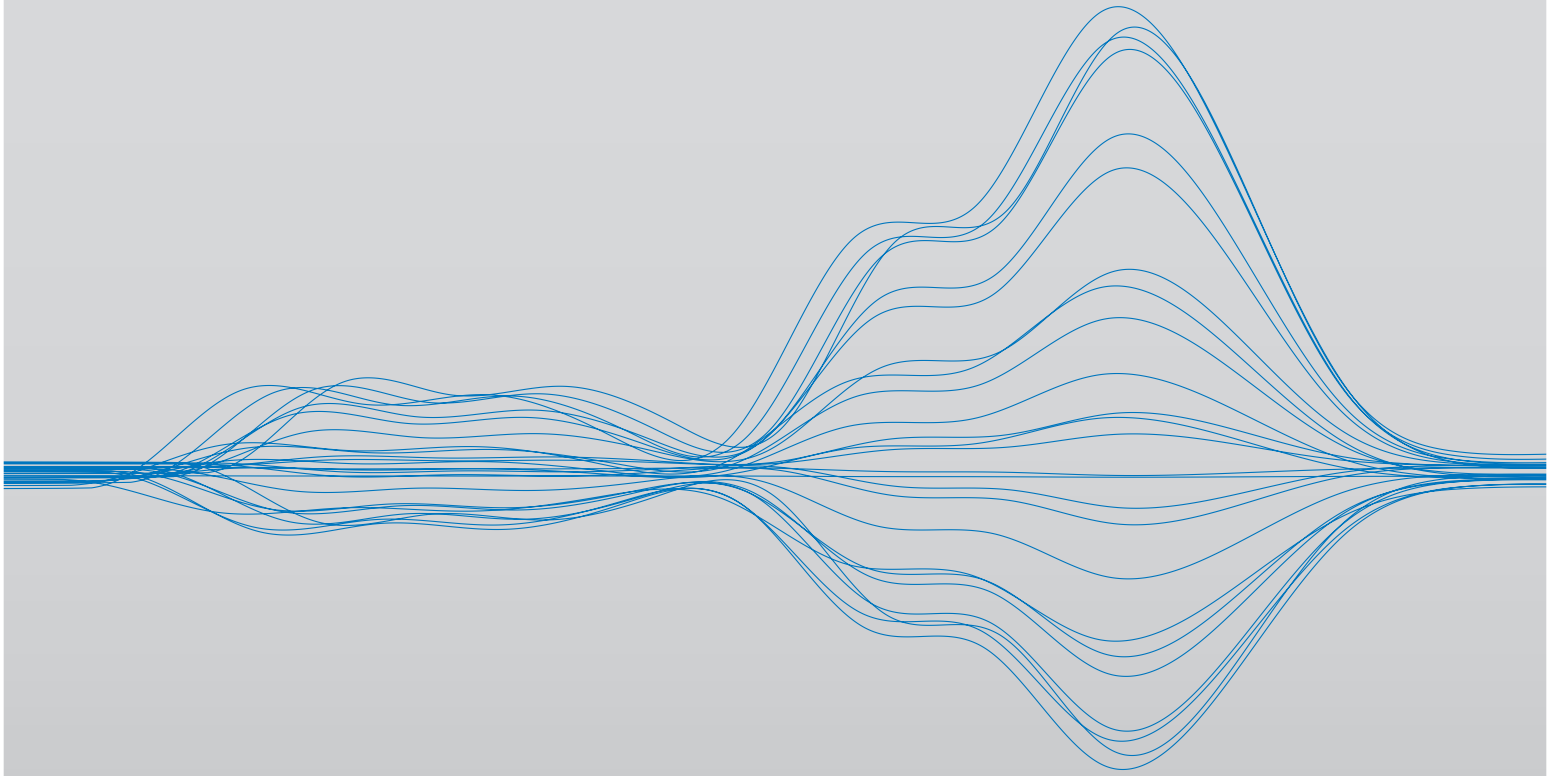
DATA PROTECTION GROUP

Practical Global Privacy



Fitting into the global picture:
Data privacy in Australia and New Zealand

DLA PIPER

Fitting into the global picture: Data privacy in Australia and New Zealand

Attitudes to data protection in Australia and New Zealand (ANZ) are changing.

