PRIVACY LAW

$1 MILLION FINES, DATA PORTABILITY AND COMPLIANCE MONITORING? RECOMMENDATIONS OF THE NEW ZEALAND PRIVACY COMMISSIONER

The Privacy Commissioner’s latest review of the Privacy Act 1993 sets out six recommendations aimed at increasing the effectiveness of, and modernising, the Act, which has now been in effect for almost 24 years.

He recommends:

- fines of up to $1 million;
- data portability;
- compliance monitoring;
- controls on the re-identification of data;
- adjustments to existing criminal offences; and
- reforming the public register privacy principles.

These recommendations are aimed at bringing New Zealand privacy laws in line with international developments, and to give the Privacy Commissioner greater powers to encourage and incentivise compliance.

THE REVIEW

Under the Act, the Privacy Commissioner is required to review and report on the operation of the Act and on any amendments the Privacy Commissioner considers are necessary and desirable at least every five years.1 This latest review covers the period 2011 - 2016, following the New Zealand Law Commission’s comprehensive 2011 review of New Zealand privacy laws.

The Privacy Commissioner has noted that rapid changes in information technology and data science, and significant developments in international legal frameworks (in particular, the European General Data Protection Regulation (GDPR), which will come into force in May 2018) since the Law Commission’s review means more matters need to be considered if we are to have a “fit for purpose” privacy framework.

THE RECOMMENDATIONS

An overview of the six recommendations is outlined below.

A right of personal information portability

A right of data portability would allow an individual to request that an agency holding the individual's personal information provide that information to the individual in a suitable electronic format that can be shared by that

---

1 Section 26 of the Privacy Act 1993.
individual. The Privacy Commissioner gives the example of a Facebook user being able to download a zip-file archive of the user’s Facebook history (including transaction data for purchases made through Facebook and details of deleted friends).

The concept of data portability has been compared to the concept of number portability that applies under telecommunications regulation, and facilitates the switching of service providers. A right of data portability would similarly facilitate switching of application or cloud service providers. It could also apply to service providers such as banks, telecommunications companies and internet service providers who maintain transaction histories for customers. Customers could also require the data to be provided in a usable form and transfer it to a competing business. Customers could also require the current service provider to transmit the data direct to a new service provider.

This recommendation is in line with the GDPR right to personal information portability. The Privacy Commissioner recommends the adoption of a right that is interoperable with the GDPR. The GDPR purports to apply to businesses outside of the European Union who process personal information of EU residents (such as New Zealand businesses selling into the EU). Adopting an interoperable approach to the GDPR is also desirable from the perspective of New Zealand maintaining its current EU adequacy status.2

Controls on the re-identification of anonymised data

The Privacy Commissioner has noted that there can be a compelling public interest in utilising data analytics, but this depends on maintaining public trust and confidence. This in turn is often based on a belief that the data is anonymised and the individuals concerned will not be able to be re-identified. The Act allows for the use and disclosure of de-identified data but does not explicitly prohibit re-identification of individuals - the Privacy Commissioner sees this as a gap in the Act that risks undermining public confidence in the robustness of de-identified datasets.

The recommendation is for adoption of a new privacy principle that limits the re-identification of previously de-identified or anonymised personal information, except in limited circumstances.

Also recommended is clarification of the obligations on agencies in relation to de-identifying datasets, such as taking reasonable precautions to limit identification, and the potential for the Privacy Commissioner to issue guidance on what this may involve.

Power for the Privacy Commissioner to require demonstration of compliance With the Act

The Privacy Commissioner recommends giving him the power to require an agency to demonstrate its ongoing compliance with the Act by:

• establishing a privacy management programme or plan that is adequate for the agency’s purposes;
• requiring a report to the Privacy Commissioner on steps taken to achieve compliance with that requirement; and/or
• publicly reporting on its position with regard to its privacy management programme.

It is proposed that the power would be discretionary and used only in limited cases such as where there is suspicion of a risk to privacy by certain practices, or as a result of the volume or nature of the personal information held by an agency.

The Privacy Commissioner sees this power as an alternative to mandatory audit powers that the Law Commission had recommended, but which the Government has not has accepted. The Privacy Commissioner believes this power will allow him to proactively address significant gaps and weaknesses in privacy practices, and mitigate the risk of future breaches, as opposed to only dealing with issues on a reactive basis.

Civil penalties of up to $1 million

The Privacy Commissioner recommends that he have the ability to apply to the High Court for civil penalties in the case of serious breaches. In the case of corporates this could involve fines of up to $1 million, and for individuals it would be up to $100,000.

Currently a breach of the Act that results in the interference with the privacy of an individual can be addressed in proceedings being brought before the Human Rights Review Tribunal by either the Director of Human Rights Proceedings or by aggrieved individuals.3 The Act also contains criminal offences that penalise a failure to comply with any lawful requirement of the Privacy Commissioner (with fines set as low as $2,000 or $10,000).4 But, there are no generic penalties to incentivise compliance with the Act. The Privacy Commissioner considers the only practical option it has available to deter significant privacy breaches is to report on them publically.

