BUDDLE FINDLAY

Five things businesses should be doing now to prepare for the new Privacy Act

Allan Yeoman, Keri Johansson

8 May 2020

The Privacy Bill 2018 (Bill) is scheduled to come into force on 1 November 2020. While this is still a few months away, implementing the new rules may take some time.

Here are five practical things that we recommend all businesses should start doing now to get ready:

1. Map your data, if you don't already

Understanding what data you collect, and how it's used, is a fundamental part of good data management practices. If not already being done, then now is a good time to map your dataflows to make sure you have a detailed record of what personal information your business collects, where you get it from, and who you share it with. This will inform what your privacy policy should cover, make sure you pick up any overseas transfers of data, and help you list any third parties like data storage providers and processors that you need to cooperate with in order to meet your obligations.

2. Introduce a data breach policy

A major new feature of the Bill is the requirement to notify the Privacy Commissioner and potentially affected individuals of certain privacy breaches, where it is reasonable to believe the breach has caused (or is likely to cause) serious harm. Failure to report where required will carry a fine of up to NZ$10,000.

To prepare for this, businesses should have a privacy breach policy in place that:

- Requires privacy breaches to be reported internally to the privacy officer and management;
- Sets out the criteria for determining whether notification is required; and
- Lists what information a breach notice should contain, applicable timeframes, and who will send the data breach notice.

Relevant staff should also be notified and trained on the new policy, and contracts with data processing providers and other suppliers should be reviewed to make sure they are required to notify you of any breaches involving your data.

3. Consider template data transfer and processing agreements

Another key change under the Bill is the new Information Privacy Principle 12, which requires businesses to ensure that personal information being disclosed out of New Zealand is protected by privacy safeguards that are comparable to ours. In practice, the simplest way to do this may involve agreeing a contract with the recipient that requires the recipient to protect the personal information as though the overseas recipient were subject to New Zealand law.

Transfers of personal information to data storage providers (or other services that only store or process data on your behalf, and don't use it for their own purposes) aren't treated as an overseas "disclosure". Under the Bill, you will remain legally responsible for how your provider treats that information, including in relation to privacy breaches. In light of this, businesses should check and update their contracts with these providers to make sure that you have the controls in place to comply with the Bill while information is held by the provider.

Where changes to your existing contracts are necessary to cover these points, a template data transfer or processing agreement can be an efficient way to put in place the necessary protections without having to renegotiate the wider relationship.

4. Make sure you have a Privacy Officer

Businesses are already required to have a privacy officer under the current Act, but with new enforcement measures coming in the Bill, it's a good time to check who that privacy officer is and make sure their training is up to date. Under the Bill there is also an option to appoint a privacy officer that is external to the agency, for example by outsourcing or sharing the role with a specialist privacy consultancy.

5. Review your Privacy Statement

Late last year, the Privacy Commissioner warned businesses that he is expecting businesses to improve their privacy disclosures, and that some practices that are currently common (such as relying on "consents" buried in pages of legalese) won't be good enough under the Bill. The Commissioner has new enforcement powers under the Bill to help facilitate this.

The Bill also clarifies that businesses should not be collecting information in identifiable form unless it is "necessary" to do so. Where businesses can carry out the same purpose with anonymous information, they should be taking this option.

Therefore, now is a good time to review your privacy statement and ask yourself:

- Are we only collecting personal information on an identifiable basis where it is necessary to do so?
- Is the privacy statement readable and presented in a way that encourages people to read it?
- Is there anything unexpected in the privacy statement that should be brought to people's attention more prominently (eg via a separate tick box)?

This article was written by Allan Yeoman and Keri Johansson for the NBR (May 2020).

Auckland

188 Quay Street
Auckland 1010

PO Box 1433
Auckland 1140
New Zealand

P: +64 9 358 2555
F: +64 9 358 2055

Wellington

Aon Centre
1 Willis Street
Wellington 6011

PO Box 2694
Wellington 6140
New Zealand

P: +64 4 499 4242
F: +64 4 499 4141

Christchurch

83 Victoria Street
Christchurch 8013

PO Box 322
Christchurch 8140
New Zealand

P: +64 3 379 1747
F: +64 3 379 5659