Justice Centre | 19 Aitken Street
DX SX10088 | Wellington
T 04 918 8800 | F 04 918 8820
ContactUs@justice.govt.nz | www.justice.govt.nz

21 October 2022

Section (9)(2)(a) [redacted]

Our ref: OIA 98726

Tēnā koe Sectio [redacted]

Official Information Act 1982 request: Submissions on overseas disclosures

Thank you for your email of 26 August 2022 requesting, under the Official Information Act 1982, information regarding copies of all submissions on the consultation of regulations for overseas disclosures under section 214 of the Privacy Act 2020. Specifically, you requested:

> *I am writing to ask you for a copy of all submissions on the consultation on regulations to be made specifying countries for overseas disclosures under section 214 of the Privacy Act 2020 (the Act), as well as opinions from the Privacy Commissioner on whether a particular country provides such comparable safeguards.*

Please refer to **Appendix A** for information in scope of your request. Some information has been withheld under section 9(2)(a) to protect the privacy of natural persons.

I can advise that the Ministry of Justice has not completed the process of prioritising the countries to be assessed by the OPC but will do so as soon as is practicable. This is due to competing demands and allocation of resources to other necessary work. I am therefore refusing the second part of your request seeking any opinions provided by the Privacy Commissioner under section 18(e) of the Act as the information requested does not exist.

You have the right under section 28(3) of the Act to complain to the Ombudsman about the decision to extend the time for responding to your request. The Ombudsman may be contacted by emailing info@ombudsman.parliament.nz.

Nāku noa, nā

Kathy Brightwell
General Manager, Civil & Constitutional, Policy Group

Appendix A – Documents in scope

No	Date	Document Title	Document Type	Notes
1.	4 December 2020	Ngā tāpaetanga a Te Hunga Rōia Māori o Aotearoa	Document	Some information is withheld under section 9(2)(a).
2.	4 December 2020	ICNZ submission on Privacy Act 2020 – prioritising countries for overseas disclosure	Document	Some information is withheld under section 9(2)(a).
3.	4 December 2020	New Zealand Bakers Association: Submission to the Ministry of Justice on the consultation on cross-border disclosure regulations under	Document	Some information is withheld under section 9(2)(a).
4.	9 December 2020	List of submissions	Document	Some information is withheld under section 9(2)(a).

Ngā tāpaetanga a Te Hunga Rōia Māori o Aotearoa

Submissions of Te Hunga Rōia Māori o Aotearoa – The Māori Law Society

Te rā 4 o Hakihea 2020

Re: Te Hunga Rōia Māori o Aotearoa views on the Cross-border disclosure under the Privacy Act 2020

A. Kupu whakataki | Introduction

1. Te Hunga Rōia Māori o Aotearoa – the Māori Law Society (**THRMOA**) was formally established in 1988. Since then, the Society has grown to include a significant membership of legal practitioners, judges, parliamentarians, legal academics, policy analysts, researchers and Māori law students. Our vision is Mā te Ture, Mō te Iwi – by the Law, for the People.

2. THRMOA encourages the effective networking of members, makes submissions on a range of proposed legislation, facilitates representation of its membership on selected committees, and organises regular national hui which provide opportunities for Māori to discuss and debate legal issues relevant to Māori.

3. When making submissions on law reform, THRMOA does not attempt to provide a unified voice for its members, or to usurp the authorities and responsibilities of whānau, hapū and iwi, but rather, seeks to provide a whakaaro Māori based legal analysis and submissions on law reform.

4. THRMOA welcomes the opportunity to make written submissions regarding Cross-border disclosure under the Privacy Act 2020 (**Disclosure**).

B. He whakarāpopototanga| Summary

5. These submissions outline two key issues:
   i. the process of consultation and lack of engagement with Māori; and
   ii. the consequences of disclosing Māori data and the importance of data sovereignty.

6. THRMOA does not support the disclosure of Māori data without specific Māori approval. While we support the principles underlying the Privacy Act 2020 (**Act**), such as increased protection of personal data, we are concerned that this specific regime does not adequately address Māori concerns regarding data disclosure for Māori.

