April 2023

Commercial Insights

Are the Australian Privacy Reforms on your radar?

The Australian privacy landscape is changing.

In December 2022, amendments came into force to amend the *Privacy Act 1998* (Cth) (the **Privacy Act**) to increase the maximum penalties related to serious and repeated breaches of the Australian Privacy Principles (the **APPs**) and the Notifiable Data Breaches Scheme. As a result of these amendments, the maximum civil penalty for serious or repeated interferences with privacy increased from the previous $2.20 million to an amount that is the greater of $50 million, three times the value of any benefit obtained from the conduct or 30% of an entity's adjusted turnover in the relevant period.

Further changes are expected within this term of parliament with the Attorney-General's Department issuing a detailed report on its review of the Privacy Act in February 2023 (the **Report**). The Report sets out 116 recommendations, many of which are significant and if implemented, will impact your business.

The reforms in the Report are aimed at strengthening the protection of personal information and the controls individuals have over their personal information. Strong privacy protections are sought to support continued digital innovation and enhance Australia's reputation as a trusted trading partner.

Of the proposals contained in the Report, key reforms include:

- **Expanding the definition of Personal Information**: The current definition of personal information captures information *'about'* an individual that is identified or reasonably identifiable. Consequently if no individual is identifiable or reasonably identifiable from the information, the Privacy Act will not apply. The Report recommends expanding the definition of personal information by replacing the word *'about'* with *'relates to'*. Consequently the amended definition will capture online and technical information (such as metadata including IP addresses and location data) and inferred information (such as predictions of behaviour and preferences). To be captured by the Privacy Act, the information will still need be connected to a specific individual.
- **Removal of the small business exemption**: As it currently stands the Privacy Act regulates how Australian Government agencies and organisations with an annual turnover of more than $3 million, and some other organisations (including organisations that provide a health service or hold health information), handle personal information. The Report recommends that the Privacy Act be extended to apply to personal information handled by small businesses, which are currently exempt from the Act.
- **Removal of employee records exemption**: As it currently stands a private sector employer's handling of records in relation to current and former employment relationships is exempt from the APPs in certain circumstances. The Report recommends that enhanced privacy protections should be extended to

private sector employees. However, it does not propose the removal of this employee records exemption entirely.

- **Introduces that individual consent is required regarding geolocation tracking data**: The Report suggests that the collection, use and storage of geolocation data requires consent.
- **Amends the definition of Consent**: Consent will only be valid if it is voluntary, informed, current, specific and unambiguous, and must be capable of being withdrawn.
- **Introduces strengthened notice requirements for businesses collecting personal information**: Currently, entities regulated by the Privacy Act are required to notify individuals of the collection of personal information, governed by APP 5. The Report recommends that the privacy collection notice mandatorily include express disclosure if an individual's information is to be collected, used or disclosed for a high privacy risk activity. That is, an activity which is likely to have significant impact on the privacy of an individual. It is understood that the OAIC will publish guidance on what may indicate an activity is high risk.
- **Introduces mandatory Privacy Impact Assessments**: The Report proposes that entities be mandatorily required to undertake privacy impact assessments to identify and mitigate risks before engaging in any high risk privacy activities. While mandatory privacy impact assessments already exist in the public sector and have long been considered best practice in the private sector, making privacy impact assessments mandatory for the private sector emphasises the increased accountability and scrutiny the amendments are intended to have on the private sector. It is also proposed that the OAIC can request production of the privacy impact assessment.
- **Increased record-keeping obligations**: businesses are required to keep records of the primary purposes for which they will collect, use and disclose personal information and this should reflect what is set out in the relevant privacy collection notice. If the business wants to subsequently use or disclose that information for a secondary purpose, it must also make a record of that secondary purpose prior to or at the time the information is used or disclosed.
- **Introduces the requirement to act fairly and reasonably:** under the current Privacy Act, a business is required to consider whether the collection of personal information is reasonably necessary for the entity's functions or activities. The proposal to introduce a fair and reasonable test is to be used to determine whether the collection, use and disclosure of personal information is fair and reasonable in the circumstances. This is an objective test and places a positive obligation on the entity that collects and uses the personal information to ensure its practices are fair and reasonable. This test will apply regardless of any consent provided. Practically, and importantly, this means that inappropriate collection and use of personal information cannot be cured by seeking consent of the individual concerned.
- **Introduces new access rights for individuals**: The Report proposes to provide individuals with greater transparency and control over their personal information, including by introducing:
  - a right to access personal information that relates to them and to request and receive an explanation of how the business collected that information and what it is used for
  - a right to object to the collection, use and disclosure of their personal information
  - a right to erasure. That is, an individual can request their personal information is permanently erased. De-identifying data in response to this request will not be sufficient. The Report suggests introducing a 30-day window for businesses to comply with all deletion requests that relate to

individuals. If a data deletion request is received, the entity is also required within this 30-day timeframe to inform any third parties to whom the personal information has been disclosed of the deletion request, and

- a right to have internet search results about them de-indexed and to correct personal information published in online publications.

