.

5. The Contracting Parties shall ensure that each supervisory authority has powers to hear complaints from individuals about the use of their personal data by the competent authorities under its supervision.

Article 17
Administrative and Judicial redress

Data subjects shall have the right to effective administrative and judicial redress for violations of the rights and safeguards recognised in this Agreement resulting from the processing of their personal data. The Contracting Parties will notify each other of the domestic legislation that each of them considers as providing for the rights guaranteed under this Article.

CHAPTER III - DISPUTES

Article 18
Settlement of disputes

All disputes which may emerge in connection with the interpretation, application or implementation of this Agreement and any matters related thereto shall give rise to consultations and negotiations between representatives of the Contracting Parties with a view to reaching a mutually agreeable solution.

Article 19
Suspension clause

1. In the event of a material breach or of non-fulfilment of obligations stemming from the provisions of this Agreement, either Contracting Party may suspend this Agreement temporarily in whole or in part by written notification to the other Contracting Party through diplomatic channels. Such written notification shall not be made until after the Contracting Parties have engaged in a reasonable period of consultation without reaching a resolution and suspension shall take effect twenty days from the date of receipt of such notification. Such suspension may be lifted by the suspending Contracting Party upon written notification to the other Contracting Party. The suspension shall be lifted immediately upon receipt of such notification.

2. Notwithstanding any suspension of this Agreement, personal data falling within the scope of this Agreement and transferred prior to its suspension shall continue to be processed in accordance with the provisions of this Agreement.

Article 20
Termination of the Agreement

1. This Agreement may be terminated at any time by either of the Contracting Parties by written notification through diplomatic channels, with three months' notice.

2. Personal data falling within the scope of this Agreement and transferred prior to its termination shall continue to be processed in accordance with the provisions of this Agreement at the time of termination.

3. In case of termination, the Contracting Parties shall reach agreement on the continued use and storage of the information that has already been communicated between them.

CHAPTER IV - FINAL PROVISIONS

Article 21
Relation to other international instruments

1. This Agreement shall not prejudice or otherwise affect or impact the legal provisions with regard to the exchange of information foreseen by any Mutual Legal Assistance Treaty, any other cooperation agreement or arrangement, or working law enforcement relationship for the exchange of information between New Zealand and any Member State of the European Union.

2. This Agreement shall complement the Working Arrangement establishing cooperative relations between New Zealand Police and the European Union Agency for Law Enforcement Cooperation.

Article 22
Implementing Administrative Arrangement

The details of cooperation between the Contracting Parties as appropriate to implement this Agreement shall be the subject of an implementing administrative arrangement concluded between Europol and the competent authorities of New Zealand, in accordance with the Europol Regulation.

Article 23
Administrative Arrangement on Confidentiality

The exchange of EU classified information, if necessary under this Agreement, shall be regulated by an Administrative Arrangement on Confidentiality concluded between Europol and the competent authorities of New Zealand.

Article 24
National contact point and Liaison officers

1. New Zealand shall designate a national contact point to act as the central point of contact between Europol and competent authorities of New Zealand. The specific tasks of the national contact point shall be listed in the implementing administrative arrangement under Article 22(1). The designated national contact point for New Zealand is indicated in Annex IV.

2. Europol and New Zealand shall enhance their cooperation as laid down in this Agreement through the deployment of liaison officer(s) by New Zealand. Europol may deploy one or more liaison officer(s) to New Zealand.

Article 25
Expenses

The Contracting Parties shall ensure that the competent authorities bear their own expenses, which arise in the course of implementation of this Agreement, unless otherwise stipulated in this Agreement or in the administrative arrangement.

Article 26
Notification of implementation

1. Each Contracting Party shall provide for its competent authorities to make publicly available a document setting out in an intelligible form the provisions regarding the processing of personal data transferred under this Agreement including the means available for the exercise of the rights of data subjects. Each Contracting Party shall ensure that a copy of that document be notified to the other Contracting Party.

2. Where not already in place, the competent authorities shall adopt rules specifying how compliance with the provisions regarding the processing of personal data will be enforced in practice. A copy of these rules shall be notified to the other Contracting Party and the respective supervisory authorities.

Article 27
Entry into force and application

1. This Agreement shall be approved by the Contracting Parties in accordance with their own procedures.

2. This Agreement shall enter into force on the date of the receipt of the last written notification by which the Contracting Parties have notified each other through diplomatic channels that the procedures referred to in paragraph 1 have been completed.

3. This Agreement shall enter into application on the first day after the date when all of the following conditions have been fulfilled:

   (a) The implementing administrative arrangement as laid down in Article 22 has become applicable; and

   (b) The Contracting Parties have notified one another that the obligations laid down in this Agreement have been implemented, including as laid down in Article 26, and that notification has been accepted.

