Deloitte.

Australian Privacy Act Proposed Changes

Top 10 operational impacts to your business

February 2023

Changes to Australian privacy law are on the horizon - what are the proposed changes?

On 16 February 2023, the Attorney-General's Department released their Privacy Act Review Report which contains 116 proposals to strengthen Australia's *Privacy Act 1988* (Cth) (Privacy Act). Deloitte highlights a snapshot of 10 key proposed changes which are likely to have significant impact on your business operations. The proposed changes represent a continuation in the uplift of the current Australian privacy law framework and a greater alignment with global privacy laws.

1. Expanded definition of personal information

Expansion of the definition of personal information, from 'information or an opinion *about* an identified individual, or an individual who is reasonably identifiable' to 'information or an opinion that *relates to* an identified individual, or an individual who is reasonably identifiable'. The amended definition would broaden the scope to include location data and technical and customer identifiers including IP addresses and customer IDs. It will also bring the definition in line with that used in the European Union General Data Protection Regulation (GDPR).

2. Strengthened consent requirements

Proposed amendments of the conditions for consent to be 'voluntary, informed, current, specific, and unambiguous'. Under the proposed changes the withdrawal or withholding of consent must be as easy as the provision of consent. These changes are intended to eliminate consent practices that lack transparency (e.g., bundled consent) to move towards a more meaningful consent model. Although implied consent may still be permissible under the proposed changes if it is deemed 'unambiguous', this would only apply in a niche set of scenarios (e.g., health related situations).

3. Enhanced protections for employee personal information

Proposed changes to the employee records exemption will result in some additional obligations when handling employee records related to private sector employees. Increased transparency of the collection and handling of information about employees, protection against unauthorised access or interference and reporting of eligible data breaches are some of the proposed obligations to be imposed.

4. Introduction of new individual rights

Providing individuals with more control over how businesses handle their personal information with the introduction of the following rights: right to erasure, right to object and the right to de-index search results. A private right of action for privacy interferences is also proposed potentially exposing organisations to class actions from individuals who have been impacted by breaches or misuse. Proposals also intend to strengthen the existing rights to correction and access. If an individual exercises one of their rights, it should be fulfilled within 30 days, unless a longer timeframe is justified.

5. Strengthened controls for overseas data flows

Moving away from taking reasonable steps to ensure overseas recipients will comply with the APPs, to facilitating the free flow of data by introducing:

- A certification scheme for countries with similar laws.
- Standard contractual clauses for countries without 'essentially equivalent' laws.
- Strengthened notice and consent requirements for overseas disclosures.

6. Shorter timeframes for data breach notification

Shorter timeframes of 72 hours, reduced from 30 days under current legislation, for reporting notifiable data breaches to the Office of the Australian Information Commissioner (OAIC) are proposed. Impacted individuals must also be notified as soon as practically possible. Information may be provided to affected individuals in phases if it is not possible to provide it at the same time as the OAIC notification. This will bring the Privacy Act in line with the GDPR and CPS234 timeframes for reporting eligible data breaches to the regulator.

7. Clarified definition and protections for de-identification

Currently, de-identified information (data that is stripped of personal identifiers and cannot be re-identified) is out of scope and not fully defined under the Privacy Act. The report proposes to extend some privacy requirements to de-identified datasets, including protecting de-identified information from unauthorised access or interference and prohibiting the re-identification of de-identified data by both third-party entities and overseas entities.

8. Additional rights and protections for marketing and targeting

Introduction of an unqualified right to opt-out of personal information being used or disclosed for direct marketing and a separate right to opt-out of receiving targeted advertising, the concept of 'trading', and limitations on the use of children's personal and sensitive information for marketing are proposed. Trading is when an organisation discloses personal information for their own benefit, advantage or for a service, and will require consent from the individual. Targeting of individuals must be fair and reasonable and must meet transparency requirements.

9. Introduction of a 'fair and reasonable' test

Introduction of a fair and reasonable test when processing personal information which is an objective assessment of how a reasonable person would expect personal information to be collected, used or disclosed is proposed. Several factors that should be assessed in a fair and reasonable test have been provided in the report, including the type, sensitivity and volume of personal information and the risk of harm to individuals.

10. Transparency and review of retention periods

Proposed introduction of two new requirements around retention including:

- Establishing minimum and maximum retention periods for all personal information held.
- Disclosing retention periods in customer facing privacy policies and records management policies.

It is proposed that retention periods are assessed and reviewed periodically and that organisations will still be required to destroy or de-identify personal information when it is no longer required.

What do the proposed changes mean for your organisation?

Deloitte focusses on the 10 key proposals which are likely to have considerable impact on your current day-to-day business operations. Deloitte highlights the impact these 10 proposals will have on your organisation, what preparations you should start making, and lessons we have learnt from the introduction and uplift of privacy laws globally.

