2023 Privacy Act Review Report

Quick Guide

The highly-anticipated report of the Attorney-General's Department's review of the Privacy Act 1988 (Cth) has finally landed with significant flair. Two years in the making, the Report has put forward 116 proposals that, if implemented, will be the most dramatic change to the Australian privacy and data protection landscape since the introduction of the APPs.

We have broken down the key themes and issues in the existing legislation, and some of the key reforms proposed by the Report.

Key themes

'Personal Information'

Collection, Use, and Disclosure

Offshore data flows and certification

Exemptions

Key issue

'Personal Information'	Collection, Use, and Disclosure	Offshore data flows and certification	Exemptions
Concerns that the definition of personal information needs to be revised to capture additional categories of information to align with consumer expectations and how personal information is now being used.	Concerns that the handling of personal information is not being carried out in a transparent manner and in a way that allows individuals to make a truly informed choice about their personal information.	Continued discussion about developing a certification scheme that will allow Australian entities to be recognised as having adequate privacy protections throughout other jurisdictions.	Concerns that Australia must align better with similar international privacy regimes and ensure that the privacy rights of individuals are balanced appropriately. This includes potentially removing / amending exemptions which exist to exclude some groups from the operation of the Privacy Act.

Key proposed reforms

'Personal Information'

- Information protected under the Act is 'personal information' that *relates to* an individual (cf. *about*) – broader, less tenuous definition.
- Inclusion of non-exhaustive list of what is 'personal information' and guidance from OAIC re what information may constitute personal information.
- Expand definition of 'collection' to expressly cover information obtained from any source and by any means, including inferred or generated information.
- Add clarification that de-identifying information is a process to be undertaken where the outcome is that the individual cannot be identified or reasonably identified in that context.
- Sensitive information will now include 'genomic' information.

Collection, Use, and Disclosure

- Introduction of a '*fair and reasonable*' test to underpin the activities of APP entities when handling personal information.
- New requirement to protect *de-identified information* both within Australia and in cross-border disclosure, including aggregated data and information.
- New requirement to ensure improved quality of privacy collection notices and consents including data retention timelines – OAIC to develop standardised templates and layouts for collection notices and privacy policies.
- Privacy policy must specify retention periods. Additional protections for 'high privacy risk practices', including a requirement to undertake a privacy impact assessment.
- Additional requirements for personal information of children and vulnerable people, including introduction of a Children's Online Privacy Code (similar to UK Age Appropriate Design Code).

Offshore data flows and certification

- Although discussions were had on CBPR and domestic certification, the reports does not contain any proposals to develop any such scheme.
- However, there has been a significant shift to align the Act with international legislation – the Report proposes to introduce familiar GDPR concepts of controllers and processors.
- Introduce a mechanism to prescribe countries and certification schemes as providing substantially similar protection to the APPs (i.e adequacy regime).
- Create standard contractual clauses to be used for cross-border transfer of data.

Exemptions

- Removal of small business exemption
- Additional privacy protection to private sector employees, including requirement to notify OAIC and individuals of any data breach involving employee information – note that the employee records exemption is ***not*** proposed to be removed
- Additional requirements to round out the political exemption, including a requirement that political entities take reasonable steps to protect and destroy / de-identify personal information and comply with the NDB scheme.
- Additional requirements for entities relying on journalism exemption, including a requirement that organisations must be subject to specific privacy standards, and must comply with APP 11 and the reporting obligations in the NDB scheme.

The View From PwC

- Whilst not fully replicating the GDPR, amendments proposed in the report would go a long way towards more closely aligning the Australian regime with GDPR. It will be interesting to see if it would be enough for Australia to receive an adequacy decision under the GDPR.
- There appears to be a move away from general principle-based regulation to a more prescriptive (or at least more comprehensively guided) approach. It is possible that this is related to the proposed expansion of the Act to apply to small businesses, who may not have the same level of regulatory / legislative sophistication of current APP entities.
- The introduction of a standard contractual clauses regime means that organisations will need to consider their supply chains and existing contractual arrangements and look to build in the relevant flexibility to potentially bring these clauses in if they are accepted and finalised.

Key themes

- Consent
- Rights for Individuals
- Control and Security
- Enforcement Powers

Key issue

Consent

Concerns that individuals are not truly given a choice in consenting to how their data is handled by entities given the length of privacy policies and consent 'bundling' practices.

