Australia: Government responds to proposed changes to Australia's privacy regime

The Australian Government confirms its agreement to make significant amendments to Australia's privacy laws, and to progress additional reforms through further consultation

In brief

The Australian Government has released its much-anticipated response ("**Response**") to the Commonwealth Attorney-General Department's report ("**Report**") on its review of the *Privacy Act 1988* (Cth) ("**Privacy Act**"). The Report recommended wholesale amendments to Australia's principal privacy legislation and contained 116 proposals for consideration by the government (for a detailed look at the Report, and the background to the review of the Privacy Act, see our previous alert here).

The Response is largely receptive to the Report's proposals, indicating positive support for a majority of the recommendations, with none rejected outright. However, the government has only "**agreed**" to the development of specific legislation for 38 of the proposals, which for the most part relate to less contentious changes focused on strengthening Australia's existing privacy regime. These include:

- Regulating information used in automated decision-making and clarifying information security requirements
- Developing a Children's Online Privacy Code to apply to online services likely to be accessed by children
- Introducing new mid-tier and low-tier civil penalty provisions to allow for targeted regulatory responses, alongside enhanced enforcement powers for the privacy regulator and the courts.

A further 68 proposals are "**agreed-in-principle**", but will be subject to further consultation to explore whether and how they may be implemented so as to balance privacy safeguards with other key concerns, such as the burden on regulated entities. These include a number of the more controversial proposals, such as:

- The introduction of a maximum 72 hour period to notify the regulator upon becoming aware that there are reasonable grounds to believe there has been an eligible data breach
- The introduction of new individual rights (including enhanced control over personal information and a "right to be forgotten") and a statutory tort for serious invasion of privacy
- Certain changes to how data collection and data breaches are managed
- The removal of existing exemptions for small businesses and employee records, and the introduction of additional safeguards relating to the journalism exemption

The 10 remaining "**noted**" proposals, which include recommendations relating to the protection of de-identified information, are flagged for potential further consideration by the government. The Response indicates that the government agrees with the broad intention of a majority of such recommendations, but not necessarily the specific approach put forward.

Contact Information

Anne Petterd
Partner
Sydney

Toby Patten
Partner
Melbourne

Adrian Lawrence
Partner
Sydney

Caitlin Whale
Partner
Sydney

Paul Forbes
Partner
Sydney

Ryan Grant
Partner
Sydney

Jarrod Bayliss-McCulloch
Special Counsel
Melbourne

Sally Pierce
Special Counsel
Sydney

Simone Blackadder
Special Counsel
Sydney

Baker McKenzie.

437640696-v9\AP_DMS

The Government has indicated there will be opportunities for further consultation but will introduce legislation in 2024. There will be a transition period for any changes. For a more detailed look at some of the key proposals that have been agreed, agreed-in-principle, and noted, see the "In depth" section below.

Key takeaways

- The Response confirms the Australian Government's appetite to address growing risks to privacy catalyzed by the ongoing expansion of the digital economy, following in the footsteps of overseas privacy regimes, such as the EU's General Data Protection Regulation ("**GDPR**"). However, the Response is fairly high-level and does not provide much certainty around the specific legislative reforms that will be put forward. Additionally, a significant number of the more controversial changes – and even some of the "agreed" proposals – remain subject to further consultation.
- Reassuringly, the government has confirmed there will be a grace period to allow regulated entities sufficient time to become compliant with the new requirements once the reforms have been introduced, with the Response describing an adequate transition period as "critical". The Response also emphasizes the importance of developing appropriate guidance and other supports to help entities understand their new compliance requirements.
-

Next steps

In the Fact Sheet accompanying its Response, the Australian Government has expressly committed to introducing further privacy legislation in 2024.

The Attorney-General's Department will now take the lead on preparing draft legislation, informed by targeted stakeholder consultations and detailed impact analyses, to address the proposals that have been "agreed".

The Department will also be responsible for engaging with regulated entities for additional consultation on proposals that are "agreed-in-principle", with advice on the outcomes of such further consultation to also be progressed to the government in 2024. The Department will also work on developing non-legislative proposals (for example, additional guidance and a Children's Online Privacy Code).

In depth

1. Proposals agreed to be addressed through legislative reform

The government has agreed to develop and propose legislative or related provisions for 38 of the 116 proposals contained in the Report. While the "agreed" proposals are not all subject to further engagement (unlike the "agreed-in-principle" proposals – see below), further targeted consultation will be undertaken with entities and consumers prior to the proposed legislation settling in its final form. This means that the introduction of the proposals may still be some time off, and the final form in which they will be legislated is not yet clear.

The key proposals from the Report for which the government has agreed to draft legislation include proposals to:

- **Enhance transparency around automated decision making**, including by requiring that privacy policies set out the types of personal information that will be used in substantially automated decisions that have a significant effect on an individual's rights. To provide some clarity, high-level indicators of these types of decisions would be included in the Privacy Act, supplemented by regulator guidance. The government has also agreed that individuals should have a right to request meaningful information about the process and effect of such automated decision-making. These changes would increase the regulatory and administrative burden for entities that engage in automated decision-making that leverages personal information.

