protiviti®
Global Business Consulting

Australia's Privacy Act is fundamentally changing: What this means for your organisation

Background

On 16 February 2023, the Attorney-General's Department released its Privacy Act Review Report (**the Report**) following a two-year review of the Privacy Act 1988 (Cth) (**the Act**). The Report contains 116 recommended amendments to the existing Act to strengthen the protection of personal information and the control individuals have over their information. If accepted and adopted, the recommendations will significantly impact the way Australian organisations handle personal information.

The public consultation period for the Report closed on 31 March 2023, meaning the Government will now review the Report and consultation submissions before providing a response. We will then have a clear understanding of the amendments to the Act and the additional compliance obligations for Australian businesses.

116 recommendations – key takeaways

The 116 recommendations in the Report are grouped into three key areas:

1. Scope and application of the Privacy Act
2. Protections
3. Regulation and enforcement

Scope and application of the Act

31 amendments have been proposed in this area. Some of the key recommendations, and Protiviti's perspective on each, include the following:

Personal information, de-identification, and sensitive information

Proposal 4.2

Include a non-exhaustive list of information which may be personal information to assist APP entities to identify the types of information which could fall within the definition. Supplement this list with more specific examples in the explanatory materials and OAIC guidance.

This amendment would provide clarity for organisations in identifying personal information and gaining a clear understanding of their compliance obligations, but may also broaden the scope of personal information by bringing related or associated data sets such as web browser cookies for example into scope.

The recommendations will significantly impact the way Australian organisations handle personal information.

Employee records exemption

Proposal 7.1

Enhanced privacy protections should be extended to private sector employees, with the aim of:

- Providing enhanced transparency to employees regarding what their personal and sensitive information is being collected and used for
- Ensuring that employers have adequate flexibility to collect, use and disclose employees' information that is reasonably necessary to administer the employment relationship, including addressing the appropriate scope of any individual rights and the issue of whether consent should be required to collect employees' sensitive information
- Ensuring that employees' personal information is protected from misuse, loss or unauthorised access and is destroyed when it is no longer required, and
- Notifying employees and the Information Commissioner of any data breach involving employee's personal information which is likely to result in serious harm.

Interestingly, the Report does not propose to remove the existing employee records exemption but instead afford more protections and transparency to employees. The recommendation proposes organisations must apply the same level of security to employee records as they would other personal information they hold, and also provide employees with clear and concise notice as to how their personal information is being handled, where it is stored, who it is disclosed to, etc.

Recommendations to amend consent requirements in the Report incorporate some key elements of the European GDPR (General Data Protection Regulation) model in that consent must be voluntary, informed, current, specific and unambiguous.

Protections

The bulk of the Report focuses on protections afforded to individuals regarding their personal information, with 64 recommendations included in this section. Some notable recommendations include:

Consent

Proposal 11.1

Amend the definition of consent to provide that it must be voluntary, informed, current, specific, and unambiguous.

Proposal 11.2

The OAIC could develop guidance on how online services should design consent requests. This guidance could address whether particular layouts, wording or icons could be used when obtaining consent, and how the elements of valid consent should be interpreted in the online context. Consideration could be given to further progressing standardised consent as part of any future APP codes.

Recommendations to amend consent requirements in the Report incorporate some key elements of the European GDPR (General Data Protection Regulation) model in that consent must be voluntary, informed, current, specific and unambiguous. This is likely to invalidate consent provided under the current Act that permits organisations to collect express or implied consent from individuals, meaning organisations may have to refresh and collect consent again from individuals in a manner that is compliant with the new requirements if adopted.

Fair and reasonable personal information handling

Proposal 12.1

Amend the Act to require that the collection, use and disclosure of personal information must be fair and reasonable in the circumstances. It should be made clear that the fair and reasonable test is an objective test to be assessed from the perspective of a reasonable person.

The Report recommended that organisations should be required to perform an objective test before collecting, using or disclosing personal information to determine if the processing is fair and reasonable. The test should consider factors such as the sensitivity of the information, whether the impact on privacy is proportionate to the benefits, whether an individual would reasonably expect their information to be processed, and whether the processing is necessary for the functions and objectives of the organisation.

Additional protections

Proposal 13.1

APP entities must conduct a privacy impact assessment for all activities with high privacy risks.

Similar to the EU GDPR, the Report recommends introducing a mandatory requirement for organisations to conduct a Privacy Impact Assessment (PIA) prior to commencing high-risk activity. High-risk activity for example may include processing sensitive personal information or children's personal information on a large scale, use of biometric information, profiling or delivery of personalised advertising content to individuals, etc.

Rights of the individual

Proposal 18.3

Introduce a right to erasure with the following features:

- An individual may seek to exercise the right to erasure for any of their personal information.
- An APP entity who has collected the information from a third party or disclosed the information to a third party must inform the individual about the third party and notify the third party of the erasure request unless it is impossible or involves disproportionate effort.

As was widely expected, the Report proposes a right to erasure for individuals, mirroring the European model. This recommendation would permit individuals to request an organisation destroy all personal information the organisation holds pertaining to them. Organisations will face the challenge of implementing appropriate procedures and technologies to accurately identify all personal information they hold relating to a request, securely destroy such information, and to notify all third parties with access to the information of the request and their obligation to destroy the information.

