asifma
Growing Asia's Markets

18 September 2026

To: Attorney-General's Department
Via online consultation portal

Submission on the Privacy Reform Consultation Paper and exposure draft of the Privacy Amendment (Personal Data Protection) Bill 2026

Asia Securities Industry & Financial Markets Association [1] ("**ASIFMA**") is an independent, regional trade association with over 150 member firms comprising a diverse range of leading FIs from both the buy and sell side, including banks, asset managers, law firms and market infrastructure service providers. Together, we harness the shared interests of the financial industry to promote the development of liquid, deep and broad capital markets in Asia. ASIFMA, on behalf of its members, is pleased to submit this letter to the Attorney-General's Department in response to the Exposure Draft Privacy Amendment (Personal Data Protection) Bill 2026 ("**Exposure Draft**") and the accompanying Consultation Paper released for public consultation on 31 August 2026. We are grateful for the opportunity to provide feedback and we write to offer our recommendations to ensure the proposed reforms remain proportionate, operationally feasible, and supportive of innovation while bolstering privacy protections for individuals.

In this letter, we have consolidated our official response, with observations and recommendations for consideration.

1. Definitions of personal information and sensitive information

While we support the updating existing definitions, we are concerned about the expanded (and unclear) definition of personal information. The definition would introduce material uncertainty, especially where an 'individual's name or legal identity is not known, and will apply retrospectively to information already held. This will require entities to re-assess existing data against the new scope, a substantial exercise for financial institutions. Financial institutions are subject to numerous regulatory retention obligations and, as a result, hold vast quantities of data solely to satisfy those requirements rather than for any active operational purpose. Given that newly collected information would in any event be subject to the amended requirements, applying the expanded definition only to data collected after commencement is both proportionate and practical.

Recommendations:

- The expanded definition should only apply to information held prior to any amendments where such personal information is subsequently used or disclosed.

[1] ASIFMA is an independent, regional trade association with over 150 member firms comprising a diverse range of leading FIs from both the buy and sell side, including banks, asset managers, law firms and market infrastructure service providers. Together, we harness the shared interests of the financial industry to promote the development of liquid, deep and broad capital markets in Asia. ASIFMA advocates stable, innovative, competitive and efficient Asian capital markets that are necessary to support the region's economic growth. We drive consensus, advocate solutions and effect change around key issues through the collective strength and clarity of one industry voice. Our many initiatives include consultations with regulators and exchanges, development of uniform industry standards, advocacy for enhanced markets through policy papers, and lowering the cost of doing business in the region. Through the GFMA alliance with SIFMA in the United States and AFME in Europe, ASIFMA also provides insights on global best practices and standards to benefit the region.

- Clarify when 'individuation' would be considered personal information, and the impacts of this expanded definition on other parts of the Privacy Act (including notifiable data breaches, information access and correction requests and the right to erasure).
- Clarify whether isolated identifiers (eg, account or membership numbers) are intended to be captured by the expanded definition of personal information.
- Confirm that the definition of 'Precise geolocation tracking data' is not intended to capture ordinary corporate device management, building access and travel records, particularly in relation to employee and contractor management.

2. Definition of consent

We support the clarification in the consultation paper that consent can remain 'current' without requiring periodic re-confirmation, and that 'unambiguous' consent may be implied where the individual's conduct clearly indicates agreement and the relevant purpose is clear from the surrounding context. However, further guidance is needed for ongoing customer relationships.

Consent obtained at onboarding, account opening or the start of a transaction should remain current unless the relevant circumstances or information-handling practices materially change, or the individual withdraws consent. Consent should also be able to cover a clearly described set of related activities. Overly granular or repeated consent requests may reduce, rather than improve, meaningful choice by creating consent fatigue.

Practical guidance should also address how consent is obtained, recorded and evidenced across multi-entity data flows, including intra-group servicing arrangements. It should also cover situations where one individual provides another individual's information, including in know-your-customer, anti-money laundering and account administration contexts.

Recommendations:

- Clarify that consent may cover a defined set of related activities and remains current unless relevant circumstances or information-handling practices materially change, or consent is withdrawn.
- OAIC guidance should address ongoing customer relationships, multi-entity data flows and evidence of consent in practical operating models.

