

Australian Information Industry Association

Submission on

**Privacy Amendment (Personal Data Protection)
Bill 2026**

About the AIIA

The Australian Information Industry Association (AIIA) is the nation's peak body for those in the digital ecosystem, leading strategic policy and advocacy to shape a thriving digital sector. Through strong engagement with government, industry, and the broader community, the AIIA ensures the voice of its members informs decision-making on technology, innovation, and digital capability.

Membership provides direct access to influential networks, premium events, and opportunities to collaborate on initiatives with the sector's best and brightest to drive industry growth, improve productivity, and secure Australia's place as a global technology leader. AIIA members access real collaboration, real connections, and real outcomes.

Introduction

The AIIA welcomes the opportunity to respond to the exposure draft of the Privacy Amendment (Personal Data Protection) Bill 2026 (the Bill) and the accompanying consultation paper.

A modern privacy regime matters both for the economy and for citizen trust in the adoption and use of new technology. New obligations placed on the technology industry should be proportionate, should not result in regulatory duplication, and should deliver a genuine uplift in protections rather than a compliance exercise.

This submission does not address every measure in the package. It concentrates on the areas where the drafting will have the greatest practical consequences for the digital ecosystem, and where targeted amendment would improve workability without weakening the protections the Bill is designed to deliver.

Summary of recommendations

Legitimate interests and the fair and reasonable test

1. Recognise a category of legitimate interests, so that documented reliance on a recognised interest is taken to satisfy proposed APP 3.
2. Define legitimate interest consistently with the GDPR and the frameworks influenced by it, with an indicative, non-exhaustive list in the Act.
3. Expressly recognise network and information security as a legitimate interest, consistent with Recital 49.

Controller–processor distinction

4. Align the definitions of controller and processor with those used in overseas laws.
5. Confine processor responsibilities to following lawful instructions, keeping data secure, notifying the controller of a breach, and assisting with investigation and remediation.
6. Confirm that processors do not report breaches directly to the Commissioner.
7. Confirm that processors do not bear user-facing obligations, including opt-out requests.

De-identified information

8. Clarify that where re-identification safeguards are in place, disclosure of de-identified information is not a disclosure of personal information.
9. Ensure obligations on de-identified data do not impede cross-border sharing required for cyber security purposes.

Trading and direct marketing

10. Confine the trading and direct marketing provisions to personal information, excluding de-identified, aggregated and cohort-level information.
11. Retain proposed APP 7.1 as drafted.

Security, destruction and retention

12. Have the APP 11 destruction obligation acknowledge statutory retention requirements, including those under foreign legislation.

Notifiable data breaches

13. Replace the complete 72-hour report with a flexible first alert, with further detail to follow.
14. Remove the requirement in proposed s 26WK(3)(e) to describe steps taken or intended.

15. Provide safe harbour relief for entities that meet published standards, report in a timely way, act in good faith and exercise due diligence.

Right to erasure

16. Limit the grounds for erasure consistently with Article 17, with regard to law enforcement requirements.
17. Maximise the cases in which quarantine or de-identification satisfies the right.
18. Provide an exception where the information is required for a transaction or contract.
19. Acknowledge statutory retention requirements, including those under foreign legislation.
20. Consider counterbalancing the right against an entity's legitimate interests, as under Article 21.

Matters not addressed

21. Remove the small business exemption, subject to staged application and a smaller penalty regime for SMEs.

Implementation and transition

22. Stage commencement on the face of the Bill, with education, support and an appropriate transition period.

1. Legitimate interests and the fair and reasonable test

The AIIA supports the introduction of a single, principles-based standard for the handling of personal information. Consolidating the requirements presently contained in APPs 3, 4 and 6 into proposed APP 3 represents a genuine simplification, and the factors set out in APP 3.2 reflect considerations that responsible entities already apply.

The difficulty lies in the certainty the framework affords. Proposed APP 3 establishes a standard but provides no means by which an entity may demonstrate, in advance and on a durable basis, that a given practice satisfies it. Each collection, use and disclosure must be assessed by weighing seven factors, none of which is determinative, and that assessment remains open to being weighed differently by the Commissioner at a later time. For settled and uncontroversial practices, this produces an ongoing exposure that is disproportionate to the privacy risk involved.