C. Ngā Tāpaetanga o THRMOA | THRMOA Submissions

(i) Comments on the consultation process to date and engagement with Māori

7. THRMOA was provided 4 weeks to provide a submission. Meaningful and adequate consultation requires longer timeframes to allow submitters to engage adequately on specific kaupapa. It appears there has been limited engagement with Māori and also limited engagement with issues which would impact Māori. We consider specific consideration of the impacts on Māori should be undertaken for the Government to properly assess potential issues under Te Tiriti. Further, in line with recommendations from the Waitangi Tribunal, we consider processes should be implemented which ensure Government officials provide properly informed advice on the likely impact that any Bill will have on the Government's Te Tiriti obligations and Māori generally. Importantly, an approach anchored in Te Tiriti is essential to ensure Te Tiriti compliant legislation and policy that adequately reflects, and responds to, Māori concerns.

8. We also note there was a distinct lack of Māori input in the development of the Privacy Bill 2018 (**Bill**) itself. THRMOA was not part of targeted consultation of the Bill and the policy documentation does not consider Te Tiriti issues. There is one mention of Te Tiriti in one Cabinet Paper, which declares that the Bill complies with Te Tiriti. However, there is no discussion contained within that Cabinet Paper regarding the reasons for such a declaration.

9. We also note the public submissions received on the Bill do not include any Māori organisations and therefore we think it is essential that current (and future) policy development on the Act includes specific and targeted consultation with Māori.

10. The Act does not contain a specific section which requires it to take into account Te Tiriti o Waitangi. This gap reflects the absence of any meaningful consideration of Te Tiriti or any meaningful engagement with Māori generally. The Departmental Report notes that one submitter on the Bill noted the absence of a Te Tiriti provision. However, the Departmental Report noted that it did not consider any changes needed to be made to the purpose provision because:[1]

> [t]he purpose provision encapsulates the Bill's focus on promoting and protecting individual privacy, primarily through the IPP framework, but with appropriate allowances or concessions for other rights and interests. We think that further refinements would risk a flow on effect in the Bill and could unintentionally create new difficulties in operating the legislation.
>
> We also think that recognising that other interests may in some circumstances need to be accommodated alongside privacy is an important inclusion in the purpose statement, as it makes the overall scheme of the Act clear to users.

[1] At [18] and [19].

11. We appreciate the broad nature of this section, which is able to encompass other rights and interests (and so therefore Te Tiriti rights and interests). But we consider such an approach places too much faith in those making assessments under the Act to have an adequate understanding of Te Tiriti (or other such rights and interests). Therefore it is likely that Te Tiriti will rarely be considered, hence the need for the Act to identify upholding Te Tiriti as a specific purpose or for the Act to include a specific clause requiring consideration of Te Tiriti and Te Tiriti principles.

12. The Government has international and domestic obligations to not only ensure that Māori are consulted on legislation which may impact them, but also to give Māori the opportunity to be meaningfully involved and genuinely influence decisions.

13. Therefore, while THRMOA supports the provisions in the Act aimed at enhancing protection of personal information, we remain concerned whether such protections can adequately protect Māori data when there has been no apparent consideration of the potential impacts for Māori or Te Tiriti. Therefore, we do not support the current cross-border disclosure framework until the Act adequately provides protections for Māori data including prior informed consent from Māori to cross-border disclosure of Māori data.

(ii) Consequences for Māori from cross-border disclosure

14. THRMOA is concerned about the cross-border disclosure of Māori data without prior informed consent from Māori. As noted by s9(2)(a) , Māori must have sovereignty over Māori data and Māori only should determine how, and what, data is shared.[2] The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data also require all purposes for the collection of the data to be communicated at the time of collecting the data.

15. In the Te Taumata report entitled *Māori Interests and Geographical Indicators: Strategic Intellectual Property Management enabling Maori whanau development*[3], the authors also suggested that benefits that arise from the use of Māori data should flow back to Māori in a manner consistent with the Nagoya Protocol.

16. Māori data sovereignty and the potential risks associated with disclosure of Māori data must be part of the Government's discussions with any countries it engages with regarding cross-border disclosure. Further, the Government must engage with Māori to ensure Māori concepts of data, best practice, and harm are accurately reflected in the discussions. The Government consultation must include tikanga experts, tohunga, and those recognised as being holders of mātauranga. THRMOA also encourages the

[2] https://www.stuff.co.nz/pou-tiaki/122212598/concerns-over-how-mori-data-will-be-looked-at-as-new-zealand-plans-to-join-international-cybercrime-treaty

[3] See https://www.tetaumata.com/news/2020/05/08/te-taumata-analysis-on-gis-and-ip-now-available-to-view/, pg 33-34.