- **Introduces obligations around de-identified information**: The Report recognises that de-identified data is subject to risks of re-identification and introduces a criminal offence for malicious re-identification of de-identified information with intent to harm another or obtain an illegitimate benefit. The Report also proposes extending:
  - APP 11.1 to protect not only personal information but also de-identified information from unauthorised access or interference, and
  - APP 8 to take steps reasonable in the circumstances to ensure overseas recipients with access to de-identified data sets do not breach the APPs.
- **Entities are transparent on data retention**: The Report proposes changes to data retention requirements so that entities must establish minimum and maximum data retention periods and that these time periods are clearly set out in the organisation's privacy policy.
- **Revises the notification timeline for reporting eligible data breaches to the OAIC**: The Report proposes that the deadline for reporting eligible data breaches to the OAIC will be reduced to 72 hours from when an organisation becomes aware that there are reasonable grounds to believe an eligible data breach has occurred. Impacted individuals must be notified 'as soon as practicable'. This tightens the existing obligations that allow an entity a 30-day period to make an assessment of the suspected breach.

In addition to the above, there are numerous other proposals contained in the Report, including to:

- increase regulatory powers
- provide individuals with a direct right of action to enforce their privacy rights
- introduce concepts of 'processors' and 'controllers' of personal information
- regulate the use of personal information in automated decision making
- regulate targeted advertising
- introduce additional protections for children and vulnerable persons, and
- introduce a statutory tort of privacy.

The world has become increasingly connected and information flows more complex. The Report does not include any draft language for legislative change. However, it is anticipated that an exposure draft of the new legislation will be before parliament in the current term.

Of course, the Report is just that – it is not enshrined law. However, it is clear that recent significant data breaches and the media attention they have received have accelerated changes in community expectations regarding privacy protection and cyber security more generally. We anticipate that in this environment many of the Report's proposals will be adopted and businesses will need to make substantial changes to the ways in which they interact with individuals and handle personal information in order to comply with the Privacy Act once amended.

April 2023

What can you do now?

There are some housekeeping steps you can take now in preparing for the introduction of the privacy reforms. We recommend that you undertake a review of your business's current privacy practices and thoroughly audit and understand the personal information that your business collects, holds, uses and discloses. For example:

- What personal information does your business collect and hold? Do you collect more personal information than your business needs in order to provide the goods or services that you provide to your customers? How long do you retain the information? How long should you retain it?
- Do you still need the personal information your business holds for the primary purpose for which it was collected? If not, now would be an opportune time to delete it.
- For what primary purpose was that personal information collected?
- Do you use personal information for other, secondary, purposes and are those secondary purposes fair and reasonable?
- Has the personal information that your business holds been collected directly from the individual? Has your business shared that personal information with a related body corporate or a third party?
- What controls and assessments do you have in place for proposed new projects which involve the collection of personal information? Do you conduct privacy impact assessments?
- Do you have records matching data sets to consents or privacy collection notices that clearly state the primary purpose for collection?
- Do you have a data breach response plan in place to allow you to respond to any suspected data breach without delay?

Further Resources

The most recent report on the Privacy Act Review published by the Attorney-General's department on 16 February 2023 is available here.

Meridian Lawyers has experience advising clients on their privacy and data security obligations, including managing responses to data breaches and developing privacy training materials. If you have any questions about your current obligations regarding the collection, use, handling or storage of personal information in Australia or steps you can be taking in advance of the introduction of the revised privacy laws, please contact Special Counsel Hayley Bowman or Principal Mark Fitzgerald.

Hayley Bowman
Special Counsel
+61 3 9810 6723
hbowman@meridianlawyers.com.au

Mark Fitzgerald
Principal
+61 3 9810 6767
mfitzgerald@meridianlawyers.com.au