Traditionally, the prevailing cultural mindset surrounding data privacy has been relaxed compared to elsewhere in the world. But data scandals have made Australians and New Zealanders more sensitive to what happens to their information.

The Cambridge Analytica case caused ripples, but then slipped from the memory of many consumers. Then came the Optus breach, which was more like a tidal wave, and will take longer to forget. The attack affected ten million consumers in Australia – around 40% of the population – driving calls for reform of the country's data protection legislation.

There are concerns about how much information is being collected and stored by businesses, why, and for how long. A topic that was once reserved for lawyers and compliance teams has become the subject of newspaper headlines. That's driving a debate about whether to impose clearer limits on what data organizations may gather, and how long they may hold it for.

Since the Optus incident, the beginning of a cultural shift can be seen. There's a move towards recognising an individual's data as their property, not that of a business that holds it. This echoes the concepts of personal control and ownership of data embodied in the European Union's GDPR.

Similarly, the length of time for which businesses may retain consumer data is also being questioned, setting the scene for a GDPR-style right to be forgotten.

Reform is taking shape, and gathering momentum. Australia has announced plans to introduce new cyber-focused legislation and increase the penalties for breaches. And it has accelerated a wider review of the Privacy Act. To what extent New Zealand may follow suit isn't yet known. But it's reasonable to assume that the country's legislators are monitoring developments closely.

Wherever reform takes ANZ's data privacy landscape, for now, the countries share a parallel approach to data privacy regulation and policy. Their legislative frameworks are underpinned by similar principles and intended outcomes.

New Zealand's Privacy Act 1993 came in just four years after Australia's, in 1988, and introduced many of the same rules and provisions. New Zealand's legislation was then replaced by the Privacy Act 2020, but the similarities remain.

There are some differences between the regimes. But businesses can be confident that complying with one goes a long way to complying with the other. That's why firms operating in both countries tend to manage data compliance on an "ANZ basis".

So against this changing backdrop, what should data compliance teams know about the region's privacy rules, and the direction in which they may be heading?

A look at the main principles

Both countries' Privacy Acts are based on flexible principles, not prescriptive requirements. And in both cases, the primary authority for processing personal information is based on business interest, rather than individual consent.

- *Principles-based legislation*

Instead of taking a prescriptive approach like the GDPR, the Acts set broad principles for companies to follow. These are designed to be flexible in how they apply to different types of information and organizations; and how the national regulators interpret and enforce them. For example, both Acts require various measures to be implemented that are "reasonable" in the circumstances. What's reasonable is deliberately flexible. In Australia, a higher standard is required for sensitive personal information, where the risk of misuse is greater.

- *Business interest*

As a rule, businesses don't need individuals' consent to collect and process personal data in ANZ, unlike in other regions. They require only a legitimate business reason for doing so. Personal data must be used for a necessary function or activity of the organization, or a sufficiently connected purpose.

Overall, this isn't a particularly pro-consumer approach. As reforms progress, we may see growing pressure for that balance to change.

In addition, it has made for a less interventionist approach from ANZ's regulators until now, compared to many countries. Though that too may be about to change, in Australia at least (see below).

"A less interventionist approach to data protection in ANZ reflects local attitudes – though these are rapidly shifting."

Comparing and contrasting with GDPR

As well as its principles-based approach, ANZ's data protection legislation is different to the GDPR in several ways. In the past, these may not have seemed too significant. But as attitudes evolve, some of their more pro-business settings may come into focus.

Data subjects' rights are more limited than in Europe. Individuals can only access and correct the information that organizations hold on them. GDPR, by contrast, contains other data-subject rights, including erasure and objection.

