18 September 2026

BSA SUBMISSION ON PRIVACY AMENDMENT (PERSONAL DATA PROTECTION) BILL 2026 EXPOSURE DRAFT

Submitted Electronically to the Attorney-General's Department (AGD)

The Business Software Alliance (**BSA**)[1] welcomes the opportunity to respond to the Exposure Draft of the Privacy Amendment (Personal Data Protection) Bill 2026 and the accompanying Privacy Reform Consultation Paper (**Bill** and **Consultation Paper** respectively).[2]

BSA is the leading advocate for the global software industry. BSA members create technology solutions that power other businesses, including cloud storage services, customer relationship management software, human resources management programs, identity management services, network infrastructure services, cybersecurity solutions, and collaboration systems. Our members have made significant investments in Australia, and we are proud that many Australian companies and organisations continue to rely on our members' products and services to do business and support Australia's economy. BSA members recognise that companies must earn their consumers' trust and act responsibly with their personal information.

BSA has engaged at every major stage of the Privacy Act reform process, from the initial review of the Privacy Act 1988 (**Privacy Act**) to the first tranche of amendments passed in 2024.[3] Our comments focus on the proposed amendments with the greatest implications for the enterprise software sector, with particular focus on the proposed exception for information processors.

Summary of BSA's Recommendations

Treatment of Information Processors

The Bill introduces the controller-processor distinction in name but not in substance. BSA urges AGD to amend the Bill so that the controller-processor framework allocates obligations by role,

[1] BSA's members include: Adobe, Alteryx, Amadeus, Amazon Web Services, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cloudflare, Cohere, Cohesity, Dassault Systemes, Databricks, Datadog, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Veeam, Workday, Zendesk, and Zoom Communications Inc.

[2] Exposure Draft, Privacy Amendment (Personal Data Protection) Bill 2026, August 2026, https://consultations.ag.gov.au/rights-and-protections/privacy-reform/user_uploads/exposure-draft-bill-2026.pdf; Privacy Reform Consultation Paper, August 2026, https://consultations.ag.gov.au/rights-and-protections/privacy-reform/user_uploads/consultation_paper.pdf.

[3] See:

- BSA Comments on Review of Australia Privacy Act 1988, January 2022, https://www.bsa.org/policy-filings/australia-bsa-comments-on-review-of-australia-privacy-act-1988;
- BSA Comments on Privacy Legislation Amendment Bill, October 2022, https://www.bsa.org/policy-filings/australia-bsa-comments-on-privacy-legislation-amendment-bill;
- BSA Comments on Australia Privacy Act Review Report 2022, April 2023, https://www.bsa.org/policy-filings/australia-bsa-comments-on-australia-privacy-act-review-report-2022;
- BSA Comments on the Privacy and Other Legislation Amendment Bill 2024, October 2024, https://www.bsa.org/files/policy-filings/10092024bsaauprivacybill.pdf.

rather than relying on an exception for individual acts that still applies consumer-facing obligations to business-to-business processors. Specifically, we recommend the following:

- Adopt role-based definitions of controllers and processors, modelled on the formulation used in the European Union's General Data Protection Regulation (**GDPR**) and privacy laws worldwide, and expressly recognise that determining if an entity acts as a controller or a processor is fact-based and context-specific.
- Ensure processors' obligations fit their role. If processors remain subject to obligations under Australian Privacy Principle (**APP**) 1 and APP 11, the Bill should ensure that consumer-facing obligations, including complaint handling, rest with controllers and not processors.
- Amend the notifiable data breaches scheme so that a processor's obligation is to notify the controller of an actual or suspected data breach without undue delay – since the processor is handling data on the controller's behalf. The controller, in turn, should be responsible for notifying the Office of the Australian Information Commissioner (**OAIC**) and affected individuals. The forthcoming complaint-handling measures should likewise apply to controllers, not processors.
- Clarify the treatment of processing performed for customers that are not APP entities. A processor should not be assigned controller obligations just because it processes data on behalf of an organisation that is not an APP entity. The processor is still not positioned to fulfil consumer-facing controller obligations.
- If the documentation requirement in section 16D is retained, clarify what suffices to specify a controller's purposes and document instructions, make clear that a contract between a controller and a processor is sufficient to specify the controller's purposes and document instructions, and provide a suitably long transition period.

