# Submission to the Attorney-General's Department

# Privacy Act Review Report

March 2023

.auDA

**Table of Contents**

# Introduction

## Who is auDA?

.au Domain Administration Ltd ("auDA") is the administrator of the .au country code Top Level Domain (ccTLD). The .au ccTLD includes the following namespaces: .au, com.au, net.au, org.au, asn.au, id.au, vic.au, nsw.au, qld.au, sa.au, tas.au, wa.au, nt.au, act.au, edu.au, gov.au.

## auDA's role

As a critical part of the digital economy, auDA's role is to ensure the .au ccTLD remains stable, reliable and secure.

auDA performs the following functions:

- Ensure stable, secure and reliable operation of the .au domain (including the registry database, WHOIS service and Domain Name System (DNS) service at the top level and second levels), as part of Australia's suite of critical infrastructure.
- administer a licensing regime for .au domain names based in multi-stakeholder processes
- respond to enquires with regards to the licensing rules
- maintain and ensure compliance with the licensing rules
- maintain appropriate compliant and dispute resolution processes associated with the licensing rules
- license the .au registry operator
- accredit and license registrars
- Advocate for, and actively participate in, multi-stakeholder Internet governance processes both domestically and internationally.

## auDA's stakeholders

auDA operates under a multi-stakeholder model, working closely with suppliers, business users, non-profit organisations, consumers and the Australian Government.

It seeks to serve the interests of the internet community as a whole and takes a multi-stakeholder approach to internet governance, where all interested parties can have their say.

auDA belongs to a global community of organisations and plays an active role in representing .au at international fora, such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the Asia Pacific Top Level Domain Association (apTLD).

## auDA's advocacy principles

auDA's local and international advocacy is undertaken in accordance with the following key principles:

1. **Purpose driven** – we are a for purpose organisation. Our purpose is to:
   - administer a trusted .au domain for the benefit of all Australians
   - champion an open, free, secure and global internet.

   Our purpose serves our vision, which is to unlock positive social and economic value for Australians through an open, free secure and global internet.
2. **Multi-stakeholder Approach** - We take a multi-stakeholder approach to our work, and we advocate for multi-stakeholder approaches to internet governance and policy matters. This involves us working closely with domain industry stakeholders, businesses, not-for-profit organisations, education and training providers, consumers, and Government entities to serve the interests of the internet community as a whole. This approach is founded on strong relationships locally and globally.
3. **Independence** - We are independent from government and from the corporate sector. This means we operate transparently and openly in the interests of all Australians.
4. **Leadership** – We seek to lead Australia's internet community to work better together on our shared work to actively advance an open, free, secure and global internet and positively influence policy and outcomes related to internet governance. We do this through quality policy advice and analysis, through research and information, and by sharing this insight with those can benefit from it. Partnership is integral to our way of working – we often seek to work together with others who support our goal, to multiply our impact.
5. **Encouraging Innovation** – We support an innovative digital economy, and through our work we foster innovation across the technology sector, recognising its benefit to growing our digital economy and, in turn, benefitting all Australians. Legislative burdens can have a negative effect on innovation in the technology sector, so we encourage the use of incentives and self-regulation where possible and a consultative approach to regulation where that is needed.

# Background

Privacy law is an integral aspect to the way the digital world operates. Strong and effective privacy law, harmonised with other comparable jurisdictions, can improve and help secure positive digital lives for all Australians. This in turn contributes to auDA's purpose which is to unlock positive social and economic value from the free open secure and global internet.

This is the rationale for our submission in response to this consultation. Our input is generally supportive of the direction set out in the report, as it supports our vision. So, in response to the

Attorney-General's Department's (the Department) Privacy Act Review Report (the Report), auDA is pleased to offer the below comment.

# Submission

It is evident from the Discussion Paper that the Department proposes amendments to the Privacy Act to better protect individuals and businesses operating in the digital economy and move towards harmonisation with international privacy law. Ensuring Australia's privacy rules are fit for purpose in the digital age is crucial to promote public trust and confidence in the digital economy.