Data-transfer rules are another area of divergence– and one where Australia and New Zealand's laws differ from each other.

Australia's Privacy Act has a much more relaxed data-transfer regime than Europe or New Zealand. Prescriptive data-transfer agreements aren't required; a binding obligation for data recipients to comply with the Australian regime is all that's necessary.

In New Zealand, companies are barred from disclosing personal information to a foreign person or entity, except when:

- the data subject authorizes the disclosure. Before doing so, they must be informed that the foreign recipient may not be obliged to protect their data to standards comparable to those in the Privacy Act.
- the disclosing organization reasonably believes that the recipient ***is*** required to protect personal data to standards comparable to the Privacy Act. That may be because legislation in the foreign recipient's jurisdiction is comparable, or due to contractual obligations between the discloser and recipient.

New Zealand's Privacy Commissioner has published model contractual clauses for this purpose. But unlike the GDPR's standard clauses, their use isn't mandatory.

The pro-business approach to privacy laws is changing in ANZ. Businesses will need to balance competing interests as the laws change. They'll want to maximize the commercial value of the data they collect. But they must also meet shifting consumer expectations around the use of personal data.

"Businesses must balance competing interests: commercializing data, while meeting consumer expectations."

Enforcement is changing

Until recently, data protection regulators in ANZ have taken a restrained approach to enforcement.

Enforcement actions are less frequent than in many parts of the world – particularly Europe, where multi-million-euro fines are now common. While the Office of the Australian Information Commissioner (OAIC) awards compensation, usually in the low thousands, it has not yet successfully sought to impose higher civil penalties.

This restrained approach is partly because the legislation in the region lacks strong penalties. Maximum fines are only AUD2.2 million in Australia (though set to rise), and just NZD10,000 in New Zealand.

Beyond fines, regulators have few powers to sanction organizations, other than naming and shaming those that don't comply. New Zealand has a statutory mechanism for data subjects to bring legal action, including class actions, in the Human Rights Review Tribunal. This can result in a range of sanctions, including damages awards. However, there have been no significant damages awards to date.

In practice, the regulators have focused on conciliation and mediation – New Zealand's regulator being required to do so in the first instance. The Privacy Act obliges the Office of the Privacy Commissioner to seek either:

- a settlement of privacy complaints
- an assurance that the alleged conduct won't be repeated.

"Data regulators in Australia and New Zealand have focused on concilation and mediation rather than enforcement."

As a result, businesses can't rely on risk-based compliance, informed by regulators' previous decisions. Official guidance is the best they have to go on.

That's not to suggest they should carry on regardless because fines for non-compliance will be limited. In Australia, at least, other regulators are stepping into the enforcement gap – and at times imposing hefty financial penalties:

- The Australian Competition and Consumer Commission (ACCC) recently settled a consumer law case with Google for AUD60 million. The sanction was for how Google had collected location data.
- The Foreign Investment Review Board has imposed data-sovereignty restrictions on transactions where the target company's assets include large volumes of data, or data that's sensitive or commercially valuable.

Reform is gathering pace

Both Australia and New Zealand have been refreshing their data privacy regimes. In both cases, it's proving a slow process – but momentum is building.

High profile data breaches like Optus and, more recently, Medibank, have upped the political and public desire for reform. Less than five weeks after the Optus incident, Australia plans to introduce legislation to increase penalties for breaches of the Privacy Act.

"The political and public desire for privacy reform is growing in the wake of high-profile data breaches."

NEW ZEALAND

New Zealand updated its data protection legislation in 2020, though the regime remains generally consistent with Australia's.

The reform followed multiple reviews, which took place over 23 years. During that time, there were calls to strengthen privacy protections and enforcement powers – not least to maintain the country's adequacy decision from the EU.

Some demanded stronger data-subject rights and a higher standard of protection for sensitive information – the concept of sensitive information doesn't exist in the Privacy Act.

Ultimately, though, the overhaul brought only minor changes.