Fair and Reasonable Handling of Personal Information

BSA supports the new fair and reasonable test as a departure from a consent-focused framework. However, such a test still involves a large degree of uncertainty, even with statutory factors to guide entities. To make the test more workable in practice and encourage companies to use this basis for processing, we recommend the following:

- Publish OAIC guidance on the fair and reasonable test, developed in consultation with industry, well before commencement. The guidance should confirm that handling covered by an individual's valid consent is ordinarily fair and reasonable, absent countervailing factors.
- Provide a transition period so that entities have adequate time to align their practices with the new framework and the guidance, and implement an initial period of guidance-first

enforcement following commencement, during which the OAIC suspends penalties and prioritises education and remediation in respect of the new test.

- Ensure that the test is enforced consistently by the regulator.

Data Breach Notification Obligations

BSA supports the scheme's risk-based approach and the alignment of the 72-hour reporting period with other reporting timeframes in Australia's regulatory landscape. To ensure the scheme encourages full and frank disclosure, we recommend the following:

- Incorporate no-fault and no-liability principles into the notification obligation, so that information provided in good faith in a breach statement, including an incomplete statement, is not used as the evidentiary basis for enforcement against the notifying entity.

Right to Erasure on "Large Digital Platforms"

BSA supports the right to erasure resting with controllers and subject to appropriate exceptions. However, the definition of "large digital platform" is significantly broader than the stated policy intent, and the Bill does not give effect to the stated intent regarding processors. We recommend the following:

- Calibrate the "large digital platform" thresholds by reference to Australian customers' actual use of the in-scope service, rather than the global revenue of an organisation's business group.
- Ensure the definition of “large digital platform” does not capture enterprise services provided to business customers.
- Include an express exception in APP 14 for personal information held in the entity's capacity as a processor, with individuals directed to the relevant controller.

Addressing Emerging Technologies and Artificial Intelligence (AI)

The growth of AI reinforces the importance of implementing the controller-processor distinction properly, as AI-enabled services increasingly process personal information on customers' behalf. We recommend the following:

- Maintain a technology-neutral, principles-based approach to AI.
- Ensure that AI-related obligations and guidance reflect the distinct roles of AI developers and deployers.

Treatment of Information Processors

The Bill introduces a controller-processor distinction into the Privacy Act for the first time, which we strongly welcome. However, getting the distinction right matters as much as introducing it. As it stands, the Bill requires significant adjustments to deliver a controller-processor distinction that functions properly.

BSA has advocated for the introduction of a controller-processor distinction at every stage of the

Privacy Act review.[4] In our view, this is the most important proposal to emerge from that process. The distinction has existed for more than 40 years and is foundational to privacy laws worldwide, including the European Union's GDPR, Singapore's Personal Data Protection Act, and state privacy laws in the United States.[5] By reflecting the different roles of controllers (which decide how and why to process personal data) and processors (which handle personal data on behalf of other companies, i.e., controllers, and pursuant to their instructions), a privacy law can craft obligations that fit both types of organisations. As the Privacy Act Review Report 2022 (**Report**) recognised, the distinction will clarify consent obligations and help entities more effectively respond to data breaches.[6]

The Bill's proposed exception for information processors does *not* adequately reflect the controller-processor distinction.

Under the new section 16D, **a processor** is an APP entity that does an act or engages in a practice on behalf of another APP entity — **a controller** — in accordance with the controller's documented instructions and only for the purposes specified in those instructions.[7] Notwithstanding these new definitions, the exposure draft does not create a distinct set of obligations for processors (as most data protection laws globally do) but instead exempts processors from certain APPs when they act on behalf of a controller. Processors also remain directly responsible for consumer-facing requirements in APP 1 (Open and Transparent Management of Personal Information) and APP 11 (Security of Personal Information) even when acting on behalf of a controller.[8]

The result is a mechanism that excuses individual acts of processors from obligations created for controllers, rather than one that defines the two roles and allocates obligations between them. For example, unlike the GDPR's approach in Article 28, the Bill does not contain a specific set of obligations that reflect a processor's role – like obligations about the type of privacy protections that should be contained in a contract between a controller and a processor.

Instead, a processor under the Privacy Act would remain directly subject to a range of consumer-facing obligations that privacy laws worldwide assign to controllers precisely because processors cannot properly perform them. The Bill also conflates the responsibilities of controllers and processors, which runs counter to the policy intention outlined in the Report. We elaborate on these concerns below.