In comparison fines are a feature of laws in other jurisdictions. Under the Australian privacy law the Australian Information Commissioner can seek civil penalties of up to AUD1.7 million for corporations and AUD$340,000 for

---

2 New Zealand has been formally recognised by the European Commission as having privacy laws that provide an adequate level of data protection under the existing European Union Directive relating to the processing of personal data (Directive 95/46/EC). This means that European companies can transfer personal data to New Zealand for processing without the need for special additional matters being taken. New Zealand is one of only five countries outside Europe to hold this status.

3 Section 82 of the Act.

4 Section 127(b) of the Act.
individuals. In the United Kingdom, the Information Commissioner can impose fines of up to £500,000. Under the GDPR the most serious breaches can result in fines of up to €20 million or 4% of global annual turnover. For less serious breaches the fines under the GDPR can be up to €10 million or 2% of global annual turnover. The GDPR allows privacy regulators to impose the fines directly.

Reforming criminal offences for obstructing the Commissioner

Under section 127(a) and (b) of the Act, it is an offence to:

- *without reasonable excuse*, obstruct, hinder, or resist the Privacy Commissioner in the exercise of powers under the Act; or
- *without reasonable excuse*, refuse or fail to comply with any lawful requirement of the Privacy Commissioner.

The Privacy Commissioner’s experience has been that the “reasonable excuse” defence has been problematic in that it has been used by agencies to obstruct or fail to comply with requirements of his office in relation to investigations.

The Privacy Commissioner therefore recommends recasting the offences as strict liability. Alternatives would be to replace the “reasonable excuse” defence with the higher threshold of “lawful justification or excuse”, or to give the Privacy Commissioner the ability to seek a pecuniary penalty for such offences.

This recommendation is in line with the Privacy Commissioner’s position that the Privacy Commissioner should be given greater investigative tools by incentivising cooperation from agencies and deterring potential obstructive behaviour.

Reforming the public register privacy principles

The Privacy Commissioner recommends an overhaul of the public register privacy principles in Part 7 of the Act. Public registers are registers or databases to which the public has rights of access, such as the electoral roll, the land titles register and the companies office register.

The Privacy Commissioner notes that the public register privacy principles were developed at a time when the registers were kept primarily in paper form and are now largely ineffective. The Privacy Commissioner considers relevant privacy safeguards can be addressed in the statutes under which the registers are established - his office is consulted on proposed amendments to these statutes.

He recommends:

- the suppression of personal information in public registers in appropriate circumstances, where there is a safety risk, by way of application to the Privacy Commissioner; and
- allowing complaints to the Privacy Commissioner in relation to breaches of the access conditions provided in the relevant public register enactment.

The Privacy Commissioner also recommends expanding the functions of the Privacy Commissioner to review any public register and to report recommended amendments to the relevant statute that may be necessary to protect (or better protect) the privacy of individuals.

WHAT NEXT?

The Act requires the Minister of Justice, as responsible Minister under the Act, to lay a copy of the report before Parliament once it has been issued. Given that new privacy legislation is in the pipeline we expect that the Privacy Commissioner’s report and recommendations will need to be considered in the context of any new legislation.

In 2014 the Government confirmed its intent to replace the Act with new privacy legislation and some of the key reforms that would be adopted. In May 2016, Minister Amy Adams indicated her intent to introduce a new Privacy Bill into Parliament in 2017 (after targeted consultation and comment by privacy experts).

At this stage there is no clearer indication as to when the draft legislation will become publically available, or whether the recent election date announcement will affect its introduction into Parliament. What is clear, however, is that the expansion of all things digital will continue to challenge the application and effectiveness of the current Act.

The Privacy Commissioner’s review and recommendations illustrate how privacy considerations are relevant in the context of developments in technology, data analytics, customer trust and confidence, and cyber security. Whether all of his recommendations should be adopted will inevitably be the subject of debate.

On one hand the recommendations raise the prospect of additional compliance burdens on businesses with the associated costs, and the powers sought by the Privacy Commissioner could be far reaching. If the recommended powers are granted, it is doubtless that close attention will be given to the parameters of those powers and the instances in which they can be exercised.

On the other hand, the recommendations are focussed on modernising the Privacy Act to better accommodate the significant developments in technology and data science, and the changes in the way we interact with each other on a business and social level. The recommendations are also consistent with measures being adopted internationally that New Zealand businesses operating on the global market will be subject to in any case. There is also the risk that if New Zealand does not take steps to modernise and update its privacy laws, we will fall behind international best practice.

---

6 https://www.beehive.govt.nz/speech/opening-address-wellington-privacy-forum