As was widely expected, the Report proposes a right to erasure for individuals, mirroring the European model. This recommendation would permit individuals to request an organisation destroy all personal information the organisation holds pertaining to them.

Security, retention and destruction

Proposal 21.2

Include a set of baseline privacy outcomes under APP 11 and consult further with industry and government to determine these outcomes, informed by the development of the Government's 2023-2030 Australian Cyber Security Strategy.

Proposal 21.3

Enhance the OAIC guidance in relation to APP 11 on what reasonable steps are to secure personal information. The guidance that relates to cyber security could draw on technical advice from the Australian Cyber Security Centre.

A welcome sight in the Report was the proposal for the introduction of security requirements to be applied to protect personal information from unauthorised access, misuse, disclosure, etc., as well as additional guidance to be published by the Office of the Australian Information Commissioner (OAIC). This will potentially remove some ambiguity from the current requirements of the Australian Privacy Principle (APP) 11.

A welcome sight in the Report was the proposal for the introduction of security requirements to be applied to protect personal information from unauthorised access, misuse, disclosure, etc.

Controllers and processors of personal information

Proposal 22.1

Introduce the concepts of APP entity controllers and APP entity processors into the Act. Pending removal of the small business exemption, a non-APP entity that processes information on behalf of an APP entity controller would be brought into the scope of the Act in relation to its handling of personal information for the APP entity controller. This would be subject to further consultation with small business and an impact analysis to understand the impact on small business processors.

Another recommendation derived from EU GDPR proposes introducing the concept of data controllers and data processors. Controllers would be deemed the party that dictates how the personal information is processed, while processors would only process personal information upon the instructions of a controller. This proposal would also assist in enforcing an organisations' third party provider compliance with the Act.

Regulations and enforcement

The final area of the Report includes 21 recommendations regarding the regulatory environment and enforcement actions, with some key recommendations including:

Enforcement

Proposal 25.1

Create tiers of civil penalty provisions to allow for better targeted regulatory responses:

- Introduce a new mid-tier civil penalty provision to cover interferences with privacy without a 'serious' element, excluding the new low-level civil penalty provision.
- Introduce a new low-level civil penalty provision for specific administrative breaches of the Act and APPs with attached infringement notice powers for the Information Commissioner with set penalties.

This proposal expands on the enactment of the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 in November 2022 which increased maximum penalties for privacy compliance breaches from $2.2m to a potential $50m. A tiering system for penalties is proposed, with a potential penalty of 2,000 penalty units (currently $5.5m) for mid-tier offences and 20% of the maximum amount of the related civil penalty for low-tier offences being considered. For example, failure to maintain a clear and up to date privacy policy, or respond to individuals' requests in a timely manner may constitute a low-tier offence.

Another recommendation derived from EU GDPR proposes introducing the concept of data controllers and data processors.

A direct right of action

Proposal 26.1

Amend the Act to allow for a direct right of action in order to permit individuals to apply to the courts for relief in relation to an interference with privacy.

The Report also recommends introducing a direct right of action for individuals or groups of individuals (class actions) to seek compensation through the courts for breaches of privacy. The Report proposes all claims are initially assessed by the OAIC or an External Dispute Resolution scheme, and where no resolution can be found the complainant(s) would have the option to pursue the matter further in court.

Understanding your organisation's data is crucial. The clock is ticking for organisations to uplift their privacy practices.

Hanneke Catts, Director, Protiviti

What should I do now?

While final amendments and enactment timeframes are currently undefined (late 2023/early 2024 may be a realistic target), the clock is still ticking for organisations to uplift their privacy practices. Making the following activities a priority for your privacy program in 2023 is recommended to uplift capabilities and comply with key areas of the reformed Act:

Understand your data: Identify and inventory how your organisation collects, uses, stores, discloses, and retains personal information. Conduct discovery sessions across the business and apply data discovery tools where applicable to identify personal information processes across your organisation. Develop, document and maintain results in a formal record of processing. This will also enable compliance with proposal 15.1 and the requirement for organisations to record the purposes for how they collect, use and disclose personal information.

Focus on data minimisation: Remove any instances of collection, use or disclosure of personal information that is not strictly necessary and for a defined purpose. Securely destroy personal information that is no longer relevant or outside its defined retention period.

Build out your security capabilities: Recent high-profile data breaches have shown that inadequate data security capabilities and excessive data retention practices can be extremely costly. Investing in security technologies and resources and maintaining and regularly testing data breach response plans will help reduce the likelihood and impact of any incidents.

Acknowledgement

Jacqueline Liang contributed to this piece.

Contacts

Leslie Howatt
Managing Director
Protiviti
+61.488.301.794
leslie.howatt@protiviti.com.au

Hanneke Catts
Director
Protiviti
+61.404.101.580
hanneke.catts@protiviti.com.au

Ghislaine Entwisle
Managing Director
Protiviti
+61.431.285.494
ghislaine.entwisle@protiviti.com.au