Rights for Individuals

Concerns of the lack of a right for individuals to bring their complaints under the Privacy Act or breach of privacy directly to court means that there is not enough incentives for compliance or remedies for individuals.

Control and Security

Concerns that the current regime is not sufficient considering number of data breaches and surveys indicating that a majority of individuals want more control and choice over collection, use and destruction of their personal information.

Enforcement Powers

Concerns that the OAIC has insufficient enforcement powers in order to appropriately drive compliance with the privacy regime.

Key proposed reforms

Consent

- Amend definition of consent to expressly require that it be "voluntary, informed, current, specific, and unambiguous".
- Online privacy settings that deal with consent must be clear and easily accessible. Guidance to be developed by OAIC.
- Express recognition of the ability to withdraw consent and to do so in a manner as easily as the provision of consent.
- Introduce a legislative provision that permits broad consent for the purposes of research, with further consideration for an exception for research without consent.
- Introduce a requirement that an individual's consent must be obtained to trade their PI.

Rights for Individuals

- Introduce a direct right of action for individuals to apply to the courts for relief for 'privacy interferences' e.g. data breach.
- Introduce a statutory tort for 'serious invasions' of privacy.
- Proposal to provide individuals with a number of new rights, which are modelled on the EU GDPR 'data subject rights', including rights to object, to request erasure, to opt-out of receiving targeted advertising and being used / disclosed for direct marketing purposes, and to have search results deindexed). Exceptions to apply for countervailing public interests, other legal interests and where it would be technically impossible or unreasonable to comply.
- APP entities must provide reasonable assistance to individuals to assist in the exercise of their rights.
- Transparency requirements for automated decisions that use personal information and have a significant effect on individuals.

Control and Security

- Clearly articulate that the 'reasonable steps' undertaken to protect personal information includes both technical and organisational measures.
- APP entities must take reasonable steps to protect de-identified information.
- Data retention periods to be included in privacy policy.
- Requirement to appoint a 'privacy officer' of sorts
- Entities to notify the OAIC within 72 hours of enhancements to the NDB Scheme, including a requirement becoming aware of a data breach, and to take reasonable steps to implement practices for effective data breach response.
- Allow the Attorney-General to permit information-sharing between entities relating eligible data breaches to reduce risk of harm to individuals.

Enforcement Powers

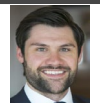
- OAIC has the power to make an APP code.
- Enabling Emergency Declarations to be more targeted, and able to be made in relation to ongoing emergencies.
- New civil penalties and new powers for the OAIC in relation to investigations, public inquiries and determinations.
- Clarification as to what constitutes a 'serious' interference or breach of privacy.
- Given the complexity of the OAIC's regulatory burden and resourcing constraints, the Report proposes further consideration into an industry funding model as well as a contingency litigation fund.

The View From PwC

- Organisations need to consider the realistic outcome that many of these changes will be accepted in some form, and will therefore need to ensure that they consider their current state and roadmap to compliance. Organisations who develop an accurate understanding of their data footprint / data holdings now, will be in a much better position to respond with agility once all changes are locked in.
- Funding of the OAIC is something that has been discussed at length, particularly given the importance of its role in regulating an economy wide and complex regime. The introduction or consideration of an industry-based funding model is something that will need to be followed closely. Query also whether the addition of personal rights is also in some way designed to take some pressure off of the OAIC playing a role as a deterrent, relying on a combination of the OAIC's role and the threat of individual action to deter non-compliance.
- Consent changes could have a significant impact on organisations who are currently relying on consents that have been obtained prior to the implementation of these changes. It is not clear how a change to this area will affect existing consents and organisations may need to consider a strategy to obtain updated consents which comply with the revised approach.
- Whilst there are some proposed expansions to the APP 11 security requirements, we still do not see the level of enhanced privacy protections that are clearly articulated under the Consumer Data Right regime. S significant change is the imposition of security and other obligations on de-identified data which could significantly impact many organisations. Organisations will need to ensure that their analysis of their PI management includes not just personal information, but where information has been aggregated and de-identified.

Contacts

Adrian Chotar
Partner, Legal
+61 (0) 457 808 068
adrian.chotar@pwc.com



James Patto
Director, Legal
+61 (0) 431 275 693
james.patto@pwc.com

Jon Benson
Partner, Assurance
+61 (0) 438 565 299
jon.benson@pwc.com

Natalie Mu
Director, Assurance
+61 (0) 400 021 227
natalie.mu@pwc.com