

27 June 2024

Office of the Privacy Commissioner
poupou@privacy.org.nz

ICNZ SUBMISSION ON POUPOU MATATAPU

1. Thank you for the opportunity to provide a submission to the Office of the Privacy Commissioner's (**OPC**) consultation on its draft guidance 'Poupou Matatapu'.
2. Te Kāhui Inihua o Aotearoa / The Insurance Council of New Zealand (**ICNZ**) is the representative organisation for general insurance companies in New Zealand. Our members collectively write more than 95 percent of all general insurance in New Zealand and protect well over \$1 trillion of New Zealanders' assets and liabilities. ICNZ members provide insurance products ranging from those usually purchased by individuals (such as home and contents insurance, travel insurance, and motor vehicle insurance) to those purchased by small businesses and larger organisations (such as product and public liability insurance, professional indemnity insurance, cyber insurance, commercial property insurance, and directors and officers insurance).
3. Thank you for granting us an extension to the deadline for making submissions. ICNZ has been working on its submission to the Justice Select Committee on the Privacy Amendment Bill which was open for submissions at the same time as the OPC's consultation on Poupou Matatapu. As a result, our comments on Poupou Matatapu, set out below, are relatively brief.

General feedback on the pou

4. We support consolidated guidance from the OPC on what doing privacy well looks like.
5. We understand the pou have been developed to help agencies do privacy well. We envisage that agencies will use the pou to review their current privacy management practices to inform opportunities for development and enhancement over time. However, to the extent that the pou "sets [the OPC's] expectations about what good privacy practice looks like", the pou may be interpreted as setting a standard beyond supporting compliance with the Privacy Act 2020. Given it is not entirely clear what the status of the pou are, it would assist if the OPC could provide greater clarity of its expectations for the outcomes of the guidance. In particular, the OPC should make clear how it intends to use the pou and if it will inform the OPC's assessment of an agency's privacy practices.
6. If there is an expectation from OPC that agencies follow this guidance, we consider that the guidance would benefit from another round of consultation, particularly given the size of the document/s in total.

7. Clarity is also required on the OPC's expectations on the timeframe in which agencies should consider the guidance in the pou in respect of their own privacy practices. This must be realistic and take into account the breadth of the guidance, resources required to work through, and the competing regulatory changes currently being implemented or anticipated, including the parallel challenge of progressing implementation of the Privacy Amendment Bill. More broadly there needs to be recognition of competing regulatory resource demands for entities, and for insurers in particular, as a range of other regulatory developments must be implemented over the next 2-3 years. There also needs to be recognition of a Consumer Data Right being implemented in some sectors and also growing expectations in the management of AI and cyber security etc, all of which can impose requirements on agencies to respond to.
8. In terms of the structure of the individual pou documents, we also suggest that the OPC consider moving the "key objectives" section to the start of each of the pou.

Governance pou

9. Staffing the governance structure is referred to in the examples in the pou but is not specifically stated in the pou's guidance sections. Adding something to the effect of "*To ensure the governance function runs effectively, it should be proportionately resourced to meet an organisation's size and demands*" could help highlight the resource required to do privacy well.
10. The Governance pou is quite prescriptive in some respects and does not recognise that many agencies already have mature structures in place, with overall responsibility for legal compliance across all relevant legislation. Perhaps the guidance could suggest how agencies use their existing governance functions to support a culture of privacy, and have oversight of privacy.
11. The section on setting a privacy strategy appears to be too prescriptive. This section should reflect that agencies may have various approaches to setting the direction of their privacy strategy which achieve the same result such as through compliance plans, privacy policy etc. The section on privacy culture should acknowledge the role that a code of conduct, privacy policy, and IT and Security standards may play in supporting a good privacy culture.
12. In relation to the 'Accountability' section, we note there may be both owners of privacy risks and owners of privacy obligations in the organisation accountable for ensuring there is an effective control environment in place to manage risk and compliance, i.e. built into an organisation's risk management framework.

Know Your Data pou

13. The Know Your Data pou posits that completing a data map and data inventory is a necessary step to assess an agency's privacy risks, to obtain a comprehensive view of the personal information the agency is responsible for. However, completing a data map and data inventory exercise could require substantial resource for large agencies, like insurance companies, who have complex business structures and numerous IT systems. It would also likely require significant effort to keep a map and inventory up to date. It is unclear if agencies may take their individual circumstances into account when assessing the need for or extent of a data mapping exercise, particularly if the agency is comfortable that it has in place a robust risk management programme.
14. Data mapping and inventory are one avenue organisations may take, although assessment of privacy risk may be achieved through existing risk management processes and having a structured approach to data governance can achieve the same view of personal information as that set out under the data mapping and inventory section of the pou. It is unrealistic of

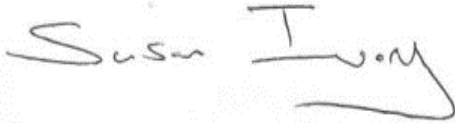
the OPC to expect all agencies to have a data map to assess their risk profile, although it is reasonable to expect organisations to be using some documented method to assess privacy risks.

15. The Know Your Data pou contains links to other documents, e.g., Assessing agency privacy risk, in the text of the pou. Any relevant requirements in those documents should be incorporated into the pou. It would assist agencies to have all the relevant requirements in the one place.

Transparency pou

16. We note this pou will need to be updated to reflect to the new requirements in the Privacy Amendment Bill if that Bill is enacted.
17. Please contact me (susan@icnz.org.nz) if you have any questions on our submission or require any further information.

Yours sincerely

A handwritten signature in black ink that reads "Susan Ivory". The signature is written in a cursive style with a large, sweeping flourish at the end of the name.

Susan Ivory
Regulatory Affairs Manager