protiviti®
Global Business Consulting

Privacy Act 1988 Review: A Compliance Burden or Welcome Change?

It has been more than two years since the Attorney-General's Department announced[i] it would be undertaking a review of the *Privacy Act 1988*. The review will likely result in the most substantial amendment to the Act since what we now know as the Australian Privacy Principles (APPs) were introduced in 2000. The objective of the review "*will consider whether the scope of the Privacy Act 1988 and its enforcement mechanisms remain fit for purpose*". Notable areas under consideration for reform in the review's Terms of Reference[ii] include:

- The definition of 'personal information';
- Current exemptions;
- Erasure/deletion of personal information;
- The impact and effectiveness of the notifiable data breach scheme; and
- The feasibility of an independent certification scheme for organisations to demonstrate compliance with Australian privacy laws.

What has happened since

The review was initially scheduled to commence in October 2020 but has experienced delays. Following the Department's invitation for submissions in response to a published issues paper[iii], the volume of interest and responses has been positive with many notable organisations providing feedback and opinions on areas of the current Act for reform. By the close of submissions, the department had received responses from private sector organisations such as Facebook, Atlassian and Google, as well as public sector agencies, academics and research centres, and even the Office of the Australian Information Commissioner (OAIC) itself.

Following a review of submissions received, the Department published a Discussion Paper[iv] in late-October 2021. The Discussion Paper sets forth a number of proposed amendments to the Act. The Department is now requesting responses to the Discussion Paper and the proposed amendments, seeking "*more specific feedback on preliminary outcomes, including any possible options for reform*".

What is going to change

The Attorney-General's Department's Discussion Paper has proposed reforms to the Act in three key areas:

1. Scope and application of the Privacy Act 1988;
2. Protections afforded to individuals and their personal information; and
3. Regulation of the Act and enforcement powers.

Scope and Application of the Privacy Act 1988

Some of the proposed areas for reform regarding the Act's scope and application include:

- Broadening the definition of *personal information* to include technical and inferred information, as well as including a supporting example list of types of information. Such broadening of the definition may bring certain types of cookies collected on websites into the scope of the Act, for example.

- Removing or amending the employee records exemption. Currently, personal information collected and used by an organisation related to its employment relationship with an individual is exempt from the Act. The proposed reform to remove or modify the exemption would see organisations' compliance obligations increase, particularly in respect of personal information collected and used by their Human Resource functions, for example.

Protections

This is the biggest discussion point of the paper and area for proposed reform. Areas being considered for reform include:

- Revising security and personal information retention and destruction requirements under the Act. The Government has committed to clarifying cyber security requirements for Australian businesses as part of Australia's Cyber Security Strategy 2020, and it is anticipated an APP code will be developed to supplement current security requirements set forth by the Act. Interestingly, contributors to the discussion paper have recommended expanding personal information security requirements in the Act to include requirements from regulations and frameworks such as the EU General Data Protection Regulation (GDPR), Australian Prudential Regulation Authority's (APRA) CPS234 (Information Security), and the Australian Signals Directorate's *Essential Eight*.

- Revising and expanding the requirements of APP 1 and APP 5 to standardise privacy notices and clearly specify when and how privacy notices should be provided. The proposed reform considers GDPR privacy notice requirements and promotes standardised wording, layouts, and icons to make privacy notices clear and understandable.

- Developing Standard Contractual Clauses (SCC) and making them available to Australian organisations to be applied when transferring personal information to a third-party recipient outside Australia. These SCCs would contain safeguards and requirements defining how an overseas recipient is expected to process personal information. Reform proposals for overseas transfers also align with the above notice and transparency proposal in that privacy notices will likely be expected to clearly state which countries personal information may be disclosed to.

- A number of restricted practices have been proposed as part of the reform. These practices are considered high-risk and should be treated as '*proceed with caution zones*', meaning an organisation would likely have to perform a Privacy Impact Assessment (PIA) and identify any risks and remediation actions if using personal information for practices such as:

    - Collection, use or disclosure of biometric or genetic data, including facial recognition software
    - Direct marketing or online targeted advertising on a large scale
    - Collection, use or disclosure of children's data on a large scale
    - Collection, use or disclosure of sensitive personal information on a large scale.