Expanded definition of personal information

How can you prepare?

- ❑ Undertake a data mapping exercise to identify all personal information held by your organisation including additional information that will fall under the expanded definition.
- ❑ Review and update the privacy framework including all supporting processes, procedures and documentation to extend existing privacy protections to new information types, to ensure it is protected and destroyed when no longer required.
- ❑ Communicate and educate technical, data and customer facing staff on the expanded definition through training and awareness.

Key lessons from around the globe

- ✓ A broader definition results in expanded responsibilities as additional personal information processing activities fall into the scope of privacy laws.
- ✓ Documenting your personal information processing activities, including what is being held, the purposes for processing, their location(s) and the security measures in place, is key to being able to manage personal information appropriately.
- ✓ Education is crucial to ensuring that staff can identify personal information and manage it appropriately.

Strengthened consent requirements

How can you prepare?

- ❑ Move to a privacy-by-default model for all online privacy settings. For example, do not use bundled consent or pre-ticked boxes to collect consent as these may not meet the new proposed conditions for consent.
- ❑ Review how consent is currently obtained and consider how more meaningful consent can be collected from individuals.
- ❑ Develop and test consent withdrawal processes to determine whether they would meet the proposed requirement for being as easy as the provision of consent.

Key lessons from around the globe

- ✓ Consent is one lawful basis – out of several – for processing personal information. However, consent guidelines should be strictly applied, monitored, and clearly defined in policies and in supporting technology to be effective.
- ✓ A consent management tool or technology platform can help you manage consent effectively from the point of collection through to managing changes to consent, including withdrawal.

Enhanced protections for employee personal information

How can you prepare?

- ❑ Consider whether any existing personal information processes can be leveraged for the protection of employee personal information and if any new processes need to be developed (e.g., a procedure for handling employee personal information, data mapping of employee information).
- ❑ Determine how enhanced transparency can be provided to employees regarding the collection and use of their personal information (e.g., through review/uplift of privacy policies).
- ❑ Update data breach response plan to include employee personal information.

Key lessons from around the globe

- ✓ As Human Resource (HR) departments are the major stakeholders for processing the personal information of employees, setting up HR privacy delegates or champions is a good first step.
- ✓ Awareness training for the HR department is a key step to gaining confidence that staff can identify personal information and manage it appropriately.
- ✓ An uptick in employee access requests may occur as individual rights are extended to employee records.

Introduction of new individual rights

How can you prepare?

- ❑ Understand where all personal information in the business resides (e.g., through data mapping and development of a register of personal information processing activities).
- ❑ Update individual rights processes and procedures to cover requirements for new and amended individual rights and to ensure that they can be fulfilled within 30 days.
- ❑ Train all relevant staff on what individual rights are and how to fulfil an individual rights request.

Key lessons from around the globe

- ✓ Data mapping and a register of personal information processing activities are key to ensuring that the organisation can locate personal information in a timely manner, including personal information held by third parties and to respond to individual rights requests within the required timeframes.
- ✓ Clear individual rights process are required to provide direction to staff to confidently respond to requests with clarity about what can and cannot be accessed, corrected or erased.

Strengthened controls for overseas data flows

How can you prepare?

- ❑ Identify and document all data flows with third parties and interorganisational data flows outside of Australia.
- ❑ Review controls for sharing personal information with third parties and consider how these can be strengthened (e.g., check that a contract exists with third parties to govern all international transfers of personal information).

Key lessons from around the globe

- ✓ If an organisation is outsourcing personal information processing activities, the organisation remains responsible for safeguarding that personal information even if the data is processed overseas.
- ✓ The right lawful basis or contract in place for overseas data flows is key to meeting privacy requirements and preventing breaches and possibly large fines.

What do the proposed changes mean for your organisation?

Deloitte focusses on the 10 key proposals which are likely to have considerable impact on your current day-to-day business operations. Deloitte highlights the impact these 10 proposals will have on your organisation, what preparations you should start making, and lessons we have learnt from the introduction and uplift of privacy laws globally.

Shorter timeframes for data breach notification

How can you prepare?

- ❑ Review and uplift data breach response plan and processes to allow for the identification and reporting of eligible data breaches to the OAIC within a 72 hour window.
- ❑ Update and test data breach response plans and processes through simulations and/or table top exercises and amend as required.
- ❑ Train staff on what constitutes a data breach and the process for reporting one.

Key lessons from around the globe

- ✓ Prior to notifying the regulator or affected individual it is important to understand the extent and severity of the data breach (e.g., which individuals are affected, the sensitivity of data) – in that light a clear plan and process are key to ensuring the 72 hours are used efficiently and effectively .
- ✓ A well-defined and tested data breach response team with expertise from various disciplines (e.g., security, privacy, legal, regulatory affairs) is key to being able to react adequately within the 72 hour window.