Government to consult Māori tech leaders/companies and Māori data sovereignty experts to guide the government when developing best practice involving Māori data, including developing practices consistent with the Nagoya Protocol.

17. Allowing Māori data to be disclosed without obtaining prior informed consent from Māori, or sharing the benefits arising from the use of that data, raises questions about the authenticity of the Government's undertaking to review Aotearoa's IP laws in light of WAI 262 as well as its undertaking to proceed with Te Pae Tawhiti, which aims to address the intellectual property issues raised under WAI 262 regarding the use of our taonga.

18. Under the Act, agencies are required to notify the Privacy Commissioner and the affected individual(s) as soon as practicable after becoming aware of a notifiable privacy breach. A notifiable privacy breach means a breach that has caused serious harm to an affected individual or is likely to do so. The assessment of serious harm is being made through a non-Māori lens and therefore THRMOA is concerned assessors will be unable to assess what is harmful from a te ao Māori perspective regarding any breach involving Māori data.

D. Kupu Whakamutumutu | In Closing

19. THRMOA considers the Government must consult Māori so it can properly assess the specific implications for Māori where Māori data is included in any cross-border disclosures.

20. We also recommend the Government review the Privacy Act 2000 to ensure its provisions adequately protect Māori data and is reviewed for compliance with Te Tiriti and the principles in Te Tiriti.

21. THRMOA expects to be informed regarding this kaupapa, including any progress and developments, further consultation, and proposed legislative amendments.

22. Should you have any pātai or wish to discuss our submissions, please contact s9(2)(a)

Ngā mihi nui ki a koutou

s9(2)(a)

ICNZ Insurance Council of New Zealand

Insurance Council of New Zealand
P.O. Box 474 Wellington 6140
Level 2, 139 The Terrace
Tel 64 4 472 5230
email icnz@icnz.org.nz
Fax 64 4 473 3011
www.icnz.org.nz

4 December 2020

Ministry of Justice
Justice Centre
Wellington

Emailed to: ipp12consultation@justice.govt.nz

Dear Madam/Sir,

ICNZ submission on Privacy Act 2020 – prioritising countries for overseas disclosure

Thank you for the opportunity to submit on the Privacy Act 2020 IPP 12 – prioritising countries for overseas disclosure consultation.

ICNZ represents general insurers that insure about 95 percent of the New Zealand general insurance market, including about a trillion dollars' worth of New Zealand property and liabilities. ICNZ members provide insurance products ranging from those usually purchased by individuals (such as home and contents insurance, travel insurance, motor vehicle insurance) to those purchased by small businesses and larger organisations (such as product and public liability insurance, professional indemnity insurance, commercial property, business interruption and directors and officers insurance).

New Zealand is part of a global general insurance market, with a number of insurers in New Zealand either operating as local branches with overseas parents or as part of wider foreign-owned insurance groups. One important aspect of being part of the global insurance market is enabling the timely transfer of information, particularly where it is needed for reinsurance or retrocession (the reinsurance of risk by a reinsurer) agreements, or for the operation of insurance companies' related entities. For these reasons, and because we believe they would provide comparable privacy safeguards to those in New Zealand, we submit that the countries be prioritised in the following order for assessment to be prescribed countries under regulations to the Privacy Act:

- Australia
- The EU
- The USA
- The UK
- Singapore – specifically as its Personal Data Protection Act 2012 provides similar safeguards to those in the Privacy Act 2020, and because Singapore is New Zealand's largest trading partner in the South East Asia region and 7th largest trading partner in the world.

In relation to the EU, we note that New Zealand is one of only 12 territories that has been granted adequacy status by the European Commission and question whether this should import some sort of reciprocity by New Zealand to specifically prioritise the EU for assessment. Given the strict EU privacy regulations and the rigorous process of the European Commission to reach an adequacy decision, we further question whether it might be appropriate for the Ministry of Justice to fast-track the assessment process to recognise the value New Zealand businesses receive through holding adequacy status.

