

15 February 2019

By email: platforminquiry@accc.gov.au

Submission to the Australian Competition and Consumer Commission Digital Platforms Inquiry

The Australian Data Privacy Certification Register (ADPCR) thanks the Australian Competition and Consumer Commission (ACCC) for the opportunity to respond to the preliminary report relating to the digital platforms inquiry.

The ADPCR is a new independent privacy framework, committed to driving stronger privacy protection, transparency and control for Australians. The ADPCR launched on January 28, 2019 and has engaged several Australian businesses regarding independent privacy certification. The ADPCR has a strong consumer focus, offering privacy news, data breach alerts and assistance, privacy related fact sheets, research and advocacy services.

This submission will specifically address the matters proposed under Preliminary Recommendation 8 – Use and collection of personal information:

- a) Strengthen notification requirements
- b) Introduce an independent third-party certification scheme
- c) Strengthen consent requirements
- d) Enable the erasure of personal information

The ADPCR supports the recommendations made by the ACCC within the preliminary report and welcomes further consultation.



Jay Gilden
Executive Director – Marketing & Partnerships
Email: Jay.Gilden@adpcr.com.au
Phone: +61 413 579 459

(a) Strengthen notification requirements

The ADPCR strongly agrees with the ACCC's recommendation to strengthen data collection notification requirements. The principles that form the ADPCR framework are centred around strengthening data rights for individuals. The ADPCR believes that there is a need for greater transparency by organisations around how and why they collected data and clearer notification of any such collection.

Current privacy laws allow organisations to create and publish lengthy and confusing privacy policies that are not easily understood by an average individual.

When an individual provides personal or sensitive information directly or indirectly to an organisation, the ownership of that data should remain with the individual. The individual therefore does not relinquish their rights to control the storage, use and disclosure of that data when that data is shared with an organisation, and total control should remain with the individual at all times.

The ADPCR supports the implementation of a simplified privacy notice, which is clear, concise, and in plain language. Privacy notices should be easily understood by an individual, and should include:

1. The complete disclosure of all data being collected by an organisation about an individual. This includes the disclosure of any advertising tags or cookies that can be used to identify any behavioural or interest-based attributes of the individual.
2. An easy to understand outline of the purpose for which the organisation is collecting the individual's data, including for uses that relate to advertising, website security, user experience or website performance. If the data is being collected to provide a product or service, this should be disclosed to the individual and explicit consent should be obtained.
3. Information surrounding the intended use, storage and security of the individual's data. Use should be limited to the purpose that was disclosed at collection, and not for any other purpose except with the explicit consent of the user. This includes the sharing of data, except where explicit consent has been agreed upon.
4. Information surrounding how an organisation maintains the accuracy of the individual's data and allows the individual to access, correct or edit their data at any time, including information about how any individual can make those requests to an organisation.

5. An easy to understand outline of data deletion schedules as required by relevant legislation.
6. Information surrounding the measures taken by the organisation to ensure secure storage of the individual's data, detailing appropriate policies and systems to enable secure storage and deter misuse.

(b) Introduce an independent third-party certification scheme

The ADPCR strongly supports the recommendation to introduce an independent third-party certification scheme that would allow for an accredited certification body to certify an organisation's compliance with Australian privacy law.

The ADPCR currently offers a privacy certification scheme for organisations but is unable to certify an organisation's compliance with the Australian Privacy Principles (APP's) due to limitations enforced by Australian privacy law.

The introduction of an independent third-party certification scheme would simplify the role of the Office of the Australian Information Commissioner (OAIC) and would allow the OAIC to more rigorously enforce relevant privacy law.

The ADPCR proposes that an independent third-party certification scheme should:

1. Be overseen by the OAIC but be delegated to an accredited certification body that has the technical capabilities to service a certification framework at scale. This certification body should not be a government organisation.
2. Be compulsory for all Australian and Norfolk Island Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than \$3 million, all private health service providers and some small businesses in line with current rules that define which organisations must comply with the *Australian Privacy Act*.
3. Be voluntary for organisations that do not meet the required thresholds under Australian privacy law.
4. Allow for the accredited certification body to audit an organisation's certification status at any time.
5. Have a single certification device (also referred to as a seal) that can be easily recognised by an individual.