We note that the 116 proposals set out in the Discussion Paper are described at a principles level and several proposals are noted as being subject to further consultation. While the Report provides a clear picture of the future direction of the Privacy Act, several elements require further consultation and assessment.

auDA considers it important that amendments made to the Privacy Act are clear, fit-for-purpose and do not lead to unintended consequences for Australians.

Below, we provide comments on select Proposals. These comments offer views about the proposed changes and sometimes provide real or hypothetical examples to help illustrate our arguments. Our intention is to add depth and some technical expertise to the Department's consideration of the issues we comment on.

## Addressing select Proposals

### Personal information, de-identification and sensitive information

**Proposal 4.1 Change the word 'about' in the definition of personal information to 'relates to'. Ensure the definition is appropriately confined to where the connection between the information and the individual is not too tenuous or remote, through drafting of the provision, explanatory materials and OAIC guidance.**

**Proposal 4.2 Include a non-exhaustive list of information that may be personal information to assist APP entities to identify the types of information that could fall within the definition. Supplement this list with more specific examples in the explanatory materials and OAIC guidance.**

**Proposal 4.5 Amend the definition of 'de-identified' to make it clear that de-identification is a process, informed by best available practice, applied to personal information which involves**

**treating it in such a way such that no individual is identified or reasonably identifiable in the current context.**

**Proposal 4.6 Extend the following protections of the Privacy Act to de-identified information:**

- **APP 11.1 – require APP entities to take such steps as are reasonable in the circumstances to protect de-identified information: (a) from misuse, interference and loss; and (b) from unauthorised re-identification, access, modification or disclosure.**
- **APP 8 – require APP entities when disclosing de-identified information overseas to take steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles in relation to de-identified information, including ensuring that the receiving entity does not re-identify the information or further disclose the information in such a way as to undermine the effectiveness of the de-identification.**
- **Targeting proposals – the proposed regulation of content tailored to individuals should apply to de-identified information to the extent that it is used in that act or practice.**

The proposed wording change (**Proposal 4.1**) brings the definition in line with other Commonwealth legislation as well as the GDPR definition of 'personal data'. This change from 'about' to 'relates to' an individual for the definition of personal information may substantially broaden the information previously and currently collected by entities subject to the Act, and have practical implications for entities' existing data holdings, systems, and internal policies. We suggest the Department considers such potential implications in further consultations.

Including a non-exhaustive list of types of personal information (**Proposal 4.2**) in the legislation itself would be useful particularly to those organisations that may not use the current OAIC guidance and explanatory material. However, we express our concern that such a list may not be able to keep pace with the technological advancement and the changing nature of technical data, and therefore become outdated quickly. Maintaining such a list as part of guidance material would preserve the technological neutrality of the Privacy Act. If such a list was included in the legislation, it would have to remain flexible and technology-neutral and clarify that listed types of personal information are not treated as exhaustive. Further, it would have to be clarified that listed types of personal information would still have to satisfy the primary elements of the definition of personal information, and that it will depend on the current context as to whether the information actually qualifies as personal information.

Entities subject to the Privacy Act would benefit from clear guidance as to what constitutes 'current context' with regards to the risk of re-identification of previously de-identified information (**Proposal 4.5**).

Subject to the precise wording of the legislative amendments to the Privacy Act, the increased obligations regarding de-identified information (**Proposal 4.6**) could impose additional burden on entities which have based their existing operations and processes on the fact that de-identified information currently sits outside the protections of the Privacy Act. Proposed amended obligations regarding de-identified information may have ramifications for

organisations' current data processing and systems, and may impose additional compliance costs on industry.