Thank you again for the opportunity to submit on this consultation. If you have any questions, please contact our Legal Counsel on s9(2)(a)

Yours sincerely,

s9(2)(a)

NEW ZEALAND BANKERS ASSOCIATION

Submission

to the

Ministry of Justice

on the

Consultation on cross-border disclosure regulations under section 214 of the Privacy Act 2020

4 December 2020

NEW ZEALAND BANKERS ASSOCIATION
Level 15, 80 The Terrace, PO Box 3043, Wellington 6140, New Zealand
TELEPHONE +64 4 802 3358 EMAIL nzba@nzba.org.nz WEB www.nzba.org.nz

About NZBA

1. The New Zealand Bankers' Association (**NZBA**) is the voice of the banking industry. We work with our member banks on non-competitive issues to tell the industry's story and develop and promote policy outcomes that deliver for New Zealanders.

2. The following seventeen registered banks in New Zealand are members of NZBA:
   - ANZ Bank New Zealand Limited
   - ASB Bank Limited
   - Bank of China (NZ) Limited
   - Bank of New Zealand
   - China Construction Bank
   - Citibank N.A.
   - The Co-operative Bank Limited
   - Heartland Bank Limited
   - The Hongkong and Shanghai Banking Corporation Limited
   - Industrial and Commercial Bank of China (New Zealand) Limited
   - JPMorgan Chase Bank N.A.
   - Kiwibank Limited
   - MUFG Bank Ltd
   - Rabobank New Zealand Limited
   - SBS Bank
   - TSB Bank Limited
   - Westpac New Zealand Limited

Introduction

3. NZBA welcomes the opportunity to provide feedback to the Ministry of Justice (**MOJ**) on its consultation on the proposed cross-border disclosure regulations under 214 of the Privacy Act 2020. NZBA commends the work that has gone into developing this consultation.

Summary

4. We understand that the criteria for determining the criteria for prioritising countries for assessment as "prescribed countries", is as follows:

   (a) the likelihood of meeting key privacy standards, as MOJ does not want to prioritise countries that are unlikely to be prescribed;

   (b) the size of the economic relationship, which will allow MOJ to prioritise countries that will be the most beneficial for New Zealand businesses and stakeholders; and

(c) New Zealand business and stakeholder views, to assist MOJ in understanding which countries would be most valuable to prioritise and why.

5. We propose the European Union (including the United Kingdom) (**EU**) and Australia receive priority consideration to be assessed as prescribed under the Privacy Act 2020 on the basis set out below.

EU and Australia likely to meet key privacy standards

6. The EU has recently enacted the General Data Protection Regulation (**GDPR**), which is widely considered to be the high bar of privacy legislation internationally.

7. Australia has the Privacy Act 1988, which informed the design of New Zealand's existing Privacy Act 1993 and is structurally very similar to the Privacy Act 2020. It is acknowledged that Australia also has privacy legislation operating at the state level and that it is not as comprehensive, but this is less relevant to determining whether a country should be a "prescribed country"

8. Both the GDPR and Australian Privacy Act 1988 share the principles-based approach to privacy with the Privacy Act 2020, with principles addressing collection, use, disclosure, correction, access, security and transparency.

9. The GDPR, Australian Privacy Act 1988 and Privacy Act 2020 also share the same conceptual origin of the 1980 OECD Privacy Guidelines, which has strongly influenced their similarity today.

10. Both the EU and Australia have functional judicial systems.

11. While the Australian Privacy Act 1988 is very similar to the Privacy Act 2020, the Privacy Act 1988 has carve-outs for employee data and for businesses with less than AUD$3 million revenue. This may mean that Australia's status as a prescribed country would have to be limited in its application to non-employee data and organisations with more than AUD$3 million revenue.

12. The Australian Attorney-General is reviewing the Privacy Act 1988. In particular, whether the exemptions should be removed. Early discussions in the market suggest the carve-outs may be removed (due to Australia wanting to be found to provide "adequate protection" – see below).

13. The GDPR has a number of privacy protections that go above and beyond the Privacy Act 2020 such as the right to an explanation of automated decisions, right to data portability, right to erasure, much larger fines, and extra protections for special categories of data.