As part of its regular review of New Zealand's adequacy status, the European Commission recently expressed concerns over a lack of transparency of indirect data collection. In response, the government has decided in principle to amend the Privacy Act. It's now carrying out a public consultation on how to do so.

AUSTRALIA

In 2019, the ACCC published a report on digital platform businesses. It highlighted weaknesses in the country's data protection laws when it came to regulating big tech.

A review began the same year, but wasn't complete come the change of administration in 2022. The incoming Attorney-General, Mark Dreyfus, signalled his intention to complete the review, and perhaps go further than originally anticipated – possibly with the public response to the Optus breach in mind.

The Privacy Act Review discussion paper, released in October 2021, explored the possibility of increasing the enforcement powers of the OAIC. Any change to the Privacy Act is likely to have this effect.

Ultimately, though, how far reform will go remains to be seen. Initially, many commentators expected little more than add-ons and adaptations, rather than fundamental change. But given the reaction to Optus, faster and more extensive reform could now be incoming.

An increase in the maximum fine for breaching the rules – to AUD10 million – was proposed in 2021. The same Bill included a framework for an online privacy code for large online providers. The detailed content of this code wasn't proposed, but the focus was on improving transparency for consumers, and addressing some of the perceived issues caused by big tech.

This has been superseded in part by the response to the Optus breach. The government will now seek to increase the maximum penalty to the greater of:

- AUD50 million
- three times the value of any benefit obtained through the misuse of information
- 30% of a company's adjusted turnover for the relevant period.

Whether or not the online privacy code will also be pursued remains to be seen.

Other potential reforms include removing exemptions in the Privacy Act for employee records, and for companies with under AUD3 million annual turnover.

Finally, the government is considering a statutory tort of privacy. This would give a much-needed direct remedy for privacy breaches to individuals, who may only complain as things stand. And it would open the door to widespread class actions.

That would significantly tip the balance of data protection in consumers' favour. We wait to see how far the government is willing to go. Again, Optus, and the public reaction to the breach, may come into its thinking here.

The power of three

With consumer demands changing, and legal reform on the horizon, there's never been a better time to review and strengthen your data compliance controls and processes.

This will typically involve three vital steps:

1. MAP YOUR DATA

Businesses often lack a holistic view of their data-gathering and processing activities. Each division will typically have visibility only of its own data.

Yet compliance won't be possible without transparency across the whole organization. So make sure you've mapped and documented all your data-processing activities – including:

- the key datasets you collect in each function
- all of the points where you collect data
- where data is stored
- how you're collecting, processing, using and disclosing data
- the reasons why you're doing so

2. DESIGN YOUR PROGRAM

Based on the results of your mapping exercise, design your compliance program to address:

- any risks in your data systems and processes
- any gaps in your data policies and controls

Are you providing all the required notices to consumers? Are you securing all necessary consents? Do any of the datasets you're collecting need additional security measures? Are you disclosing any data unnecessarily? Are you retaining data for longer than necessary?

3. TRAIN YOUR PEOPLE

An organisation is only as good as its people. So you'll need to conduct data privacy training across the company, to embed awareness of the organization's data processing obligations under ANZ law. This will also help break down silos between business units where data is concerned.

All staff should receive basic training, such as on the data policies they need to follow. More extensive training will be needed for employees with high exposure to personal information, like those in the HR and marketing teams.

Our Data Protection, Privacy and Security team can help you to optimize your data protection compliance in the ANZ region. Get in touch to discuss how we can support your business.

Sarah Birkett
Senior Associate
Melbourne
T +61 3 9274 5464
sarah.birkett@dlapiper.com

Nicholas Boyle
Partner
Sydney
T +61 2 9286 8479
nicholas.boyle@dlapiper.com

Nick Valentine
Partner
Auckland
T +64 9 916 3703
nick.valentine@dlapiper.com

James Clark
Senior Associate
Leeds
T +44 2073 490 296
james.clark@dlapiper.com