By way of example, extending APP 11.1 to de-identified information may pose practical challenges for organisations deploying technologies such as data analytics and artificial intelligence. Such technologies often intentionally de-silo data sets to gain in-depths business/customer insights. Keeping de-identified information separate from 'other' personal information to avoid the risk of re-identification, may impose additional compliance costs and disincentivise organisations to invest in digital transformation. Supplementary guidance to better understand the 'reasonable steps' to take to protect de-identified information would be helpful. We encourage the Department to further consult on the potential practical implications of such amendments.

## Small business exemption

**Proposal 6.1 Remove the small business exemption, but only after:**

a) **an impact analysis has been undertaken to better understand the impact removal of the small business exemption will have on small business - this would inform what support small business would need to adjust their privacy practices to facilitate compliance with the Act**
b) **appropriate support is developed in consultation with small business**
c) **in consultation with small business, the most appropriate way for small business to meet their obligations proportionate to the risk, is determined (for example, through a code), and**
d) **small businesses are in a position to comply with these obligations.**

We are generally supportive of the removal of the small business exemption but only *after*

- an impact analysis has been completed,
- support of appropriate scope and scale has been developed,
- the most appropriate way for small businesses to meet their obligations is determined and
- small businesses are in a position to comply with the obligations imposed by the Privacy Act.

Considering the increase in data collection, use and disclosure across the Australian economy and the Government's efforts to accelerate the expansion of the digital economy, it is our view that businesses of all sizes should strive to ensure the data privacy of their customers is safeguarded. In line with other consumer protection frameworks

, Australians should be able to expect a baseline of protection across businesses of all sizes. The removal of the exemption helps to standardise privacy protections for Australians across the economy and brings privacy protections in step with community expectations. Our support for the removal of the exemption is underpinned by the latest research findings from the Consumer

Policy Research Centre (CPRC), which highlight that consumers perceive the harms from "*poor data practices*" by businesses to be the same regardless of their size. More precisely, the majority of Australians (82 per cent), shared the view that "*small businesses should not collect personal information [..] if they cannot make sure it is safe and secure*."

We believe that the removal of the exemption benefits small businesses in the long term, notwithstanding the transitional costs involved, as increased data privacy and security measures will 'legitimise' their operations in the digital economy and make them an equal and more attractive trading partner for larger businesses, thereby creating economic opportunities for small businesses.

Removing the exemption will also ensure that Australia can become eligible for an adequacy finding under GDPR, ending the current lockout that small businesses face in offering services to European customers. This is of particular relevance considering global supply chains and small businesses' ability to partake as trading partners in cross-border supply chains. The Department, in cooperation with small business associations (such as COSBOA) and peak bodies representing the technology industry, could consider exploring opportunities to encourage small businesses to engage in the digital economy.

We note that the 'long term vision' of the exemption removal lacks a clear timeline (i.e., it is uncertain whether it will be months or years until the exemption removal comes into effect). Clarification of when appropriate resources and notice to small businesses will be provided would be beneficial.

## Privacy policies and collection notices

**Proposal 10.3 Standardised templates and layouts for privacy policies and collection notices, as well as standardised terminology and icons, should be developed by reference to relevant sectors while seeking to maintain a degree of consistency across the economy. This could be done through OAIC guidance and/or through any future APP Codes that may apply to particular sectors or personal information-handling practices.**

It is our view that a standardised format for privacy policies and collection notices provides better protection to individuals' privacy by allowing consumers to develop expertise in reviewing and understanding the scope of such policies and notices. Standardised templates would also make it easier for individuals to digest large amounts of information regarding privacy law (thus minimising information fatigue), compare different providers and services, and help consumers being more confident when engaging in the digital economy. 'Privacy-by-design' principles should inform the development of those templates to ensure that only information that is needed for basic functionality of the service/application is collected. The CPRC's conclusion that

[1] CPRC (2023): Not a fa r trade Consumer v ews on how bus nesses use the r data, p. 18, 29 March 2023, ava ab e at: CPRC work ng paper Not a fa r trade March 2025.pdf (accessed on 30 March 2023).

the majority of Australian (79 per cent) agree that businesses should only collect information required to deliver relevant products or services, further reiterates this suggestion.[2]

It is our view that form and content of privacy policies and collection notices should be as simple, short, and comprehensible as possible. However, care should be taken not to oversimplify complex concepts that prevail certain sectors.