A legitimate interests principle, integrated with the fair and reasonable test, would address this. The AIIA does not propose a second and separate requirement. The fair and reasonable standard should continue to govern all handling of personal information; what is sought is a defined pathway through that standard. Reliance on the pathway would be optional, and an entity that prefers to assess a practice against the legislated factors directly would remain free to do so.

Recommendation One: The Act should recognise a category of legitimate interests, and provide that where an entity handles personal information in reliance on a recognised legitimate interest and has documented an assessment addressing the nature of the interest, the necessity of the handling for that interest and the impact of the handling on the individual, the handling is taken to satisfy proposed APP 3.

It is important that legitimate interest be defined consistently with the definition under the General Data Protection Regulation¹ and the overseas frameworks influenced by it. Many global organisations already rely on that basis in their established processes and practices. A divergent characterisation in Australian law would require the construction of a separate domestic analysis for identical activities, introducing uncertainty into the processing and flow of data internationally without any corresponding benefit to individuals.

Recommendation Two: Legitimate interest should be defined consistently with the General Data Protection Regulation and the overseas frameworks influenced by it, and an indicative and non-exhaustive list of recognised interests should be included in the Act.

¹Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1 ('GDPR').

Network and information security is the clearest illustration of the need. Protecting systems and customers requires the routine handling of personal information, including the scanning of IP addresses and traffic metadata, the inspection of applications hosted in cloud environments, and the sharing of indicators of compromise with other organisations and across national boundaries. Consent is not available as a mechanism for any of this. Recital 49 of the General Data Protection Regulation addresses the position directly, recognising that processing to the extent strictly necessary and proportionate to ensure network and information security constitutes a legitimate interest of the controller, and extending that recognition to computer emergency response teams, computer security incident response teams, providers of electronic communications networks and services, and providers of security technologies and services.² The nearest equivalent in the Bill is the permitted general situation concerning unlawful activity or serious misconduct relating to an entity's own functions,³ which is directed at responding to suspected wrongdoing rather than to preventive security operations, and does not address the position of a security provider handling information in order to protect a third party.

Recommendation Three: Network and information security should be expressly recognised as a legitimate interest, consistent with Recital 49 of the General Data Protection Regulation.

2. The controller–processor distinction (Schedule 6)

The introduction of a controller–processor distinction is the most consequential structural improvement in the Bill. The distinction will reduce confusion and compliance burden and increase the Act's efficiency by allocating responsibilities relating to notification, consent and security in accordance with the different roles of data controllers and processors. It means that obligations reflect an organisation's actual role in interfacing with customer data, providing vital privacy safeguards with regard to risk and practicality. It will also place privacy protections with the controller of the data, being the business owner who has the direct relationship with the consumer and may have multiple databases, technology suppliers and platforms.

The concepts of controllers and processors have existed for more than forty years and are key parts of global privacy and data protection frameworks including the OECD Privacy Guidelines, Convention 108, the APEC Privacy Framework and ISO/IEC 27701.⁴ To realise

²GDPR (n 9) recital 49.

³Exposure Draft Bill (n 1) sch 2 pt 2, proposed s 16A(1) item 2.

⁴AIIA 2023 Submission (n 4). See OECD, *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD Doc C(80)58/FINAL (as amended, 11 July 2013); *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, opened for signature 28 January 1981, ETS No 108 (entered into force 1 October 1985); Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2015); International Organization for Standardization and International Electrotechnical Commission, *ISO/IEC 27701:2019 — Security Techniques: Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management* (2019).

the benefits of interoperability, it is important that the definitions adopted in Australian law align with the definitions used in those frameworks.

Recommendation Four: The definitions of controller and processor under Australian law should align with the definitions used in overseas laws such as the General Data Protection Regulation, in order to realise the benefits of interoperability.

The responsibilities of a processor

The AIIA submits that processors should have responsibilities to:

- follow the controller's reasonable and lawful instructions;
- keep data secure;
- notify the controller of a data breach to the extent it does or should be aware of it; and
- provide reasonable assistance to the controller in remedying and investigating the breach.

We note that proposed s 6A(2A) preserves direct responsibility for processors under APP 1 and APP 11, which is consistent with the second of these responsibilities.