- **Facilitate cross-border data transfers,** by creating a mechanism to prescribe countries assessed as having substantially similar privacy laws to Australia. This would support the free flow of information to certain jurisdictions without the need for contractual provisions or other measures.
- **Clarify information security requirements**, including by specifying that "reasonable steps" to protect personal information include technical and organizational measures, and having the Office of the Australian Information Commissioner ("**OAIC**") issue additional guidance on information security and destruction or de-identification of personal information.
- **Ensure there is appropriate guidance on high-risk activities**, through continued development by the OAIC of practice-specific guidance for new technologies and emerging privacy risks.
- **Fine-tune data breach reporting arrangements**, by giving further consideration to streamlining multiple reporting obligations for data breaches in conjunction with the government's cyber security initiatives, and permitting information sharing about data breaches between relevant entities, in certain circumstances and subject to limitations, to enable a coordinated response with the aim of reducing harm to individuals.
- **Improve protection of children and vulnerable people**, including through the development of a Children's Online Privacy Code for online services that are likely to be accessed by children. The government has endorsed alignment with international approaches, such as the UK Age Appropriate Design Code, and also agrees that OAIC guidance in relation to vulnerable people should be enhanced. This will be of particular importance to the many businesses who interact with or provide services to children or vulnerable people in an online context.
- **Strengthen regulator abilities and enforcement mechanisms**, including through:
    - Clarification of what constitutes a "serious" interference with privacy
    - New mid- and low-tier civil penalty provisions to cover medium and low severity interferences with privacy, with the latter having an attached infringement notice regime with set penalties
    - Increased powers for courts to make any orders they see fit in relation to breaches of civil penalty provisions
    - Additional requirements for entities to identify, mitigate and redress actual or foreseeable loss suffered by an individual due to an interference with privacy
    - Increased discretion and powers for the Information Commissioner, such as in relation to the development of privacy codes, emergency declarations, complaint investigations, investigations of civil penalty provisions, and public inquiries into specified matters in certain cases
- **Consult further** on certain matters, most notably, possible clarifications to the test for extra-territorial application of the Privacy Act.

2. Proposals agreed-in-principle subject to further consultation

The 68 proposals "agreed in-principle" will be subject to further consultation to examine the impacts on regulated entities, with a view to balancing the benefits of such proposals with the associated economic costs.

Some of the most interesting proposals that are "agreed-in-principle", but that will undergo further consultation, include proposals to:

- **Expand the definition of personal information,** and clarify when an individual would be considered "reasonably identifiable". The Response states that the government considers "an individual may be reasonably identifiable where they are able to be distinguished from all others, even if their identity is not known". While some would argue that this proposal would simply clarify the status quo, there may be significant consequences for businesses dealing with technical data and anonymous identifiers, which they have been treating as non-personal information.
- **Introduce a "fair and reasonable" test** for the collection, use and disclosure of personal information, irrespective of whether consent has been obtained.

- **Impose additional requirements for privacy policies and collection notices**, including that notices would have to be clear, up to date, concise and understandable, with the possibility of standardization across templates, layouts, terminology and icons.
- **Adopt a distinction between controllers and processors** of personal information, to recognize differing degrees of control that certain entities have over the handling of personal information. This proposed change reflects terminology used in the GDPR.
- **Introduce a new direct right of action for individuals** to sue for breaches of the Privacy Act and a new statutory tort for serious invasions of privacy in certain circumstances.
- **Recognize new and enhanced individual rights**, including a right to access personal information held by an entity and seek an explanation of how such information is sourced and handled, a right to object to the collection, use or disclosure of personal information, and a right to erasure of personal information (often referred to as a "right to be forgotten").
- **Tighten obligations relating to eligible data breaches**, including by introducing a hard deadline to notify the OAIC within 72 hours of becoming aware of an eligible data breach, similar to the timeframe set for personal data breach notification under the GDPR (though noting that the Response expressly indicates that the government will further explore appropriate timeframes with stakeholders). The government also agrees-in-principle that individuals should be notified of eligible data breaches as soon as practicable, and that entities should be subject to new positive requirements to take reasonable steps to respond to data breaches.
- **Enhance consent mechanisms**, including by enshrining in legislation the notion that consent must be voluntary, informed, current, specific and unambiguous, and that it can be withdrawn as easily as it is given.
- **Introduce a 'privacy-by-default' framework** for privacy settings for online services, to be determined by what is fair and reasonable in the circumstances.
- **Remove or amend certain exemptions** in the Privacy Act, including by removing the small business exemption and reviewing reforms to the employee record exemption (subject to further stakeholder consultation and impact analysis), and introducing new requirements for media organizations to comply with security and destruction obligations and reporting obligations for notifiable data breaches.

3. Proposals noted for further consideration

The government has "noted" the remaining 10 proposals and in most cases, flagged them for further consideration, although no commitments have been made as to when or how such consideration may occur. Most significantly, these include proposals to:

- **Apply specific protections to de-identified information**, including by introducing a requirement to take such steps as are reasonable to protect de-identified information from certain mistreatment (e.g. misuse and unauthorized re-identification or disclosure). The Response states that the government generally agrees with the policy intent of protecting de-identified information from unauthorized re-identification, and will consider further how this may be achieved.
- **Introduce an unqualified right for individuals to opt-out of targeted advertising**. The government has indicated that further consideration will be given to how to give individuals greater autonomy and control in this area, including through the introduction of layered opt-outs or industry codes.

A full list of the proposals and the government's view on each of them can be found in the table at the end of the Response.

While the Response is moderate in tone, it indicates a definite and deliberate intention to put proposed reforms into action in the near and medium term. All entities handling personal information in Australia should remain alert to future developments.

With thanks to Kirsten Foley, Alison Chen, Nicholas Langsworth and Liz Grimwood-Taylor for their work on this alert