Size of the economic relationship, and business and stakeholder views

14. The Ministry for Foreign Affairs and Trade has listed Australia as our biggest services trade partner here and the Closer Economic Relations Trade Agreement is particularly comprehensive. In addition, the EU is one of our largest markets by volume of trade.

15. We also note that the GDPR has a regime which looks at whether countries provide "adequate protection" (which has been found to mean "essentially equivalent" protection) compared to the high standard of the GDPR. This is conceptually similar to the "prescribed countries" regime that MOJ is now consulting on, and should mean international disclosures to countries providing "adequate protection" are aligned to disclosures that occur within the EU.

16. New Zealand has been found to provide adequate protec ion by the European Commission (as has Argentina, Canada (commercial organisations), Israel, Japan, Switzerland, Uruguay, and discussions with South Korea are ongoing). In addition to finding EU countries as providing 'comparable safeguards', MOJ could form a view that the European Economic Area, and any country which the European Commission has found to provide "adequate protection", all provide 'comparable safeguards' and hence could be added to the NZ "prescribed countries" list.

17. Essentially MOJ could rely on the comprehensive review the European Commission carries out in determining 'adequate protection' in an EU context, and add those countries to the NZ "prescribed countries" list. Including all countries (i) subject to the GDPR, or (ii) found to provide "adequate protection" (essentially equivalent protection) to the GDPR, would greatly expand the relevant amount of trade impacted.

Contact details

18. If you would like to discuss any aspect of this submission, please contact:

s9(2)(a)