- **First, the definitions do not clearly set out the roles and responsibilities of controllers and processors.**

  The proposed section 16D defines a controller simply as an entity on whose behalf the processor acts, whereas a processor is an entity that acts in accordance with the

[4] See the submissions listed at footnote 3. See also "Privacy reform must reflect different roles in data handling", September 2024, https://www.innovationaus.com/privacy-reform-must-reflect-different-roles-in-data-handling/.

[5] Controllers and Processors: A Longstanding Distinction in Privacy, July 2026, https://www.bsa.org/policy-filings/controllers-and-processors-a-longstanding-distinction-in-privacy.

[6] Privacy Act Review Report 2022, February 2023, https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf, p. 231.

[7] Bill, Schedule 6, item 6 (new section 16D).

[8] Bill, Schedule 6, items 2 and 4 (new subsections 6A(2A) and 6B(2A)). See also Consultation Paper (2026), p. 37. BSA notes that the Bill proposes to amend APP 11 to "Security *and Destruction* of Personal Information" [emphasis added] to make clear that an APP entity should consider destroying or de-identifying personal information in certain circumstances.

controller's instructions. The Bill fails to state the substance of the controller-processor distinction, which is that the controller is the entity that determines the *purposes and means* of processing personal information, and therefore bears primary responsibility for responsibilities resulting from those determinations. This sets the Privacy Act apart from every major formulation of the controller-processor distinction in other parts of the world. For reference, the GDPR defines a controller as the entity that "alone, or jointly with others, determines the purposes and means" of processing, and a processor as an entity that "processes personal data on behalf of the controller".[9] Privacy laws across the globe have replicated that approach. BSA recommended in 2023 that Australia adopt this formulation and that the Act expressly recognise that determining whether an entity acts as a controller or processor is fact-based and context-specific, since a single company may be a controller for some services and a processor for others.[10] Both recommendations remain unaddressed.

Without role-based definitions, the Privacy Act has no principled basis for allocating obligations between controllers and processors. The consequence is that consumer-facing obligations will fall on processors by default, even though processors cannot properly discharge them. For example, a processor has no relationship with the individuals whose personal data is collected by other companies; they often cannot identify or contact those individuals and may lack access to the information needed to respond to requests from individuals.

- **Second, processors remain subject to consumer-facing obligations within APP 1 and APP 11.**

  The two APPs that processors carry in full — APP 1 and APP 11 — contain obligations written for entities that have a direct relationship with individuals and control over the information. Processors generally have neither.

  Under APP 1, a processor must implement practices, procedures and systems to deal with inquiries and complaints from individuals (APP 1.2), maintain a privacy policy describing matters such as how an individual may access and seek correction of their personal information and how they may complain (APP 1.4), and provide that policy in the particular form an individual requests (APP 1.6). These requirements are fundamentally incompatible with the role of a processor. In contrast, leading privacy laws worldwide adopt the same structure for consumer rights: individuals submit requests to the controller, which decides how and why their data is processed, and the controller works with its processors to fulfil requests involving data held by those processors.[11]

  Processors play an assisting role rather than a consumer-facing one, for good reason. A processor does not typically interact with individuals and may be unable to verify the identity of a person making a request. Nor does it make the decisions required to respond to one, such as what data to provide in response to an access request, whether data

[9] GDPR, Articles 4(7) and 4(8).

[10] BSA Comments on Australia Privacy Act Review Report 2022 (2023), pp. 2-3.

[11] Consumer Rights to Access, Correct, and Delete Data: A Processor's Role, July 2026, https://www.bsa.org/policy-filings/consumer-rights-to-access-correct-and-delete-data-a-processors-role.

sought to be corrected is actually inaccurate, or whether an exception applies because the data is subject to a legal hold. Those decisions sit with the controller. BSA identified in 2023 that these consumer-facing elements of APP 1 are not suited to processors and recommended amendments recognising that consumer-facing transparency requirements do not apply to them.[12]

APP 11, as amended by the Bill, contains similar issues. The new APP 11.2 requires an entity to consider destroying personal information that it "no longer needs" for any purpose for which it may use or disclose the information, and the new APP 11.4 requires an entity to take any steps needed to ensure it can identify the personal information it holds.[13] A processor's retention needs are defined by its controller's instructions, not its own purposes, and a processor that destroys information on its own assessment could destroy data its controller is legally required to retain. In other words, it is the controller that decides when its data is no longer needed. That determination should not be made by processors, which only handle data on behalf of controllers and do not exercise this sort of decision-making authority. Equally, a processor's ability to identify the personal information it holds is often deliberately limited by privacy and security controls built into its products and enforced by contract.[14] BSA supports processors remaining responsible for securing the information they hold, but these obligations should be framed to reflect the processor's role rather than assume the entity controls the information.