We agree that prior to the implementation of standardised templates, consumer comprehension testing should be conducted to ensure that standardisation is effective and benefits consumers. In this regard, we echo and reiterate the CPRC's[3] suggestion to involve representative samples of the Australian population in such consumer comprehension testing research and include people of different age groups, from various ethnic backgrounds, with different levels of digital literacy etc.

As noted in the Report, it would be impractical to develop one standardised template to be applicable across all entities subject to the Privacy Act. Instead, templates that reflect industry-specific practices, while attempting to maintain certain levels of uniformity and consistency across the economy, would be of greatest value for consumers. The development of such templates and layouts for privacy policies and collection notices should be undertaken in cooperation with industry.

## People experiencing vulnerability

**17.1 Introduce, in OAIC guidance, a non-exhaustive list of factors that indicate when an individual may be experiencing vulnerability and at higher risk of harm from interferences with their personal information.**

The rapid advancement in new technologies suggests that the scale and nature of vulnerability in the digital age are changing quickly. Technological trends such as Artificial Intelligence (AI) and Internet of Things (IoT) are set to continue. They will be accompanied by emerging trends such as immersive technologies (e.g., augmented and virtual reality). These evolutions will require swift and innovative approaches to foster digital inclusion and guarantee the rights and privacy of all Australians.

Several members of society continue to be disproportionately vulnerable – particularly disadvantaged, marginalised, minorities, and underrepresented groups. auDA's research on Digital Lives of Australians 2022 found that older Australians are generally less confident in their ability to undertake common online activities. Also, Australians with hybrid work arrangements

[2] CPRC (2023): Not a fa r trade Consumer v ews on how bus nesses use the r data, p. 4, 29 March 2023, ava ab e at: CPRC work ng paper Not a fa r trade March 2025.pdf (accessed on 30 March 2023).
[3] CPRC (2022): Subm ss on to the Attorney Genera 's Department Pr vacy Act Rev ew D scuss on Paper, 10 January 2022, ava ab e at: Response 415346702 to Pr vacy Act Rev ew D scuss on paper Attorney Genera 's Department C t zen Space (ag.gov.au) (accessed on 24 March 203).

feel more vulnerable to cyber security threats and other forms of online harms.[4] These and other groups listed in the Privacy Act Review Report may lack the technical, critical and social skills to engage with the internet and more specifically digital service providers in a safe and beneficial manner. Certain practices performed by digital platforms including profiling or targeting based on identified or inferred vulnerabilities may magnify the harms these vulnerable consumers could face.

In today's online environment, most if not all of us can be vulnerable at different times and in different contexts. The guidance to be developed by the OAIC should take a human-centric and people-focused approach and empower all members of society. It should also consider the growing digital environment within which our lives and work take place, and which often poses greater risk of privacy harms. A list of situational factors and circumstances that pose risks can significantly enhance individual's ability to recognise online threats, deploy preventative measures to protect themselves from harm, or seek help from trusted sources/authorities.

## Rights of the individual

**18.3 Introduce a right to erasure with the following features:**

a) **An individual may seek to exercise the right to erasure for any of their personal information.**
b) **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.**
c) **In addition to the general exceptions, certain limited information should be quarantined rather than erased on request, to ensure that the information remains available for the purposes of law enforcement.**

**18.5 Introduce a right to de-index online search results containing personal information which is:**

i. **sensitive information [e.g. medical history]**
ii. **information about a child**
iii. **excessively detailed [e.g. home address and personal phone number]**
iv. **inaccurate, out-of-date, incomplete, irrelevant, or misleading**

**The search engine may refer a suitable request to the OAIC for a fee. The right should be jurisdictionally limited to Australia.**

[4] auDA (2022): D g ta L ves of Austra ans 2022 Research Report, 2022, p. 17, ava ab e at: auda d g ta ves of austra ans 2022 research report 171122.pdf (accessed on 15 March 2023).

