PRIVACY REFORM IS HERE: IT'S TIME TO GET YOUR HOUSE IN ORDER!

Date: 6 March 2023

Australia Corporate Alert

By: Cameron Abbott, Rob Pulham, Stephanie Mayhew

WHAT YOU NEED TO KNOW

Following a number of high-profile cyber incidents last year, the Australian Government (the Government) is proving that privacy is a serious issue that corporations need to face. Recently, we saw the enactment of the *Privacy Legislation Amendment (Enforcement and Other Measures) Amendment Act 2022* (Cth) (Enforcement Act). This expanded the extraterritorial application of the Privacy Act, increased the maximum civil penalty for a serious or repeated interference with the privacy of an individual, and expanded the investigation and enforcement powers of the Office of the Australian Information Commissioner (OAIC).

We knew more reform was on the horizon, with the Attorney General's Department still to release its long awaited Privacy Act Review Report and on 16 February 2023 (the day after we presented to 250 people on privacy reform), the Government released its report into the review of the *Privacy Act 1988* (Cth) (Privacy Act).

WHAT DOES THIS MEAN?

The Enforcement Act signals a move toward more active enforcement activities by the OAIC and ultimately to greater legal risk for corporations in Australia that suffer data breaches. It ultimately closes some of the gaps the OAIC was faced with when dealing with the recent Australian cyber incidents.

The Review Report indicates that Australia is trying to adapt its privacy regime to follow more European style privacy laws. The Report makes 116 proposals with an aim to improve the privacy rights of individuals, clarify the privacy responsibilities of APP entities and enhance the OAIC's powers. All agencies and organisations, including small businesses, will be affected.

WHAT'S NEXT?

The Government is seeking feedback to the Review Report by 31 March 2023 (access the Report here). While we don't have an exact timeframe, we anticipate the review will be finalised towards the end of the first half of 2023. All businesses therefore need to prepare themselves for the proposed reforms and ensure they have their 'house in order' to streamline such changes.

THE ENFORCEMENT ACT

The biggest result from the Enforcement Act is the increase to maximum penalties. The increased penalties mirror recent increases to the maximum penalties under the *Competition and Consumer Act 2010* (Cth) that were introduced through the *Treasury Laws Amendment (More Competition, Better Prices) Act 2022* (Cth).

For organisations, this increases the penalty from the current AU$2.22 million (per contravention) to whichever is the greater of:

- AU$50 million;
- If the court can determine the value of the benefit that the body corporate, and any related body corporate, have obtained directly or indirectly and that is reasonably attributable to the conduct constituting the contravention—three times the value of that benefit; and
- If the court cannot determine the value of that benefit—30% of the adjusted turnover of the body corporate during the breach turnover period for the contravention.

These changes ensure penalties under the Privacy Act are comparable with those of other domestic and international regulators. Keep in mind that the increased penalty regime does not apply to all data breaches. Just because an organisation has suffered a data breach does not mean it has breached the Act. In the case of APP11.1, it remains the case that the organisation must have failed to take reasonable steps in the circumstances to secure personal information, in order for there to be a breach of APP 11.1. This stresses the importance of ensuring you are well prepared.

THE REVIEW REPORT

The Privacy Act Review aimed to investigate the effectiveness of Australia's current data privacy protection regime. Following the publication of an issues paper in October 2020, a discussion paper in October 2021 and several rounds of public consultation, the long awaited Report has been released.

The Report describes 116 proposals and is marked as being subject to further consultation. Some of our top issues if all the proposals were implemented are discussed below.

Broader definition of personal information

The definition of personal information will be expanded from information "about" an individual to information that "relates to" an individual. It is also proposed that any inferred or generated information will be deemed to have been 'collected' within the meaning of the Privacy Act.

Narrower exemptions and applying the Privacy Act to all small businesses

The small business exemption will be phased out until removed entirely. The employee records exemption will be narrowed, with increased obligation in respect of employees including a requirement to notify staff and the OAIC of data breaches affecting employee personal information.

Greater consent requirements

The OAIC's current guidance that consent must be voluntary, informed, current, specific and unambiguous will be included within the Privacy Act. It has also been put forward that there be specific requirements around an individual's ability to withdraw consent.

Greater collection requirements

Collection statements (current APP 5 notification) will be required to be clear, up-to-date, concise and understandable. Privacy policies will also be required to include more details about an entity's information handling practices including listing the entity's retention periods. There is potential for 'standard form' policies and notices to be required.

Personal information handling practices must be 'fair and reasonable'

The introduction of an objective test is that collection, use or disclosure of personal information must be fair and reasonable in the circumstances. The test will require consideration of a number of factors that range from how an individual would expect their personal information to be handled to whether the impact of privacy is proportionate to the benefit to collecting the information.

More individual privacy rights

This includes the right to erasure and the right to object to collection, use or disclosure of personal information.

Automated decision-making

Information about automated decision-making will need to be included in entities' privacy policies and individuals will be given the right to request meaningful information about how automated decisions with substantial legal or similarly significant effects are made.

Enhanced OAIC powers and more penalties

There's still more to come in addition to the Amendment Act on this front. Further powers will be given to the OAIC with the OAIC, Federal Court and Federal Circuit and Family Court of Australia all being allocated powers in respect of civil penalties. The threshold for a "serious" privacy breach is also lowered and it will no longer be required that a breach be a "repeated" interference.

Direct rights of action

Individuals will be given a direct right of action to allow them to apply directly to the Federal Court where they have suffered loss or damage as a result of a privacy interference by an APP entity.

Statutory tort for serious breaches of privacy

A statutory tort for privacy will see the recommended model from the Australian Law Reform Commission 2014 report serious invasions of privacy in a digital era implemented.

Privacy impact assessments

Currently, agencies are only required to undertake a Privacy Impact Assessment (PIA) for high risk privacy activities. This obligation will now extend to all APP entities. Emerging technology, such as facial recognition and biometric technology, may also face additional regulation.

KEY WAYS TO 'GET YOUR HOUSE IN ORDER'

Our best tips for basic privacy compliance:

- *Stocktake* – information holdings – understand your information assets and system environments;
- *Downsize* – information holdings – need to have vs nice to have (at collection and data retention stages);

- *Update* – privacy policy/collection statements/all relevant policies;
- *Secure* – current security measures, keep up to date with latest OAIC lessons;
- *Promote* – embed a strong privacy culture throughout your organisation; and
- *Monitor* – make sure you stay up-to-date with the latest developments, advice from regulators, and major contributors to other breaches.

KEY CONTACTS

CAMERON ABBOTT
PARTNER

MELBOURNE
+61.3.9640.4261
CAMERON.ABBOTT@KLGATES.COM

ROB PULHAM
SPECIAL COUNSEL

MELBOURNE
+61.3.9640.4414
ROB.PULHAM@KLGATES.COM

STEPHANIE MAYHEW
LAWYER

SYDNEY
+61.2.9513.2371
STEPHANIE.MAYHEW@KLGATES.COM