- **Third, processors remain subject to consumer-facing obligations outside the APPs altogether.**

  The exception excuses breaches of the APPs and registered APP codes only. It provides no relief from obligations in the body of the Privacy Act. The most significant is the notifiable data breaches scheme in the Privacy Act, which applies to any APP entity that holds personal information subject to APP 11.1 (and therefore includes processors). Under the scheme, a processor would be required to give the OAIC a statement within 72 hours of an eligible data breach, including recommendations about the steps individuals should take in response, to notify affected individuals or publicise the statement, and to take reasonable steps to mitigate harm to affected individuals.[15]

  As highlighted above, due to the privacy and security controls built into their products and enforced by contract, processors often have limited access to, and knowledge of, the personal information they handle on behalf of their customers. A processor may therefore lack the facts needed to determine whether an incident amounts to an eligible data breach. Moreover, the processor will often lack insight into the type of information that was compromised, including whether such data included personal information, and the steps individuals should take in response. Privacy laws worldwide resolve this by requiring the processor to notify the controller, which then notifies the regulator and individuals. The GDPR, for example, requires a processor to notify the controller "without undue delay"

[12] BSA Comments on Australia Privacy Act Review Report 2022 (2023), p. 3.

[13] Bill, Schedule 3, Part 2, item 22 (new APP 11.2 and 11.4).

[14] BSA Comments on Australia Privacy Act Review Report 2022 (2023), p. 4.

[15] Bill, Schedule 3, Part 1, items 7 and 10 (new sections 26WDA, 26WDB, 26WK and 26WL).

after becoming aware of a breach, and places the obligations to notify the supervisory authority and data subjects on the controller.[16] BSA recommended this allocation of responsibilities in 2023.[17]

The same gap will apply to the complaint-handling measures the Consultation Paper indicates will be added to the Bill, which would require APP entities to provide accessible complaint mechanisms, respond to complaints within 60 days, and issue written decisions, with non-compliance constituting an interference with privacy.[18] Because these obligations would sit outside the APPs, processors would carry them in full, notwithstanding that individuals do not have a relationship with processors and should raise complaints with the controller they deal with. A processor that responds directly to an individual could also be forced to act against a controller's instructions — even though by definition processors are to act on behalf of controllers and pursuant to their instructions. For example, if an individual requests access to information that a controller has instructed be withheld, the Bill puts the processor in the middle.

The Bill should not place processors in these positions. Structurally, privacy obligations should mirror the two relationships that exist: the processor answers to the controller, and the controller answers to the individual.

- **Fourth, the exception only applies if: 1) both the controller and the processor are APP entities; *and* 2) the act is done "on behalf of a controller" under instructions "documented in writing".**

  Both conditions could unintentionally nullify the exception in practice.

  On the first condition, an APP entity processing information on behalf of a customer that is *not* an APP entity, such as an organisation with an annual turnover of AUD 3 million or less,[19] would not qualify as a processor and could not rely on the exception. The APP entity would then be subject to all obligations under the Privacy Act and all APPs, which would include the consumer-facing obligations described above, in respect of information it does not control. This scenario describes software providers serving Australian small businesses, which make up the substantial majority of Australian businesses, providers hosting data for state and territory government agencies, including public hospitals and schools, and providers whose Australian infrastructure serves overseas customers with no other connection to Australia. In each case, the provider's role is identical to that of a processor serving a large Australian enterprise, yet the exception would be unavailable.

  On the second condition, section 16D requires that the act be done in accordance with instructions given by the controller, for one or more purposes of the controller specified in

[16] GDPR, Articles 33 and 34. Article 33(2) provides that "the processor shall notify the controller without undue delay after becoming aware of a personal data breach".

[17] BSA Comments on Australia Privacy Act Review Report 2022 (2023), pp. 4-5.

[18] Consultation Paper (2026), p. 38.