Granting individuals greater control over their personal information reflects community expectations and fosters trust and confidence in the digital economy. Should a right to erasure be introduced (**Proposal 18.3**), it should be aligned with the GDPR to the greatest extent possible in order to avoid regulatory fragmentation, particularly for globally operating entities that have to comply with several privacy frameworks.

De-indexing of webpages containing personal information from the results on that search, can help individuals to protect their privacy. This is particularly important in cases where personal information may be sensitive and/or vulnerable to online harms. We note that only the search result is removed, not the content itself, which remains at its source on the internet.

We agree with the OAIC that there is a case for the right to de-index, particularly where attempts made by individuals to get their information removed from the source, were ignored, or are not feasible due to the source residing overseas or being anonymous. we caution that it is likely for situations to emerge, where individuals request to de-index search results containing what they perceive to be 'misleading' information, whereas other individuals consider the information as relevant and useful.

We reiterate that – unless executed for legitimate purposes as outlined in the proposal – the right to de-index can be a form of censorship if it is conducted in the absence of appropriate oversight.

## Automated decision-making

**Proposal 19.1 Privacy policies should set out the types of personal information that will be used in substantially automated decisions which have a legal or similarly significant effect on an individual's rights.**

**Proposal 19.2 High-level indicators of the types of decisions with a legal or similarly significant effect on an individual's rights should be included in the Act. This should be supplemented by OAIC Guidance.**

**Proposal 19.3 Introduce a right for individuals to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made. Entities will be required to include information in privacy policies about the use of personal information to make substantially automated decisions with legal or similarly significant effect.**

**This proposal should be implemented as part of the broader work to regulate AI and ADM, including the consultation being undertaken by the Department of Industry, Science and Resources.**

We believe that the proposals would benefit from more clearly outlined definitions of "*legal or similarly significant effect*" (**Proposal 19.1**) and "*high-level indicators of the types of decisions*"

(**Proposal 19.2**) as the terminology currently used appears to be broad and vague. Such matters could be addressed in the OAIC Guidance.

To ensure individuals have sufficient understanding about the rationale for automated decisions (**Proposal 19.3**), the requested '*meaningful information*' will need to be jargon-free and comprehensible by Australian consumers. The information should not only explain how the decision was made and what information was used to derive at the decision, but also the reasoning behind the decision (explainability of Automated Decision-Making (ADM) outcomes). Rather than providing the affected individual with incomprehensible 'raw data' which would require expert knowledge to interpret, the information should enable an individual to interrogate the results, identify potential errors and enable them to exercise other rights to contest the decision made. This is consistent with recommendations made in the Australian Human Rights Commission's (AHRC) Report[5] and the OECD Recommendation[6].

We note that the Report does not propose to provide individuals with the right to have decisions reviewed by a human/individual. Further consultations conducted by the Attorney-General's Department and the Department of Industry, Science and Resources should consider making automated decisions subject to review, preferably internal human review. The individual, as subject of the decision, must be informed of that review option. This suggestion is consistent with the Ombudsman's Guide[7] as well as the OECD Recommendations and the AHRC Report.

If the proposals are approved, those organisations deploying ADM systems will be required to revise their processes and policies to comply with the obligations. They will also have to consider how their disclosures about the use of personal information in ADM processes are provided to individuals before the information is collected and used, and prepare responses to individuals who seek meaningful information about how the automated decisions are made. Guidance material and examples provided by the OAIC may be helpful for organisations deploying ADM. Further, a standardised process on the disclosure of such information could be considered.