6. Maintain a certification register that is up to date and provides individuals with a summary of the organisation's purpose of collection and use of data.
7. Require re-certification on an annual basis, at the cost of the organisation.
8. Truly represent an individual's best interests and strive for the continued protection of those interests.

The accredited certification body should not only certify an organisation's compliance with Australian privacy law but should also have a strong focus on individuals over and above what a government organisation could sustain.

The accredited certification body should be required to support individuals with privacy related concerns, which would allow for the OAIC to focus resourcing on the creation of new privacy law, enforcement of existing privacy law, monitoring of the accredited certification body, management of privacy related disputes and complaints, management of the notifiable data breaches scheme, and management of proactive privacy related investigations.

Further, the ADPCR agrees that that OAIC should remain the enforcer and regulator of non-compliant businesses.

The separation between the accredited certification body and OAIC as the enforcement body is crucial, as it ensures a distinction between responsibilities. This separation dispels any potential conflicts of interest between certification and enforcement of non-compliance.

The ADPCR proposes that the accredited certification body would manage requests, queries and complaints relating to the certification organisations, while the OAIC would continue to manage complaints relating to breaches of privacy and Australian privacy law. This would remove the need to implement a digital platforms ombudsman to manage complaints regarding the conduct of digital platforms.

The ADPCR proposes that the accredited certification body would work with the OAIC to determine the privacy principles contained within the framework that organisations would be required to comply with to achieve certification.

The ADPCR agrees with the ACCC that Australia should not adopt all of the principles defined by the General Data Protection Regulation (GDPR), but notes that changes to Australian privacy law are required to ensure sufficient privacy protection for Australians. Many aspects of GDPR would provide immediate benefits for Australian individuals and should be considered.

(c) Strengthen consent requirements

The ADPCR strongly supports the ACCC's recommendation to strengthen consent requirements.

Australian privacy law does not clearly define valid consent, and this lack of criteria enables organisations to bury consent clauses deep within privacy policies and terms of service, which can result in the collection and use of an individual's data without their knowledge.

The ADPCR strongly believes that Australian privacy law should require organisations to seek and receive explicit consent from users before collecting any data about an individual, and that this principle should form a part of a certification framework.

The introduction of this principle would allow an individual to make an informed decision as to whether the benefit of engaging with an organisation is balanced with the use of their data.

Special provisions should be introduced to protect the interests of children, and vulnerable individuals such as the elderly or disabled.

(d) Enable the erasure of personal information

Currently, there are no provisions within the APP's that require an organisation to erase an individual's personal information upon request. An individual can request an organisation reviews whether the collection of their personal information is necessary, however this provision makes it difficult for an individual to revoke their consent.

The introduction of an explicit consent principle should allow for an individual to request immediate and complete deletion of their personal information, as long as deletion is not unlawful.

The ADPCR strongly supports the ACCC recommendation to implement changes to Australian privacy law that would allow for an individual to revoke consent and have their data erased.

The ADPCR proposes that erasure should be a compulsory and a uniform principle implemented as a condition of certification, and that changes to notification requirements should incorporate this principle with a clear and easy to understand notification that details how an individual can request erasure of their personal information.

Further, the ADPCR proposes that changes should be made to Australian privacy law and the APP's to incorporate a notice that reinforces to organisations that an individual does not relinquish their rights to their data when that data is shared with an organisation, and that an

organisation cannot use an individual's data outside of the stated purpose of collection, ensuring that total control remains with the individual at all times.

Summary

The ADPCR strongly supports the changes to Australian privacy law as proposed by the ACCC. The recommendations provide a well thought out and contemporary view on key privacy issues in the digital age.

The ADPCR welcomes further consultation from the ACCC should any matters above require clarification or further information.