[19] Privacy Act, sections 6C and 6D. Small business operators, defined as businesses with an annual turnover of AUD 3 million or less, are generally not APP entities unless an exception applies, such as private sector health service providers and businesses that trade in personal information. Other examples of entities that are not APP entities include state and territory government agencies, which are regulated by state and territory privacy laws, and overseas organisations that do not carry on business in Australia.

those instructions, with the instructions "documented in writing" by the controller.[20] Every element must be satisfied, and the exception applies act by act. The effect is that whether an entity is deemed a processor becomes an issue of strict contractual interpretation, rather than a factual assessment of a provider's relationship with its customer. These requirements also do not reflect commercial realities. For example, a cloud provider's routine operational acts, such as replicating data across backup servers, are rarely spelled out as explicitly documented "instructions" for "specified purposes" in a services agreement. On a strict reading, such acts could fall outside the exception and be tested against the APPs in full, including the fair and reasonable test, which the provider cannot meaningfully apply to information whose collection context it does not know.

Taken together, these issues mean the Bill introduces the controller-processor distinction in name but not in substance. Processors would remain directly subject to consumer-facing obligations they cannot properly discharge, while the exception's availability would turn on the identity of the customer and the state of its contracts rather than on which entity actually controls the information. This outcome would run counter to the Government's own objectives of reducing the compliance burden for entities acting as processors and bringing Australia into line with leading privacy frameworks in other jurisdictions.

Recommendations: AGD should amend Schedule 6 and related provisions so that the controller-processor framework allocates obligations by role, rather than relying on an exception for individual acts. Specifically, we recommend the following.

- **Adopt role-based definitions of controllers and processors.** The Privacy Act should define a controller as the entity that, alone or jointly with others, determines the purposes and means of processing personal information, and a processor as an entity that processes personal information on behalf of a controller, consistent with the formulation used in the GDPR and privacy laws worldwide. The Act should also expressly recognise that determining whether an entity acts as a controller or a processor is fact-based and context-specific, and that a processor which determines its own purposes for processing takes on the obligations of a controller in respect of that processing.
- **Confine processors' obligations under APP 1 and APP 11 to their role.** Processors should remain transparent about their own practices, for example by clearly stating instructions for handling information in their contracts with processors. However, consumer-facing elements of APP 1, including the requirements to deal with inquiries and complaints from individuals and to describe how individuals may access and correct their information, should rest with controllers. Otherwise, the legislation would insert processors between controllers and their consumers and require processors to answer questions that each controller may resolve differently, such as what data to provide in response to an access request or whether to verify a correction request before making it. Similarly, the destruction and identification obligations in the amended APP 11 should be framed so that a processor acts on, and consistently with, its controller's instructions, rather than requiring the processor to make its own assessment of whether information is still needed.

[20] Bill, Schedule 6, item 6 (new section 16D(1)).

- **Allocate data breach notification responsibilities by role.** The notifiable data breaches scheme should be amended so that a processor's obligation when becoming aware of an actual or suspected data breach is to notify the relevant controller without undue delay, with the controller responsible for assessing whether an eligible data breach has occurred, providing the statement to the OAIC, and notifying affected individuals. This mirrors the approach taken in the GDPR and other leading privacy laws and reflects the fact that the controller is best placed to provide the information that the regulator and individuals need.
- **Apply the forthcoming complaint-handling measures to controllers, not processors.** The dispute resolution and complaint-handling obligations foreshadowed in the Consultation Paper should rest with controllers, which are the entities that individuals deal with and can meaningfully complain to. Processors should instead be required to provide reasonable assistance to the controller in responding.
- **Clarify the treatment of processing performed for customers that are not APP entities.** An entity should not assume controller-level obligations by default in respect of information it does not control merely because its customer is not covered by the Privacy Act i.e., because the customer is a small business, a state or territory government agency, or an overseas organisation. Instead, controller obligations should apply to controllers subject to the Privacy Act and processor obligations should apply to processors handling personal information on behalf of controllers subject to the Privacy Act. The Bill currently captures a wider range of processors than the range of controllers it covers, without any clear justification. AGD should revise the Bill to avoid this result.
- **Clarify the documentation requirement and provide adequate transition.** If the documentation requirement in section 16D is retained as is, notwithstanding the recommendations above, the AGD should make clear that a contract between a controller and processor is sufficient to "specify" a controller's purposes and to document instructions under section 16D; AGD should also provide a suitably long transition period before the commencement of this obligation, so that controllers and processors can update their agreements to the section 16D standard.