Recommendation Five: Processor responsibilities should be confined to following the controller's reasonable and lawful instructions, keeping data secure, notifying the controller of a data breach, and providing reasonable assistance to the controller in remedying and investigating the breach.

We do not believe it is reasonable for a processor to have an obligation to directly report breaches to the Information Commissioner, as the processor will not have all the necessary information to assess the impact of the data breach. Schedule 6 operates in relation to the Australian Privacy Principles and registered APP codes. We ask that the Bill also confirm the position under Part IIIC of the Act, so that the notification obligation rests with the controller.

Recommendation Six: The Bill should confirm that processors do not bear an obligation to report data breaches directly to the Information Commissioner, as a processor will not have all the information necessary to assess the impact of the breach.

We further submit that data processors should not have user-facing obligations regarding personal data. These are better assigned to controllers who have greater control and visibility over the personal data they collect.

Recommendation Seven: The Bill should confirm that processors do not bear user-facing obligations, including in relation to opt-out requests, those obligations being appropriately assigned to controllers.

3. De-identified information

The definition of de-identified in proposed s 6FG, and the concept of information that is reasonably available in proposed s 6FF, should be modified to clarify that where an entity has implemented mechanisms to prevent re-identification, disclosures of de-identified information fall outside the scope of a disclosure of personal information.

The need for that clarification arises from the interaction between the definition of de-identified and the definition of trade. Where an entity shares data with an organisation that has the ability to re-identify the information, that sharing would be treated as a disclosure of personal information. Entities consequently have no reliable basis on which to treat any de-identified dataset as falling outside the scope of the Act, which discourages the use of de-identification as a privacy-protective measure.

Recommendation Eight: The definition of de-identified should be modified to clarify that where an entity has implemented mechanisms to prevent re-identification, disclosures of de-identified information fall outside the scope of a disclosure of personal information.

The extension of data processing protections to de-identified data also warrants attention. For cyber security purposes, the sharing of information, including de-identified data, is essential to addressing and mitigating threats and vulnerabilities, especially when those threats cross international boundaries and require international transfers of the data.

Recommendation Nine: The utility of de-identified data in cyber security use cases should be accounted for, so that obligations attaching to de-identified information do not restrict or add compliance burden to transfers required to address threats and vulnerabilities across international boundaries.

4. Trading and direct marketing

The breadth of the trading provisions

Proposed s 6FC defines a trade to include the disclosure of personal information for monetary or other consideration, or for the purposes of direct marketing. Where a disclosure is a trade, consent is required.

The AIIA's concern is with the breadth of that provision in its application to digital advertising. Extending the scope of the Act to non-personal data that is de-identified, or to information about groups or cohorts, would be out of step with global privacy regimes including the General Data Protection Regulation and the California Consumer Privacy Act.⁵

The position is complicated by the breadth of proposed s 6FD, Note 1 to which identifies characteristics, behaviours, traits, preferences and patterns of activity as capable of rendering an individual identifiable. Audience segmentation previously conducted on a non-identified basis may therefore fall within the trading provisions, notwithstanding that the definition of direct marketing is itself anchored to personal information relating to the individual. The consultation paper contemplates that the definition of trade may capture disclosures of cookies or pixels in programmatic advertising processes, which is the clearest instance of that difficulty. The Department should confirm the intended boundary in the explanatory materials.

Recommendation Ten: The trading and direct marketing provisions should be confined to the handling of personal information, and the Bill should confirm that they do not extend to de-identified or aggregated information, or to information about groups or cohorts.

Allocation of the opt-out obligation

Proposed APP 7.1 places the obligation to give effect to an opt-out request on the organisation making the direct marketing communication. The AIIA supports that allocation. Opt-out requests should be directed to controllers rather than to processors, an approach seen internationally and one that recognises that it is controllers that are consumer-facing and hold the relationship with the individual. We also support the qualification that an organisation take such steps as are reasonable in the circumstances, which properly recognises that direct marketing may be delivered across multiple accounts, devices and identifiers that cannot always be linked to a single individual.

Recommendation Eleven: Proposed APP 7.1 should be retained as drafted, with responsibility for giving effect to an opt-out request resting on the organisation making the communication rather than on processors.

