IN CONFIDENCE

Privacy Act 2020 – Guidance for Agencies

28 January 2020

1. Introduction

The new Privacy Act 2020 (the **Act**) came into effect on 1 December 2020, replacing the Privacy Act 1993. Amongst others, the Act introduces the following key changes:

(a) That an entity may not require personal information unless it is necessary for the lawful purpose for which the information is collected; and
(b) Introducing a new regime for mandatory reporting of a "notifiable privacy breach" (see further below).

This is a high-level overview of the actions New Zealand Government Procurement (**NZGP**) has taken in accommodating for the Act.

This practice note / centrally produced guidance summarises the key changes that will likely affect agencies' procurement practices. It is not intended to replace agencies' own policies or guidance to address these changes, although agencies may find this is a useful framework for how they accommodate the key changes of the Act if they haven't yet done so.

2. Overview

The purpose of the Act is to promote and protect individual privacy by:

(a) providing a framework for protecting an individual's right to privacy of personal information, including the right of an individual to access their personal information, while recognising that other rights and interests may at times also need to be taken into account; and
(b) giving effect to internationally recognised privacy obligations and standards in relation to the privacy of personal information, including the OECD Guidelines and the International Covenant on Civil and Political Rights.[1]

3. Application to Agencies and Procurement

Procurement practitioners at government agencies, including NZGP, have responsibilities under the Act in terms of the treatment of personal information which has been collected and held.

Collecting information

- An entity may not require an individual's personal information unless it is necessary for the lawful purpose for which the information is collected.
- Accordingly, it is a good time to review and update your agency's privacy statements. Ask:
    - Is your privacy statement clear enough about the purposes of collection and use of the personal information being sought?
    - Is there a clear link between the information your agency is collecting and your functions?

Holding information

[1] Privacy Act 2020, s 3.

- Your agency should consider your retention policies for documents containing personal information, e.g. consultation documents and commercial proposals submitted in response to RFxs. Ask:
    - How long is personal information being retained and is this appropriate?
    - Does your Business Continuity Plan cover your obligations with regards to personal information?
    - Teams that manage documents containing personal information should consider and review their practices.

- Remember that your agency must provide timely and efficient access to any person who wants to access their personal information. A failure to meet this requirement could constitute a notifiable breach (see below).
    - Ensure you know what personal information you hold and for what purpose. Ensure you have practices in place to promptly respond to requests to access personal information.

- Please note: there is an ability to extend the timeframe within which access to information must be granted if [2]:
    - the request is for a large quantity of information, or necessitates a search through a large quantity of information and meeting the original time limit would unreasonably interfere with the operations of the agency; or
    - consultations necessary to make a decision on the request are such that a response to the request cannot reasonably be given in the original time limit; or
    - the processing of the request raises issues of such complexity that a response to the request cannot reasonably be given within the original time limit.

Breach of the Privacy Act 2020 (e.g. unauthorised access or disclosure, information collected without consent, use of information for an unauthorised or unlawful purpose)

- The Act has introduced a new regime for mandatory reporting of a "notifiable privacy breach". As such, notification of breaches to the Office of the Privacy Commission (**OPC**) is now mandatory for privacy breaches that "cause, or are likely to cause, serious harm" (each a "notifiable breach").
    - Your agency must have in place a policy that specifies more clearly when it will report breaches to the OPC, consistent with your wider agency policy.
    - This policy should be reviewed periodically against your wider agency policy and any OPC and law firm guidance that is published from time to time.

- The OPC has powers to request information from your agency in performing its functions. As you do with other regulators with similar powers (e.g. Commerce Commission, OAG), you should request that the OPC reference the statutory power when making the request. This protects your agency and branch from liability that may otherwise arise from making a disclosure to a third party.

Contracting with suppliers

- If a supplier carries on business within New Zealand, it must apply the Act to personal information it holds or processes in New Zealand and overseas.
    - Consider whether your agency wishes to add additional contractual safeguards such as ensuring notification of any breaches, warranties as to minimum standards of protection in place etc.

- Agencies can only transfer personal information to a foreign company if it is subject to:

[2] Privacy Act 2020, s 48.

- laws that provide comparable safeguards to the Act (a list of prescribed countries will be set out in regulations[3]); or
- contractual obligations that are comparable to the Act.

- This requirement does not apply where the personal information is just held by the foreign company on behalf of an agency (e.g. where it is held by a cloud services provider for safe custody or processing – but is not used for any other purpose). In these circumstances, the agency should ensure that the foreign entity complies with any obligations the agency has under the Act.

- For GMC templates for which personal information is shared to enable the performance of the services, consider adding a new sub-clause in clause 2 as follows:

  Privacy: Where the Supplier is holding or processing any personal information (as defined in the Privacy Act 1993) the Supplier must:

  (a) comply with its obligations under the Privacy Act 2020, including any Code of Practice made under that Act;

  (b) report any breach or potential breach of its obligations in respect of such personal information; and

  (c) give the Buyer reasonable notice in advance of making a mandatory breach notification to the Privacy Commissioner (or, where prior notice is not reasonably possible, promptly after).

  This may also be useful for other contracts used by your agency.

4. Actions

This high-level guidance has been produced to help agencies consider how they incorporate the new changes implemented by the Act. It is important for all government officials who handle personal information to be aware of the new changes and implement actions now to accommodate them.

If you have not already done so, take the time to consider and review your agency's privacy clauses, corresponding policies and general work conduct to reflect these changes.

5. Further information

To expand your knowledge on the Act and more importantly, reporting privacy breaches, the OPC has created a short Privacy Act 2020 animation that explains the key changes introduced by the Act.

[3] Privacy Act 2020, s 214.