## Direct marketing, targeting and trading

**20.2 Provide individuals with an unqualified right to opt-out of their personal information being used or disclosed for direct marketing purposes.**

**Similar to the existing requirements under the Act, entities would still be able to collect personal information for direct marketing without consent, provided it is not sensitive information and the individual has the ability to opt out.**

---

[5] AHRC (2021): Human R ghts and Techno ogy F na Report 2021, ava ab e at: AHRC R ghtsTech 2021 F na Recommendat ons.pdf (humanr ghts.gov.au) (accessed on 15 March 2023).
[6] OECD (2019): Recommendat on of the Counc on Art f c a nte gence, ava ab e at: OECD Lega nstruments (accessed on 15 March 2023).
[7] Commonwea th Ombudsman (2023): Automated Dec s on Mak ng Better Pract ce Gu de, ava ab e at: OMB1188 Automated Dec s on Mak ng Report F na A1898885.pdf (ombudsman.gov.au) (accessed 25 March 2023).

The right to opt-out of direct marketing raises important questions about individuals' privacy, access to information on the internet, and innovation and the digital economy. While such a right can help protect individuals' privacy, enhance their control over personal information, and increase trust in internet-based services, its implementation should be carefully balanced with the potential implications for consumers, businesses and digital service providers.

The CPRC proposes to provide consumers with an opt-in option.[8] Opting-in as opposed to option-out gives the consumer more control over their data as they would have to actively subscribe to receive personalised advertisements. This alternative option could be considered by the Department for further consultations.

Direct marketing can have significant benefits for businesses, particularly small businesses. The right to opt out of the collection and use of personal information could also have implications for innovation and the acceleration and growth of the digital economy. For example, businesses may become hesitant to invest in digital technologies or services that help them acquiring and servicing new customers, thereby negatively affecting the growth of the digital economy. As such, the proposals need to strike the right balance between business needs and enhancing consumers' privacy protection. The proposal as it stands, does not seem to take into consideration the implications of the extended definition of personal information (see our comments on **Proposals 4.1** and **4.6**). The Department should consider these implications in its further consultation process.

## Security, Destruction and Retention of Personal Information

**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 Guidelines 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.**

**21.5 The OAIC Guidelines in relation to APP 11.2 should be enhanced to provide detailed guidance that more clearly articulates what reasonable steps may be undertaken to destroy or de-identify personal information.**

The .au DNS is recognised as a critical infrastructure asset under the SOCI Act. The SOCI Act contains security requirements for the .au supply chain that includes auDA, the .au registry operator and auDA accredited registrars. We engage with registrars on our shared security responsibilities.

[8] CPRC (2023): Not a fa r trade Consumer v ews on how bus nesses use the r data, 29 March 2023, p. 14, ava ab e at: CPRC work ng paper Not a fa r trade March 2025.pdf (accessed on 30 March 2023).

Considering the threat environment, we are in favour of a more consistent update of foundational cyber security mechanisms and controls across the economy and the establishment of a 'cyber security baseline'. We see the Privacy Act and 2023-2030 Australian Cyber Security Strategy as an important tool to contribute to a general cyber security and privacy uplift and welcome further direction as to how these two processes (and guidance/legislation) will interact.

With respect to destroying or de-identifying personal information (**Proposal 21.5**), some organisations may benefit from guidance that clearly outlines the 'reasonable steps' entities are expected to take. Further, considering the controller-processor concept proposal (see our comment to **Proposal 22.1**), it remains unclear whether the responsibility to destroy/de-identify personal information, should sit with the controller.

## 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.**

Amending the Privacy Act to introduce the concepts of 'processors' and 'controllers' in a manner that is consistent with the GDPR, is reasonable. The introduction of the concept of controllers and processors enables Australia to better engage with other digital economies. Further, the controller-processor distinction provides consumers with more clarity with respect to exercising their rights.