Fair and Reasonable Handling of Personal Information

The Bill repeals existing APPs 3, 4, and 6 and replaces them with a single principle permitting the collection, use and disclosure of personal information only where it is fair and reasonable in the circumstances, having regard to various legislated factors: the data subject's reasonable expectations, transparency, data minimisation, genuine choice, and proportionality.[21]

BSA agrees with this approach, which departs from a consent-focused framework. As a general principle, consent should be reserved for situations where it is most meaningful to consumers, such as high privacy risk situations, and privacy laws should recognise other valid grounds for handling personal information to avoid burdening consumers with a high volume of consent requests that produces consent fatigue.

[21] Bill, Schedule 2, Part 1, item 10 (new APP 3). See also Consultation Paper (2026), pp. 10-15.

Our concern remains the one we raised in 2023: a principles-based test of this breadth necessarily involves a large degree of uncertainty, even with statutory factors to guide entities.[22] The Consultation Paper confirms that no single factor is determinative and that entities must make a holistic assessment of the circumstances.[23] Two safeguards are important to make this workable in practice:

- **Guidance before commencement.** We welcome the Consultation Paper's confirmation that the OAIC will provide guidance, including practical examples, to assist entities.[24] This guidance should be developed in consultation with industry and published well before the new APP 3 commences, so that entities can build compliance programs against a settled interpretation rather than retrofitting them after enforcement begins. The guidance should also confirm that where an individual has provided valid consent in respect of a collection, use or disclosure of their personal information, that handling should ordinarily be regarded as fair and reasonable in the circumstances, absent countervailing factors.
- **Consistent, regulator-led enforcement.** BSA has previously recommended that a fair and reasonable test be enforced by the central regulator, which can issue guidance about how the standard applies over time and in different scenarios and promote consistent outcomes.[25] This is particularly important now that the statutory tort for serious invasions of privacy is in force, as inconsistent judicial and regulatory interpretations of fairness-based standards would create uncertainty for both consumers and entities. Relatedly, given the uncertainty stemming from this new framework, AGD and OAIC should also implement enforcement in stages. AGD should provide an adequate transition period before commencement so that entities can align their practices with the new framework and the guidance. Following commencement, the OAIC should adopt a guidance-first approach to enforcement for an initial period, during which it suspends penalties and prioritises education and remediation in respect of the new framework.

Recommendations: AGD should ensure that OAIC guidance on the fair and reasonable test, developed in consultation with industry, is published well before commencement, and that the test is enforced consistently by the regulator. Such guidance should confirm that a collection, use, or disclosure covered by an individual's valid consent should ordinarily be regarded as fair and reasonable, absent countervailing factors. AGD should provide an adequate transition period so that entities can align their practices with the new framework and the guidance, and the OAIC should implement an initial period of guidance-first enforcement following commencement, during which it suspends penalties and prioritises education and remediation in respect of the new test.

[22] BSA Comments on Australia Privacy Act Review Report 2022 (2023), pp. 9-10.

[23] Consultation Paper (2026), p. 10.

[24] Consultation Paper (2026), p. 10.

[25] BSA Comments on Australia Privacy Act Review Report 2022 (2023), pp. 9-10.

Data Breach Notification Obligations

The Bill requires entities to give the OAIC a statement within 72 hours of becoming aware of reasonable grounds to believe an "eligible data breach" has occurred.[26] Where it is impossible or impracticable to provide a complete statement within that period, entities may submit an incomplete statement and supplement it as soon as practicable.[27]

BSA supports reasonable and appropriate data breach notification requirements, and we welcome the scheme's risk-based approach. The threshold remains an eligible data breach that a reasonable person would conclude is likely to result in serious harm, and the 72-hour reporting period runs from awareness of reasonable grounds to *believe* a breach has occurred, not mere suspicion. We also support aligning the reporting period with similar timeframes under the *Security of Critical Infrastructure Act 2018* and the *Cyber Security Act 2024*, as we have consistently encouraged harmonisation of reporting obligations across Australia's regulatory landscape to reduce duplication and complexity for regulated entities.[28] We also welcome the Consultation Paper's confirmation that the expanded statement requirements will not require disclosure of information that could compromise cyber security or response activities.[29]

To supplement the above, we recommend incorporating no-fault and no-liability principles into the operation of the scheme. The purpose of a breach statement is to give the regulator and affected individuals an accurate and timely picture of the incident, including its deficiencies. BSA has consistently advocated for these principles in security reporting obligations, on the basis that the punitive use of disclosed information discourages full and frank disclosure and ultimately weakens the regulator's visibility over the risks it is seeking to manage.[30] This is particularly important under the Bill, which makes non-compliance across the expanded scheme an interference with privacy attracting civil penalties. Entities need confidence that an incomplete statement will not itself become the evidentiary basis for enforcement against them. Without that confidence, the incentive shifts toward defensive drafting, where entities disclose only the minimum necessary, which undermines the very purpose the notification scheme is meant to serve. Enforcement efforts should focus on failures to notify or to take required steps, rather than on the content of notifications made in good faith.

