

Privacy Commissioner's Submission to the Justice Select Committee on the International treaty examination between New Zealand and the European Union on the Exchange of Personal Data between Europol and the Authorities of NZ Competent for Fighting Serious Crime and Terrorism

Introduction

1. Thank you for the opportunity to provide a submission on the public consultation on the examination of the Agreement Between New Zealand, of the one part, and the European Union, 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 (herein referred as the Agreement), specifically on the national interest analysis.
2. The Agreement would enable the lawful transfer of personal data between Europol and domestic law enforcement authorities in New Zealand, namely, Police, Customs and Immigration as "competent authorities" under the Agreement. This would be allowed for the purpose of preventing and fighting criminal offending while taking into account the required privacy and human rights safeguards.
3. The Privacy Act 2020 (the Act) is New Zealand's primary source of privacy law and governs the collection, use, storage, and disclosure of personal information. It also provides a statutory mandate under section 17 for my Office to examine wider developments or actions that may affect individuals' privacy.
4. The European Commission formally ruled in December 2012 that New Zealand's privacy law provided an 'adequate level' of privacy protection to meet European standards. This adequacy status means that personal data information can legally be sent here from Europe for processing without special additional measures being taken by the European companies and enables this Agreement.¹

Consistency with the Privacy Act 2020 and appropriate privacy safeguards

5. My office has been consulted as part of the development of the Agreement.
6. I am of the view that the provisions of the Agreement are consistent with the expectations of the Act, in that it contains a privacy framework that reflects the requirements of the Information Privacy Principles (IPPs) of the Act. Although the Agreement is not directly enforceable,² the Agreement expresses a commitment by each party that the processing of personal data will comply with the Agreement and protect the rights of data subjects (and to adopt rules as to compliance and enforcement).

¹ More information is available [here](#).

² National Interest Analysis, para 10.

7. In some respects, the Agreement creates specific safeguards. For example, article 13 requires regular review of retained data and automatic erasure of personal data after 3 years if continued storage is not justified. There are also specific data security measures that are required to be implemented under article 15. Additional care shall be taken when transferring personal data of persons under the age of 18 or personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (for the purpose of uniquely identifying a natural person), data concerning health, or data concerning a person's sex life or sexual orientation. (Article 5).
8. I note that the privacy protections in the Agreement can only be effective if there are operational systems in place at the relevant agencies that give effect to those protections. Under the Agreement, the New Zealand government as the Contracting Party must require the competent authorities to implement appropriate technical and organisational measures to demonstrate that they have the appropriate systems in place to comply with the Agreement and that the rights of individuals are protected.³ This is an important principle of accountability.
9. The Committee may wish to seek formal assurance from each of the competent authorities that they each have implemented the necessary technical and organisational measures.
10. The competent authorities also have to adopt rules specifying how compliance with the provisions regarding the processing of personal information transferred under the Agreement will be enforced in practice, and notify these to my Office as the supervisory authority and to the European Union.⁴
11. The Committee may wish to seek my comment on the adoption of these rules by the competent authorities in due course.
12. Some of the protections and safeguards relating to the handling of personal information that I would expect to see demonstrated by the parties as required under the Agreement include:
 - **A data minimisation approach:** Information exchanged should be adequate, relevant and not excessive (article 4.1).
 - **Ensuring accuracy of information:** Information exchanged should be accurate and up to date. Information that is not accurate, up to date or relevant should not be exchanged (article 8).
 - **Appropriate retention periods:** Information exchanged should not be retained for no longer than necessary. Internal systems should be established to ensure information is safely destroyed as soon as the purpose is fulfilled (article 13).
 - **Right of access:** Individuals should have a right to obtain confirmation whether or not information related to the individual has been processed and have access to their information. This right should at least include certain information about the processing such as the purposes of and legal basis for the processing, the right to lodge a complaint with the supervisory authority or the categories of personal information concerned. Competent authorities should ensure information of this

³ Article 4.4.

⁴ Article 26.2.

exchange of personal information is made available to individuals and their rights to redress in order to achieve transparency to individuals (article 9).

- **Restrictions on onwards transfers:** Competent authorities should have mechanisms in place to ensure information is only further transferred if there is a legal basis to do so and if there are appropriate safeguards in place. Competent authorities should be held liable to prove that they have the relevant authorisation to do the onward transfer (article 7).
- **Automated processing of personal information:** Competent authorities should not make automated decisions which will produce an adverse effect on the individual's rights. Competent authorities should provide necessary safeguards for individual rights (article 6).

13. The Agreement also provides that details of cooperation between the parties to implement the Agreement will be subject to an implementing administrative arrangement between Europol and the New Zealand competent authorities.⁵ The Committee may wish to seek my comment on that arrangement in due course.

Conclusion

14. I am comfortable that the Agreement as drafted is consistent with the expectations of the Privacy Act.

15. The Committee may wish to seek formal assurance from each of the competent authorities that they each have implemented the technical and organisational measure to demonstrate compliance with the Agreement and the protection of the rights of individuals.

16. The Committee may wish to seek my comment on the adoption of compliance and enforcement rules by the competent authorities in due course.

17. The Committee may also wish to seek my comment on the implementing administrative arrangement in due course.

18. I trust my comments in this submission will be of use to the Committee in its considerations. I do not seek to speak to my submission, but I will appear if it will be of assistance to the Committee.



Michael Webster
Privacy Commissioner

5 August 2022

⁵ Article 22.