## Overseas Data Flow

**Proposal 23.2 Introduce a mechanism to prescribe countries and certification schemes as providing substantially similar protection to the APPs under APP 8.2(a).**

We are supportive of **Proposal 23.2**. A mechanism to prescribe countries and certification schemes as providing substantially similar protection to the APPs under APP 8.2(a), would provide greater certainty on other jurisdictions' laws or schemes that afford substantially similar protection. Not only would the introduction of such mechanism enhance entities' operational efficiency with respect to cross-border data flows, but also provide consumers with appropriate safeguards. Proposed certification schemes should not be overly restrictive in nature to leverage the social and economic benefits of cross-border data flows as opposed to encouraging the adopting of undesirable data localisation policies.

## Notifiable Data Breach Scheme

**28.1 Undertake further work to better facilitate the reporting processes for notifiable data breaches to assist both the OAIC and entities with multiple reporting obligations.**

**28.2 Amend paragraph 26WK(2)(b) to provide that if an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of the entity, the entity must give a copy of the statement to the Commissioner as soon as practicable and not later than 72 hours after the entity becomes so aware, with an allowance for further information to be provided to the OAIC if it is not available within the 72 hours.**

**Amend subsection 26WL(3) to provide that if an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of an entity the entity must notify the individuals to whom the information relates as soon as practicable and where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases as soon as practicable.**

**Require entities to take reasonable steps to implement practices, procedures and systems to enable it to respond to a data breach.**

As critical infrastructure asset, auDA complies with the obligations under the SOCI Act. The SOCI Act requires entities to report data breaches using a standardised and approved form. We believe that there is benefit in keeping reporting schemes as consistent as possible, and support the Department's initiatives (**Proposal 28.1**) to assess and create practical solutions to ensure breaches are reported correctly and those with multiple reporting obligations are not unnecessarily burdened. Such suggestions are aligned with recommendations by the Productivity Commission, which argues that cyber incident reporting should be streamlined and occur via a single online interface.[9]

It is our understanding that the Department of Home Affairs is in the process of establishing a Cyber Security Coordinator that will be supported by the National Office for Cyber Security within the Department of Home Affairs: "*In a cyber incident, they [the Coordinator] will coordinate work across government, to support a streamlined response and help manage the consequences for everyday Australians […].*" [0] In our view, streamlined and better breach reporting enables the Government to improve its breach intelligence and, in turn, the development of mitigating and preventative measures.

According to **Proposal 28.2**, entities would be required to notify the Commissioner of an eligible data breach not later than 72 hours after the entity becomes aware of the breach, with an allowance for further information to be provided to the Commissioner if such information is not available within 72 hours. While such changes to the Privacy Act better reflect community

[9] Product v ty Comm ss on (2023): 5 year Product v ty nqu ry: Advanc ng Prosper ty Recommendat ons and Reform D rect ves, March 2023, ava ab e at: Recommendat ons and Reform D rect ves Advanc ng Prosper ty (pc.gov.au) (accessed on 17 Marc 2023).

[10] See C are O'Ne 's MP speech at the Austra an nformat on Secur ty Assoc at on's (A SA) Austra an Cyber Conference 2023, 22 March 2023.

expectations – that individuals will be notified quickly if their personal data has been compromised – those changes may raise practical issues for entities around the ability to identify whether a data breach gives rise to a risk of serious harm and reinforces the need for entities to have in place clear and concise data breach notification plans. Provided that the small business exemption is approved, those businesses would require guidance and support developing and executing such plans (see also our comment on **Proposal 6.1**).

While the NDB scheme was effective in raising awareness around the importance of breach reporting, we agree that more needs to be done to prevent data breaches from occurring. Cyber resilience and support for small business to improve their cyber security are policy priority areas in the Department of Home Affairs' current consultation on the 2023-2030 Australian Cyber Security Strategy, and we suggest both Departments coordinate their efforts to address those matters in a coherent manner.