5. Security, destruction and retention

The AIIA supports the objectives of proposed APP 11. Data minimisation and the timely destruction of information no longer required are among the most effective privacy

⁵California Consumer Privacy Act of 2018, Cal Civ Code §§ 1798.100–1798.199.100, as amended by the California Privacy Rights Act of 2020.

protections available, and an uplift in cyber resiliency across the Australian economy benefits the digital sector and the community alike.

Any obligation to destroy personal information needs to acknowledge existing statutory record retention requirements, such as those applying to taxation and corporate records, including those required by legislation applying in foreign markets. Proposed APP 11.3 recognises retention required under an Australian law or a court or tribunal order but does not address obligations arising in other jurisdictions in which Australian businesses operate. An entity subject to a foreign retention obligation would face a direct conflict of laws.

A further review of legal provisions outside the Privacy Act that require certain forms of personal information to be retained would also be valuable. In many cases industry retains information in order to comply with legislative requirements, such as in the case of telecommunications regimes, and the right balance must be struck with government considering national security, law enforcement, privacy and the regulatory burden on industry.

Recommendation Twelve: The destruction obligation in proposed APP 11 should acknowledge existing statutory record retention requirements, including those required by legislation applying in foreign markets.

6. Notifiable data breaches

Reporting timeframes

The AIIA supports the intention of dovetailing and streamlining reporting obligations, which underlies the alignment of the notification period in proposed s 26WK(2) with the critical infrastructure regime. The length of the period nonetheless warrants attention. There are necessarily unknown unknowns in the immediate aftermath of a cyber security and privacy event, and containing and understanding the scale of the breach must be the primary focus of a responding entity. Rushing a report may lead to erroneous statements being inadvertently made because the full picture was unavailable. Rather than requiring a complete report within 72 hours, the scheme could require a first alert putting the Commissioner on notice that a matter has come to the entity's attention, with further detail forthcoming once the breach has been investigated or contained. There should be flexibility in the form that first alert takes, particularly for smaller organisations where the person responsible for submitting the report is also responsible for containing the reported event.

Recommendation Thirteen: Rather than requiring a complete report within 72 hours, the scheme should provide for a first alert putting the Commissioner on notice that a matter has come to the entity's attention, with further detail to follow once the breach has been investigated or contained, and with flexibility in the form that first alert may take.

Steps taken in response to a breach

The AIIA does not support the requirement in proposed s 26WK(3)(e) and the corresponding amendment to s 26WR(4), and opposed the equivalent proposal when it was made in the Privacy Act Review Report.⁶ Requiring a statement to set out the steps an entity has taken or intends to take is overly prescriptive and adds a further layer of resource-intensiveness at a critical juncture in the immediate aftermath of an incident. Within 72 hours a response is by definition incomplete, and the obligation to notify material changes and corrections means any account given at that point will frequently require revision.

Recommendation Fourteen: Proposed s 26WK(3)(e) should not require a statement about an eligible data breach to set out the steps the entity has taken or intends to take in response.

Penalties and safe harbour

The AIIA welcomes a tiered approach to the penalty regime, including the introduction of a mid-tier, which is essential in the wake of the increase in penalties for serious breaches. Any privacy penalty regime needs to support and enable early and full disclosure as soon as possible following a breach, including for smaller companies. Encouraging entities to seek help from government bodies such as the Australian Cyber Security Centre in the event of a breach is essential, especially where breaches have occurred that would be difficult to prevent and involve sophisticated state and non-state actors. Where government sets out examples or gold standards of the steps expected of entities, relief should be available to those that meet them, so that the standard operates as an incentive rather than only as a benchmark for liability. The introduction of civil penalty exposure in proposed s 13K(2) and the expanded categories in s 13(4A) make this more rather than less important.

⁶Privacy Act Review Report (n 19) proposal 28.3.

Recommendation Fifteen: The penalty regime should support and enable early and full disclosure as soon as possible following a breach. Where government sets out examples or gold standards of the steps expected of entities, safe harbour relief from penalties should be available to organisations that have met those standards, engaged in timely reporting, acted in good faith and exercised due diligence in their data and cyber security practices.

7. Right to erasure

Full implementation of a right of erasure poses practical difficulties for the technology sector. Data in modern systems is distributed across production stores, replicas, backups, archives and derived datasets, and destruction on request is frequently not achievable within a reasonable period without compromising system integrity. Given that the Government has determined to proceed, the AIIA sets out below the qualifications it considers necessary.