4. The Contracting Parties shall exchange written notifications confirming the fulfilment of the above conditions through diplomatic channels.

Article 28
Amendments and supplements

1. This Agreement may be amended in writing, at any time by mutual consent between the Contracting Parties by written notification exchanged through diplomatic channels. The amendments shall enter into force in accordance with the same legal procedure prescribed under paragraphs 1 and 2 of Article 27.

2. The Annexes to this Agreement may be updated, as necessary, by exchange of diplomatic notes. Such updates shall enter into force in accordance with paragraphs 1 and 2 of Article 27.

3. The Contracting Parties shall enter into consultations with respect to the amendment of this Agreement or its Annexes at the request of either Party.

Article 29
Review and Evaluation

1. The Contracting Parties shall jointly review the implementation of this Agreement one year after its entry into force, and at regular intervals thereafter, and additionally if requested by either Party and jointly decided.

2. The Contracting Parties shall jointly evaluate this Agreement four years after its entry into application.

3. The Contracting Parties shall decide in advance on the modalities of the review of the implementation of the Agreement and shall communicate to each other the composition of their respective teams. The teams shall include relevant experts on

data protection and law enforcement. Subject to applicable laws, any participants in a review shall be required to respect the confidentiality of the discussions and have appropriate security clearances. For the purposes of any review, the New Zealand and the European Union shall ensure access to relevant documentation, systems and personnel.

Article 30
Territorial applicability

1. This Agreement shall apply to the territory in which and in so far as the Treaty on European Union and the Treaty on the Functioning of the European Union are applicable and to the territory of New Zealand.

2. This Agreement will only apply to the territory of Denmark or Ireland if the European Union notifies New Zealand in writing that Denmark or Ireland has chosen to be bound by this Agreement.

3. If the European Union notifies New Zealand before the entry into application of this Agreement that it will apply to the territory of Denmark or Ireland, this Agreement shall apply to the territory of such Member State on the same day that this Agreement applies to the other Member States of the European Union.

4. If the European Union notifies New Zealand after the entry into force of this Agreement, that it applies to the territory of Denmark or Ireland, this Agreement shall apply to the territory of such Member State 30 days following the date of the notification.

Done at , on the in duplicate 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, each text being equally authentic.

For **New Zealand** For **the EU**

ANNEX I – AREAS OF CRIME

Criminal offences as defined in Article 2(e) are:

– terrorism,

– organised crime,

– drug trafficking,

– money-laundering activities,

– crime connected with nuclear and radioactive substances,

– immigrant smuggling,

– trafficking in human beings,

– motor vehicle crime,

– murder, grievous bodily injury,

– illicit trade in human organs and tissue,

– kidnapping, illegal restraint and hostage taking,

– racism and xenophobia,

– robbery and aggravated theft,

– illicit trafficking in cultural goods, including antiquities and works of art,

– swindling and fraud,

– Crime against the financial interests of the Union

– Insider dealing and financial market manipulation

– racketeering and extortion,

– counterfeiting and product piracy,

– forgery of administrative documents and trafficking therein,

– forgery of money and means of payment,

– computer crime,

– corruption,

– illicit trafficking in arms, ammunition and explosives,

– illicit trafficking in endangered animal species,

– illicit trafficking in endangered plant species and varieties,

– environmental crime, including ship-source pollution,

– illicit trafficking in hormonal substances and other growth promoters,

– sexual abuse and sexual exploitation, including child abuse material and solicitation of children for sexual purposes,

– genocide, crimes against humanity and war crimes.

The forms of crime referred to in this Annex shall be assessed by the competent authorities of New Zealand in accordance with the law of New Zealand.

ANNEX II – COMPETENT AUTHORITIES OF NEW ZEALAND AND THEIR COMPETENCES

The competent authorities of New Zealand to which Europol may transfer data are as follows:

Authority
New Zealand Police (as principal competent authority)
New Zealand Customs Service
New Zealand Immigration Service

ANNEX III – LIST OF UNION BODIES

Common Security and Defence Missions/Operations, limited to law enforcement activities

European Anti-Fraud Office (OLAF)

European Border and Coast Guard Agency (Frontex)

European Central Bank (ECB)

European Public Prosecutor's Office (EPPO)

European Union Agency for Criminal Justice Cooperation (Eurojust)

European Union Intellectual Property Office (EUIPO)

ANNEX IV – NATIONAL CONTACT POINT

The national contact point for New Zealand to act as the central point of contact between Europol and competent authorities of New Zealand is hereby designated as

New Zealand Police

New Zealand will have the duty to inform Europol in case the Contact point changes.