## Interactions with other schemes

**29.1 The Attorney-General's Department develop a privacy law design guide to support Commonwealth agencies when developing new schemes with privacy-related obligations.**

**29.2 Encourage regulators to continue to foster regulatory cooperation in enforcing matters involving mishandling of personal information.**

**29.3 Establish a Commonwealth, state and territory working group to harmonise privacy laws, focusing on key issues.**

We strongly support cooperation and collaboration between regulators. As noted in the Report, the DP-Reg is a good example of several government entities and regulators working together on cross-cutting policy issues relating to the regulation of digital platforms, including privacy and data issues. By way of example, we note that members of the Council of Financial Regulators (CFR) have been involved in and/or led public consultations addressing multiple policy issues that overlap with the DR-Reg's regulatory reform agenda.

To avoid siloes and overlapping consultation processes facilitated by different regulators, and drive greater certainty amongst industry and consumers, auDA suggests a preferred approach would see *all* relevant regulators *and* policymakers actively participate in a multi-stakeholder policy development approach to harmonise privacy laws, and relevant policies that cut across privacy and data matters. Such an approach is aligned with the ANU Tech Policy Design Centre's

[11] See e.g. Treasury (2023): Consu tat on on D g ta P atforms Government consu tat on on ACCC's regu atory reform recommendat ons, December 2022 February 2023, ava ab e at: D g ta P atforms Consu tat on on Regu atory Reform | Treasury.gov.au (accessed on 15 March 2023); see a so Par amentary Jo nt Comm ttee on Corporat ons and F nanc a Serv ces (2021): nqu ry nto Mob e Payment and D g ta Wa et F nanc a Serv ces, October 2021, ava ab e at: Mob e Payment and D g ta Wa et F nanc a Serv ces (aph.gov.au) (accessed on 15 March 2023).

(TPDC) proposed Tech Policy and Regulator Coordination Council (TPR-CC).[2] Membership would consist of regulators *and* policymakers. The TPR-CC as an advisory and coordination body would help improving the overall effectiveness of regulation development process by enhancing coordination, improving transparency and democratic oversight of *all* actors in the tech-ecosystem, while respecting and preserving the independence of regulators.

In this regard, we note that privacy, cyber security, and digital identity remain priority policy items on the ministerial agenda.[3] Data and privacy are the common denominator between all three policy matters, and reforms in each domain will directly impact the others. Despite this, each will be subject to different approval processes within government. We urge the responsible regulators and departments to make a concerted effort to foster cooperation between all regulators (**Proposal 29.2**) and policymakers across Commonwealth, state and territory levels (**Proposal 29.3**).

Regarding the international alignment of privacy laws and other relevant policy development, the recently released ANU Tech Policy Design Centre's (TPDC) Global Tech Policy Atlas, a public repository of national and international tech policy, strategy, legislation and regulation, is suggested as a useful way in which stakeholders may remain abreast of international policy developments and overseas regulators' experiences.

Lastly, the shape and format of the proposed privacy law design guide (**Proposal 29.1**) could be informed by the Tech Policy Design Kit developed by the TPDC in collaboration with the Tech Council of Australia and the Digital Technology Taskforce in the Department of Prime Minister and Cabinet (PMC). The Design Kit is user-friendly, easy to understand, and takes into consideration relevant stakeholders involved in and affected by law reforms.

# Conclusion

We suggest that a multi-stakeholder approach becomes the 'default' approach when the Australian Government consults on cross-border digital and privacy policy matters.

We recommend that practical implications and ramifications of proposed amendments are considered in further consultation processes.

[12] TPDC (2022): Tend ng the Tech Ecosystem who shou d be the tech regu ator(s)?, May 2022, ava ab e at: TPDC Report NO1 2022 d g ta re ease.pdf (anu.edu.au) (accessed on 17 March 2023).
[13] See Department of F nance (2023): Data and D g ta M n sters Meet ng Commun que, 24 February 2023, ava ab e at: data and d g ta m n sters meet ng commun que 240223.pdf (f nance.gov.au) (accessed on 27 February 2023).

We thank you for considering these matters. If you would like to discuss our submission, please contact auDA's [redacted], [redacted] on [redacted]

.au Domain Administration Ltd
www.auda.org.au

PO Box 18315
Melbourne VIC 3001
info@auda.org.au