New Zealand Banking Association
Te Rangapū Pēke

Submission

to the

Office of the Privacy Commissioner – Te Mana Mātāpono Matatapu

on the

Draft Guidance: *Poupou Matatapu – Doing Privacy Well*

27 June 2024

NEW ZEALAND BANKING ASSOCIATION – TE RANGAPŪ PĒKE
PO Box 3043, Wellington 6140, New Zealand
www.nzba.org.nz

About NZBA

1. The New Zealand Banking Association – Te Rangapū Pēke (**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 eighteen 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.
- KB Kookmin Bank Auckland Branch
- Kiwibank Limited
- MUFG Bank Ltd
- Rabobank New Zealand Limited
- SBS Bank
- TSB Bank Limited
- Westpac New Zealand Limited

Contact details

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

Antony Buick-Constable
Deputy Chief Executive & General Counsel
antony.buick-constable@nzba.org.nz

Sam Schuyt
Associate Director, Policy & Legal Counsel
sam.schuyt@nzba.org.nz

Introduction

4. NZBA welcomes the opportunity to provide feedback to the Office of the Privacy Commissioner – Te Mana Mātāpono Matatapu (**OPC**) on the Draft Guidance: Poupou Matatapu – Doing Privacy Well (**Guidance**). NZBA commends the work that has gone into developing the Guidance.

5. In general, we support OPC issuing this guidance and think it provides a helpful outline for how to manage a privacy function.

6. Set out below is our feedback on particular elements of the following pou:

    6.1. Governance

    6.2. Know your Data

    6.3. Building Capability and Awareness

    6.4. Breach Management

    6.5. Measure and Monitor

Governance

7. NZBA considers that several defined terms in this section would benefit from clarification. For example:

    7.1. "Governance members" should be defined earlier in the Guidance to provide industry with clarity on whom the document is referring to.

    7.2. "Governance function" is confusing and could include a number of meanings. "Committee" would, in our view, be an appropriate replacement, given many larger organisations have a governance function that does not include a privacy focus.

    7.3. OPC should consider referencing the key Privacy Officer duties as per the Privacy Act, as this would be useful clarity for organisations.

    7.4. The description for "Who should be the privacy officer" is lacking necessary detail for industry. We encourage OPC to consider the UK Information Commissioner's Office's (**ICO**'s) guidance on data protection officers by way of example to provide further detail (but to be tailored, as appropriate, for New Zealand), which will support industry in appointing appropriate officers to meet its obligations in this area.

Know your data

8. We consider that the Guidance should clearly express that this pou is not a privacy obligation, but rather, that it is a globally recognised best practice methodology to understand privacy risks for agencies.

9. In our view, the Guidance does not fully acknowledge the different and wide range of businesses that could apply this Guidance. Agencies will have a range of different solutions for how they arrange and understand their data. For example, this could range from a small business using a table that requires manual input, to a large organisation using a fully automated system that is integrated with other systems across a business.

10. A range of practice solutions should be accepted if they are fit for purpose for a particular organisation to map and record their data.

11. This pou says that organisations should have minimum (statutory) and maximum (necessary business purposes) retention periods. Technology systems need clear rules to be able to apply disposal rules – setting minimums and maximums is not clear enough to achieve this.

12. We submit that the Guidance should advise organisations to set a single time limit for each category of information. The decision relating to the time limit should then factor in any statutory requirements (for example, retention periods under an agency's anti-money laundering / countering financing of terrorism (**AML/CFT**) programmes) and / or legitimate business needs.

13. More specifically in relation to this section of the Guidance:

    13.1. The Guidance should be consistent with its terminology to avoid potential confusion. It should use either "data map" or "data inventory", rather than both.

    13.2. The sentence "or are collecting personal information about individuals outside of New Zealand" is subject to interpretation, and should be reframed to avoid misinterpretation.

Building Capability and Awareness

14. As drafted, we submit that the Guidance is overly prescriptive in this section. Due to the level of training required, organisations often embed sophisticated and mandatory training modules. Further, the use of prescriptive language in the Guidance undermines the purpose of guidance generally, which in our view is meant to provide flexibility for organisations.

15. We also submit that this section should be aimed at all employees, as privacy is a matter that concerns all employees.

Breach management

Definitions of 'harm'

16. One of the types of serious harm listed in this pou is financial fraud, including unauthorised credit card transactions or credit fraud. While we agree that financial fraud could *lead* to serious harm, in our view the existence of fraud does not automatically equate to serious harm. Further, we do not consider that all financial information is sensitive information, or leads to fraud and identity theft.

17. All types and levels of fraud or financial harm need to be viewed in their wider context, i.e. the privacy breach they relate to. In our view, a few unauthorised credit card transactions of small amounts, which were caught early and refunded to the customer promptly, should not meet the definition of serious harm.

18. This pou also sets out an additional level of harm, listed as extreme harm. We query why extreme harm is listed as a new category without a statutory basis, particularly where the pou says that if extreme harm has been caused, agencies are advised to call the Police before notifying OPC. Without the statutory basis (and noting that it would be for the Ministry of Justice to amend legislation) we consider that extreme harm should not be referred to in the Guidance.

19. We submit that the roles and responsibilities of affected individuals and agencies should reflect the context of the breach and the amount of harm. In some cases, it will be more sensible for agencies to support the affected individual in making police reports where required – we do not think it is always an agency's role to notify Police.

20. If the extreme harm category does remain in the final version of the Guidance, we submit that it is clarified to say to either call 105 or 111 depending on whether there is imminent or immediate harm, or whether the harm has already occurred.

21. We further submit that the use of "theft of significant amounts of money" as an example of extreme harm is inconsistent with the other examples listed (kidnapping, national security and risk to an individual's life).

Additional comments

22. We submit that the Guidance would benefit from further clarification. In particular, we would welcome further detail on the relationship between situations where the Guidance suggests the police should be called, and where an agency may be subject to "tipping off" obligations where it has reported a SAR.

23. We note that the Guidance provides information on areas that are already captured in the Privacy Act and previous OPC guidance – for example, sections 112 – 117 of the Privacy Act have been repeated, along with previous OPC guidance on "Working with

sensitive information". Reiterating these elements risks causing confusion among users as to which Act / guidance they should be referring to.

24. We consider that a "debrief meeting" should be where and when warranted, not held after every incident, as the seriousness of incidents can vary.

25. We encourage OPC to use the wording in the Privacy Act in relation to reporting "notifiable breaches", the Guidance refers to notifying "serious privacy breaches" and this could cause confusion.

Measure and monitor

26. This pou could, in our view, be amalgamated with the "Measure and Monitor" and "Privacy Management Plan" pou.

27. NZBA considers the various risk types should be outlined for clarity – for example Privacy Collection, Use and Disclosure, and Retention.

General

28. We question how the Poupou Matatapu will be positioned. We understand that the Guidance has been described as setting pillars of good practice, but by the way certain elements have been drafted (for example, in terms of building capability) it appears to be more like strong, directive guidance. We would appreciate further clarity as to how OPC intends the Guidance to operate.

Conclusion

29. NZBA is happy to provide further detail on the above submission if helpful.