Recommendation: AGD should incorporate no-fault and no-liability principles into the data breach notification obligation, so that information provided in good faith in a breach statement, including an incomplete statement, is not used as the evidentiary basis for enforcement against the notifying entity.

---

[26] Bill, Schedule 3, Part 1, items 6 and 8 (new sections 26WBA and 26WE); Consultation Paper (2026), pp. 23-24. The Bill defines an "eligible data breach" as a data breach where a reasonable person would conclude that the unauthorised access to, or disclosure of, the information would be likely to result in serious harm to any of the individuals to whom the information relates. Where the breach is constituted by a loss of information, the test is whether a reasonable person would conclude that any unauthorised access to, or disclosure of, the information would be likely to result in serious harm.

[27] Bill, Schedule 3, Part 1, item 10 (new section 26WK); Consultation Paper (2026), p. 25.

[28] See, most recently, BSA Comments on Streamlining and Modernising the Security of Critical Infrastructure Act 2018, July 2026, https://www.bsa.org/policy-filings/australia-bsa-comments-on-streamlining-and-modernising-the-security-of-critical-infrastructure-act-2018.

[29] Consultation Paper (2026), p. 25.

[30] BSA Comments on Streamlining and Modernising the Security of Critical Infrastructure Act 2018 (2026), Measure 15.

Right to Erasure on "Large Digital Platforms"

The Bill introduces a new APP 14, under which an organisation that is a "large digital platform" must, on request by an individual, destroy personal information that relates to the individual, subject to exceptions. An organisation is a large digital platform if it provides a social media service, relevant electronic service or designated internet service within the meaning of the *Online Safety Act 2021* (**Online Safety Act**) and meets either a gross revenue test (business group gross revenue of at least AUD 500 million for the previous financial year) or an end-users test (an average of at least 2.5 million monthly end users in Australia).[31]

As a general principle, the obligation to meet such individual requests should fall on the personal information controller and be subject to appropriate exceptions. Our concerns with APP 14 therefore relate primarily to the scope of entities captured, rather than to the right itself.

- **First, the definition of "large digital platform" is significantly broader than the stated policy intent.**

  The Consultation Paper states that the thresholds are "intended to capture organisations that are sufficiently large to meet the erasure obligations" and platforms that "collect significant amounts of personal information and present heightened privacy risks".[32] However, the Online Safety Act's definitions apply to an extremely broad category of entities and services. In particular, a "designated internet service" operates as a residual category covering, in effect, any service that allows end-users to access material using an internet carriage service.[33] This captures enterprise services that present a substantially different risk profile from the consumer platforms this measure is aimed at – as highlighted previously, enterprise service providers often have no direct relationship with the end users of their services, and are subject to technical, legal and contractual obligations not to inspect the data of their enterprise customers.

  Furthermore, the gross revenue test is calculated on the gross revenue of the organisation's entire business group, and it does not matter whether that revenue has an Australian source or relates to the in-scope service.[34] As a result, an organisation whose Australian-facing service is limited may nevertheless be captured as a large digital platform solely because of the size of its global business group. The size of an organisation's global business group says little about the volume of Australians' personal information its service collects or the privacy risks that service presents. BSA therefore recommends that the thresholds be calculated by reference to Australian customers' actual use of the in-scope service, which is the metric that reflects the service's significance to Australians, rather than the global revenue of the organisation's business

[31] Bill, Schedule 4, Part 2, items 6 and 11 (new section 6EB and new APP 14). See also Consultation Paper (2026), pp. 33-34.

[32] Consultation Paper (2026), p. 33.

[33] Online Safety Act 2021, section 14. A "designated internet service" includes a service that allows end-users to access material using an internet carriage service, other than a social media service or relevant electronic service.