Clarified definition and protections for de-identification

How can you prepare?

- ❑ Identify all de-identified data sets held and assess whether they can still be considered as de-identified under the proposed definition. This should include an assessment of the re-identification risk.
- ❑ Consider removal of de-identified data sets that are no longer required, and which are at risk of re-identification.
- ❑ Consider how current security and overseas disclosure requirements and controls can be extended to de-identified data sets.
- ❑ Review de-identification techniques and assess whether they are still fit for purpose of if they need to be strengthened.

Key lessons from around the globe

- ✓ Where the same outcome can be achieved through the use of de-identified information, this is the approach that should be taken.
- ✓ There can often be a risk of re-identification where de-identification has not been applied correctly or the definition of de-identification is not well understood.
- ✓ De-identification techniques differ in relation to the nature of the personal information. For example, photos or complex data sets may require a more advanced technique of deidentification.

Additional rights and protections for marketing and targeting

How can you prepare?

- ❑ Review all direct marketing and targeted advertising activities and consider limiting, amending or ceasing activities that do not align with the proposed requirements and with the expectations of the individual.
- ❑ Review all direct marketing and targeted advertising activities directed at children, assess whether these activities are in the best interest of the child and cease activities that are not in their best interest.
- ❑ Develop an opt-out method for targeted advertising and ensure that it meets the requirements for withdrawing consent as easily as providing the consent.

Key lessons from around the globe

- ✓ Ensure Customer Relationship Management (CRM) systems are configured properly to apply the correct privacy controls around consent (e.g., accurate recording and tracking of consent).
- ✓ Implementing the right privacy measures for direct marketing will help to prevent large fines imposed from authorities for misuse.
- ✓ Transparent and privacy friendly direct marketing activities are a brand asset (e.g., it supports to protect the reputation of a brand as a trusted digital player).

Introduction of a 'fair and reasonable' test

How can you prepare?

- ❑ Review existing personal information uses in line with the 'fair and reasonable' test and remediate where activities do not align with the test.
- ❑ Document the fair and reasonable test prior to processing personal information for any new uses to demonstrate it has been considered.
- ❑ Review privacy policies, collection notices and consent and consider how they meet the fair and reasonable test, in particular, transparency and appropriate collection and use.

Key lessons from around the globe

- ✓ Privacy notices describing the categories of data that is processed, the purpose of the processing activities and the rights of the data subjects are a powerful tool for organisations to demonstrate fair, transparent and reasonable data handling practices to the data subjects.
- ✓ Embedding privacy in internal controls and processes is an effective measure to implement fair and reasonable data handling practices within an organisation in a systematic way.

Transparency and review of retention periods

How can you prepare?

- ❑ Review retention schedule and associated records management policies and define minimum and maximum retention periods, considering legal and business requirements for retention.
- ❑ Update privacy policies to include specified minimum and maximum retention periods for personal information.
- ❑ Review personal information retained against the retention periods defined and conduct remediation of any records that are no longer required.

Key lessons from around the globe

- ✓ It is important that data owners are identified and assigned the responsibility of assessing the purposes for retaining personal information and the retention periods.
- ✓ It is often difficult to destroy personal information from legacy systems and where this cannot occur other controls for protecting and restricting access to the personal information should be considered.

How can you get on the front foot?

Deloitte is a global leader in Data, Privacy and Cyber Security – and is willing to have a conversation today, to set you up for tomorrow.

How Deloitte can help

Deloitte works with clients to answer questions that matter the most:

- How can we prepare for privacy changes on the horizon?
- How can we use personal information more effectively?
- How can we demonstrate effective compliance?
- How should we manage breaches and notifications?
- How can we embed privacy capability within our organisation?

Deloitte offers a tested and comprehensive suite of end-to-end privacy services to help our clients transform and maintain their management of regulatory and operational challenges.

We help clients transform their privacy and data protection strategies, and create measures to report on and implement these strategies.

Get in touch now

Daniella Kafouris
Partner | Risk Advisory
Cyber & Strategic Risk
dakafouris@deloitte.com.au
+61 3 9671 7658

Kate Monckton
Partner | Risk Advisory
Cyber & Strategic Risk
kmonckton@deloitte.com.au
+61 2 8260 6059

Lucy Mannering
Partner | Risk Advisory
Cyber & Strategic Risk
lmannering@deloitte.com.au
+61 412 122 561

Gautam Kapoor
Partner | Risk Advisory
Cyber & Strategic Risk
gautakapoor@deloitte.com.au
+61 2 9322 3241