Name: - Name	Organisation: - Org	Please provide your views on the countries you would find it most valuable to see prioritised and why: - Feedback	Last Modified Date	Response ID	IP Address	Created Date	Citizen Space Version	Consultation State	Browser Identification	Submitted Date	Visited Pages - Consultation
Not Answered	Not Answered	European Union countries the UK and a l white- isted jurisdictions (as determined by the European Commission). This enables alignment with the GDPR and ensures a consistent approach.	2020- 0-29 10:07:16	ANON-ZYVJ-CBYA-8	s9(2)(a)	2020-10-29 10:07: 6	v5.11.1	open	Mozi la/5.0 (Windows NT 10.0; WOW6	2020-10-29 10:07:28	Consultation
Not Answered	Not Answered		2020- 0-29 10:10:31	ANON-ZYVJ-CBYJ-H		2020-10-29 10:10:31	v5.11.1	open	Mozi la/5.0 (Windows NT 10.0; Win64	2020-10-29 10:10:36	Consultation
Not Answered	Not Answered	Australia USA Canada UK Europe Hong Kong	2020- 0-29 10:42:36	ANON-ZYVJ-CBYD-B		2020-10-29 10:42: 6	v5.11.1	open	Mozi la/5.0 (Windows NT 10.0; Win64	2020-10-29 10:43:26	Consultation
Not Answered	Not Answered	These are countries we do business in predominantly and have they dave developed privacy laws but are not necessarily comparable to NZ (some more some less some different). Australia as it is part of our regional banking group and The Netherlands as that is where our shareholder and global head office is.	2020- 0- 0 11:56:20	ANON-ZYVJ-CBYX-Y		2020-10-30 11:56:20	v5.12.0	open	Mozi la/5.0 (Windows NT 10.0; Win64	2020-10-30 11:56:48	Consultation
Not Answered	Not Answered	Australia Ongoing difficulties	2020- 0-31 11:17:46	ANON-ZYVJ-CBYH-F		2020-10-31 11:17:46	v5.12.0	open	Mozi la/5.0 (Linux; Android 7.1.1; SM-J	2020-10-31 11:18:12	Consultation
Not Answered	Not Answered	GDPR compliant countries would be my first priority. due to their rigorous privacy laws. Australia as they provide cloud servers for a lot of NZ software Vendors which means that a lot of data is stored over there .	2020-11-02 15:44:19	ANON-ZYVJ-CBYU-V		2020-11-02 15:44:19	v5.12.0	open	Mozi la/5.0 (X11; Ubuntu; Linux x86_6	2020-11-02 15:44:24	Consultation
Not Answered	Not Answered	Least valuable is the US as they pay little head to overseas regulations i e. Facebook's disregard of GDPR.	2020-11-02 17:06:27	ANON-ZYVJ-CBYS-V		2020-11-02 17:04:04	v5.12.0	open	Mozi la/5.0 (Android 10; Mobile; rv:81	2020-11-02 17:06:33	Consultation
Not Answered	Not Answered	I would recommend MOJ prioritise the following countries/areas: - UK - EEA - Australia The main reason for this is these countries/areas are where the majority of data partners are currently located. Whilst there is growth in APAC regions this is at a slower pace than these other countries/regions. If adequacy were to be given for these regions this would considerably ease the compliance burden for SMEs when they look to work with partners worldwide. A secondary reason (for larger global organisations with a presence in NZ) is that these organisations are more likely to have presence in these countries/areas. A third reason is that these regions have comprehensive privacy law regimes in place so it is realistic to assume that an adequacy arrangement could be made (particularly in the case of the EEA which already considers NZ a country with adequate privacy laws).	2020-11-04 13:42:47	ANON-ZYVJ-CBY2-S		2020-11-04 13:42:47	v5.12.0	open	Mozi la/5.0 (Macintosh; Intel Mac OS)	2020-11-04 13:43:21	Consultation
Not Answered	Not Answered	I do not believe any personal information should be shared with other countries. Good day Thank you for the opportunity to provide a view I would not wish for cross-border disclosures except where there is already some official or legal connection. For example I hold joint NZ/UK passports by default of being born in UK Therefore I would only accept cross-border disclosures of my personal data with UK There is no requirement for any other countries to gain access particularly not USA or any other countries in Europe. Whilst many countries have laws there are too many cases of governments / other bodies collecting data and a lowing use of it in inappropriate manner	2020-11-06 20:56:14	ANON-ZYVJ-CBYY-Z		2020-11-06 20:56:14	v5.12.0	open	Mozi la/5.0 (iPhone; CPU iPhone OS 14	2020-11-06 20:56:31	Consultation
Not Answered	Not Answered	Thank you Don't I repeat DON'T trust the USA. The government there continues to show its incompetence in maintaining personal privacy. They also regularly seeks personal private information on US citizens living abroad by use of nefarious and extortionist means threatening foreign countries and entities with freezing assists if they fail to comply with US Government attempts to track and control US citizens abroad.	2020-11-07 12:28:36	ANON-ZYVJ-CBY9-T		2020-11-07 12:28: 6	v5.12.0	open	Mozi la/5.0 (Macintosh; Intel Mac OS)	2020-11-07 12:28:57	Consultation
Not Answered	Not Answered	Australia: as this country is a close trading partner with New Zealand.	2020-11-08 08:00:11	ANON-ZYVJ-CBY8-Z		2020-11-08 08:00:11	v5.12.0	open	Mozi la/5.0 (iPhone; CPU iPhone OS 13	2020-11-08 08:00:50	Consultation
Not Answered	Not Answered	European Union: given detail in the EU General Data Protection Regulation (GDPR).	2020-11-24 14:25:35	ANON-ZYVJ-CBYS-T		2020-11-24 12:33:27	v5.12.0	open	Mozi la/5.0 (Windows NT 10.0; WOW6	2020-11-24 14:25:49	Consultation
Not Answered	Not Answered	Dear Justice Department on Cross-board disclosures. We currently are a health IT solutions provider in New Zealand and wish to engage multi-national cloud service providers to use some of their advanced tools that support scalable use of their technology systems to improve New Zealand health service delivery. Some involve using secure but cognitive services technologies that process personal health information in certain jurisdictions but provide those back to NZ for use. Some of these services are currently based in the fo lowing jurisdictions and we would like clarity over whether these services can be considered within the prescr bed country rules. - Australia (AWS South East Microsoft Azure South East Google Sydney) - Singapore (AWS Google Microsoft) - Ireland (AWS) - London (AWS Google Microsoft) - Frankfurt (AWS Google Microsoft) We are aware of the sensitivity of the Patriot Act in the US and it w ll not be somewhere we believe it can be certain for health information to be used in that environment. Same applies to Hong Kong and the equivalent legislation to health information in China.	2020-11- 0 16:40:41	ANON-ZYVJ-CBYC-A		2020-11-30 16:40:41	v5.13.0	open	Mozi la/5.0 (Windows NT 10.0; Win64	2020-11-30 16:41:04	Consultation