[34] Bill, Schedule 4, Part 2, item 6 (new subsections 6EB(2) and (3)). Subsection 6EB(3) provides that it does not matter whether revenue has an Australian source.

group. We note that the end-users test already reflects this approach, as it is calculated by reference to average monthly end users in Australia.

- **Second, the Bill does not give effect to the stated policy intent regarding processors.**

  The Consultation Paper states that large digital platforms "would not be required to destroy personal information held solely in their capacity as a processor".[35] BSA agrees with this position. Erasure requests relating to information that a provider processes on behalf of a business customer should be directed to, and handled by, that customer as the controller. However, APP 14 contains no express exception for processors. The outcome instead depends on the proposed general exception for processors, which only excuses acts done in accordance with a controller's documented instructions. Whether the exception relieves a processor of APP 14 is therefore uncertain, and a platform that receives an erasure request faces genuine doubt as to whether it must respond directly to a consumer it has no relationship with, in respect of information it does not control.

  To give effect to the stated policy intent, APP 14 should include an express exception for personal information held in the entity's capacity as a processor. Individuals whose requests relate to such information should be directed to the relevant controller, which is the entity able to assess the request and act on it.

Recommendation: AGD should calibrate the "large digital platform" thresholds by reference to Australian customers' actual use of the in-scope service, rather than the global revenue of an organisation's business group, and ensure the definition does not capture enterprise services provided to business customers. AGD should also include an express exception in APP 14 for personal information held in the entity's capacity as a processor, with individuals directed to the relevant controller.

Addressing Emerging Technologies and AI

The Consultation Paper seeks feedback on whether the reform package adequately addresses privacy risks associated with emerging technologies, including AI.[36]

BSA supports addressing these risks through a technology-neutral, principles-based Privacy Act, rather than through technology-specific rules. The data-intensive nature of AI underscores the importance of meaningful consumer privacy protections, and consumers deserve to know how their personal information is used and protected.[37] A technology-neutral framework delivers those protections while remaining relevant as technologies evolve. In this context, we note the following:

- **First, the growth of AI makes it more important than ever to implement the controller-processor distinction properly.**

[35] Consultation Paper (2026), p. 34.

[36] Consultation Paper (2026), pp. 41-42.

[37] BSA Comments on the Privacy and Other Legislation Amendment Bill 2024 (2024), p. 5.

AI has deepened the role-based structure of the modern data economy: organisations increasingly rely on AI-enabled services provided by others, with the provider processing personal information on the customer's behalf and pursuant to its instructions.

In the absence of a clear controller-processor distinction, obligations can become increasingly blurred. For example, a business may hire a vendor to fine-tune an AI model based on the business's own data. Without a controller-processor distinction, both companies may be treated as responsible for any personal information that is processed, creating duplicative obligations even though the vendor does not make decisions about the legal basis for that processing or have relationships with any individuals whose information may be processed. A properly implemented controller-processor distinction, allocating these obligations to the controller on whose behalf the information is generated, is the mechanism that keeps the Privacy Act workable as AI-enabled services become embedded across the economy.

- **Second, any AI-related obligations should reflect the different roles of AI developers and deployers.**

  As BSA noted in its comments on the Privacy Act Review Report, there are at least two key stakeholders with varying degrees of responsibility for managing the risks associated with an AI system: the developer, which designs and develops the system, and the deployer, which uses it.[38] A deployer generally does not control design decisions made by the developer, and a developer generally does not control how a deployer subsequently uses the system. To the extent AGD addresses these related but separate issues in future guidance, such guidance should reflect these distinct roles, so that each entity's obligations correspond to the decisions it actually controls.

Recommendations: AGD should maintain a technology-neutral, principles-based approach to AI. AGD should also ensure that AI-related obligations and guidance reflect the distinct roles of AI developers and deployers.

Conclusion

We thank AGD for the opportunity to provide our recommendations in response to the Consultation Paper and the Bill. We hope our comments assist AGD in refining the Bill so that it provides greater clarity for regulated entities. We welcome AGD's continued engagement with industry stakeholders, including BSA and our members, and we look forward to continued dialogue as the Bill progresses.

Yours sincerely,

Tham Shen Hong

Director, Policy – APAC

[38] BSA Comments on Australia Privacy Act Review Report 2022 (2023), pp. 10-11. See also Effective Accountability Along the AI Value Chain: Right-Sizing AI Responsibilities for the Role, June 2026, https://www.bsa.org/policy-filings/effective-accountability-ai-value-chain-right-sizing-ai-responsibilities-role.