    A number of prohibited practices are also being considered, meaning practices such as profiling or behavioural advertising directed at children would be treated as '*no-go zones*' under the Act.

- The primary rights available to an individual under the current Act are access to personal information and correction of personal information. Following the GDPR model, the discussion paper proposes introducing additional rights for individuals such as the right to erasure and the right to object to personal information processing. The right to erasure was a particular talking point when GDPR was introduced in 2018. The introduction of such a right into the revised Privacy Act would require organisations to delete all personal information held pertaining to an individual upon request, provided certain criteria apply.

Regulation and Enforcement

The final theme proposed for reform in the discussion paper considers enhancing the OAIC's regulatory and enforcement powers. Proposed reforms in this area include:

- Enhancing the penalty structure and implementing a tiering model which will guide penalty decisions for first time, low-level offences to repeated and serious violations of the Act. Whilst no figures are explicitly proposed in the discussion paper, the Attorney-General's Department is performing a similar review of the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (the Online Privacy Bill) which includes draft provisions to increase the maximum penalty for serious and repeated offences to **$10 million**, or **10% of the offender's annual Australian turnover**.

How does this impact me?

Whilst some may initially view the proposed reform as an additional compliance burden and increased risk, the proposed amendments to the Privacy Act should be viewed as positive. The general consensus is that the European GDPR model is the gold standard in terms of privacy regulation. The proposed reforms will ultimately increase Australia's privacy legislation and go a long way towards achieving adequacy with the EU. Whilst other Asia-Pacific nations such as New Zealand and Japan have been granted an adequacy decision from the EU, Australia's privacy legislation does not currently meet EU standards. If Australia were to be granted an adequacy ruling, it would remove many barriers Australian organisations currently face when sharing information with third parties overseas.

Further, enhancements such as standardised privacy notices, contractual clauses, etc., and clear and concise definitions and examples of Australian organisations' privacy obligations will provide clear guidance and help streamline processes. Operating in a well-regulated environment will inevitably drive compliance and enhance organisations' privacy practices, ultimately providing value for the end customers and assurance their personal information is being managed securely and responsibly.

What can I do now?

The Department closed responses and consultations regarding the Discussion Paper on 10 January 2022. Whilst there is no clear date as to when the reforms will be finalised and the Privacy Act will be amended, the changes will likely occur at some stage this year subject to the revised Act passing through Parliament. To uplift privacy management in your organisation and enable a smooth transition towards compliance with the new provisions, consider:

- Understanding, assessing and, if necessary, revising your privacy management structures, including governance arrangements which oversee privacy. Whilst the current Act and supporting APP codes require only government agencies to have a designated Privacy Officer in place, the OAIC has proposed adding a requirement for all organisations to appoint a designated Privacy Officer. This requirement would align with requirements in place under the GDPR to incorporate greater accountability by having a designated individual to ensure compliance with the Act, liaise with regulators and assist with PIAs, amongst other privacy matters.

- Conducting data discovery or mapping exercises to identify, understand and inventory the types of personal information your organisation handles, the purpose(s) for which the information is used, who has access, what organisations they are shared with and where they are located, etc. These *records of processing* are mandatory under the GDPR, and the Discussion Paper again considers adapting this practice in the reform of the Act to place greater accountability on organisations.

- Performing Privacy Impact Assessments on any high-risk processes or critical information systems to identify risks and noncompliance and develop remediation activities. With PIAs for certain personal information processing activities likely becoming mandatory, regularly performing PIAs for high-risk processes will be crucial for privacy compliance.

[i] https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988
[ii] https://www.ag.gov.au/system/files/2020-10/privacy-act-review-terms-of-reference.pdf
[iii] https://www.ag.gov.au/system/files/2020-10/privacy-act-review--issues-paper-october-2020.pdf
[iv] https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/