First, the grounds for requesting erasure should be limited, as is the case under Article 17 of the General Data Protection Regulation,⁷ and law enforcement requirements should be considered. Where retention is necessary for the original purpose for which the data was collected, the right to erasure should not apply.

Recommendation Sixteen: The grounds for requesting erasure should be limited, as is the case under Article 17 of the General Data Protection Regulation, and law enforcement requirements should be considered.

Second, the cases in which quarantine or de-identification is deemed to satisfy the right should be maximised. Proposed APP 14.1 requires destruction, and while the exception for technical impossibility or infeasibility is welcome, it is expressed as a high threshold and will not cover cases where destruction is achievable but seriously disruptive. Permitting irreversible quarantine or de-identification would deliver the same protection to the individual at materially lower cost and risk.

Recommendation Seventeen: The Government should seek to maximise the cases in which the quarantine or de-identification of data is deemed to satisfy the right.

Third, an exception should be provided where personal information is required for a transaction or contract. An erasure request should not leave an entity unable to complete a transaction to which the individual is a party. The consultation paper describes the legal interest exceptions as covering circumstances where destruction would be inconsistent

⁷GDPR (n 9) art 17.

with a law, a court or tribunal order, or a contract with the individual. Proposed APP 14.3 does not give effect to the last of these: paragraph 14.3(c) is confined to retention required under an Australian law or a court or tribunal order, and paragraph 14.3(e) to information strictly necessary to continue providing a requested good or service. Neither covers a contractual obligation owed to the individual that does not involve an ongoing service. The drafting should be aligned with the policy described in the consultation paper.

Recommendation Eighteen: An exception should be provided where personal information is required for a transaction or contract.

Fourth, the right should acknowledge existing statutory record retention requirements, such as those applying to taxation and corporate records, including those required by legislation applying in foreign markets.

Recommendation Nineteen: The right should acknowledge existing statutory record retention requirements, including those required by legislation applying in foreign markets.

Fifth, the right may benefit from being counterbalanced against an entity's legitimate interests. Under Article 21 of the General Data Protection Regulation, the right to object is counterbalanced against the data controller's legitimate interests for the processing, which could in some cases override the right to object.⁸ We ask that the Department consider that model. We note also that bringing organisations into contact with individuals requesting erasure frequently and on a case-by-case basis, particularly where access and visibility are granted in respect of incorrect data, places organisations in a high-stakes legal environment on a repetitive basis.

Recommendation Twenty: Consideration should be given to counterbalancing the right against an entity's legitimate interests, as the right to object is counterbalanced under Article 21 of the General Data Protection Regulation.

8. Matters not addressed by the package

The AIIA firmly believes that all businesses, regardless of size, should be held accountable for protecting the privacy of Australians and their personal and sensitive information, and has identified the small business exemption as anomalous when compared with other mature jurisdictions.⁹ Uplifting cyber resiliency across the entire Australian economy would be achieved by a phased and scaled incorporation of small and medium enterprises

⁸GDPR (n 9) art 21.

⁹Privacy Act (n 3) s 6D.

into the privacy regime, and enterprises working in critical sectors must meet minimum privacy and security standards. The exemption is not addressed in this package.

Recommendation Twenty-One: The small business exemption should be removed, all businesses regardless of size being accountable for protecting the privacy of Australians, subject to staged application and a smaller penalty regime for small and medium enterprises.

9. Implementation and transition

The AIIA asks that commencement periods be settled and set out on the face of the Bill, staged by schedule. A privacy- and security-first mindset takes time to incorporate into the operations and capabilities of a business. The lead time for achieving maturity in these domains is crucial to consider, and providing practical capacity-building and accessible toolkits is essential. Businesses must feel that it is safe to iterate towards best practice and the ideal settings in a regulatory landscape, rather than being penalised for attempting to satisfy the APPs. The package requires every collection, use and disclosure to be reassessed against a new test, every collection notice to be rewritten, and processor arrangements across the economy to be documented. Where new obligations are extended to small and medium enterprises, a smaller penalty regime applicable to those enterprises will be important and appropriate.

Recommendation Twenty-Two: Commencement should be staged and accompanied by appropriate education and support, with a suitable transition period and staged application of laws, penalty regimes and regulatory frameworks.