3. Definition of discloses

We seek clarity on whether the proposed definition of 'discloses':

- includes any circumstance where information is made accessible to another person or body even where the discloser has not released 'control' over the information; this appears broader than the current control-based test and could capture ordinary service-provider access and arrangements where currently there is not considered to be a disclosure (for example cloud hosting arrangements); and
- is intended to remove the prior distinction between a 'use' within effective control and a disclosure, which was an important feature of historical guidance and often relevant in the context of cloud storage.

Recommendation:

Clarify the meaning of discloses in the context of service-provider and processor access, including the importance of 'control' when considering whether information is 'accessible' and whether 'storage' in a third party service can occur without making information 'accessible'.

4. Trading of personal information

The broad definition of 'trade' (and narrow exceptions) could have a number of unintended consequences. In particular:

- The definition could capture intragroup or multinational group sharing of personal information, where such sharing is part of business as usual group activities and operations.
- The definition could capture the disclosure of personal information to third parties for direct marketing purposes or for an introductory service which is explicitly requested by the individual (ie. where the individual requests an organisation to provide their personal information for an introduction to a third party service provider for potential provision of goods or services). It is not clear if the exception in section 6FC(2)(a) is designed to permit this sort of 'trade', where the ultimate product or service may be being provided by the entity the organisation is disclosing the information to. Is the provision of that 'introduction' considered a provision of a service by the organisation?
- The definition could also capture legitimate risk intelligence, sanctions screening, adverse media screening and due diligence services that financial institutions rely on to meet their anti-money laundering, sanctions, fraud and scam prevention and broader regulatory compliance obligations. It is not practical to obtain consent for certain risk-screening use cases.
- The processor exception does not capture overseas processors who are not APP entities (given the proposed definition of 'processor' in section 16D is limited to APP entities). This would unnecessarily restrict the use of processors located overseas, even where the 'controller' has complied with the requirements of APP 8.
- The exception in section 6FC(3)(a)(i) and (ii) appears to limit unlawful activity and wrongdoing of a serious nature, to that *only* involving fraud. This is unnecessarily limited and could give rise to other information sharing related unlawful activity or serious wrongdoing being considered a trade of information (eg, scams or money laundering). As drafted we do not believe the exception appropriately captures all of the activities identified above in respect of legitimate risk intelligence, sanctions screening, adverse media screening and due diligence services that financial institutions rely on.

Recommendations:

- Include an exception to the prohibition on trading personal information for intra-group and multinational group transfers, where those transfers occur pursuant to appropriate contractual protections.
- Include an exception to the prohibition on trading personal information for direct

marketing or introducer purposes where the sharing of personal information is based on a request of an individual.

- Update the exception for processors to capture non-APP entities; removing the 'involving fraud' limitation in section 6FC(3)(a)(i) and (ii).
- Clarify and, where appropriate, create an exception to ensure that the provisions do not inadvertently restrict the provision and use of risk screening and due diligence services that financial institutions rely upon to meet their regulatory and compliance obligations.

5. Processor/controller framework and definition of 'discloses'

Whilst we are supportive of GDPR concepts being included in the Privacy Act, we seek clarification on:

- the interaction between the Privacy Act and the Commonwealth contracting regime, including the rationale for excluding contracted service providers as 'processors'; and
- the rationale for limiting 'processors' to APP entities only, particularly given the requirements of APP 8 continue to apply to the 'controller'.

Recommendations:

- 'Processors' should be expanded to include non-APP entities who act on behalf of an APP entity.
- Minimum contractual content (via OAIC guidance) should be prescribed regarding when a processor is acting on behalf of a controller, rather than relying on 'documented instructions' alone. Further detail will be needed to understand the level of detail expected for 'documented instructions' to meet the requirements of the processor / controller provisions.

6. GDPR alignment

We support the introduction of a controller and processor framework. This would better align Australian privacy law with international privacy practice and recognise that accountability should principally sit with the organisation that determines the purposes and means of handling personal information. Many global financial services firms already structure contracts, governance and operating processes using GDPR-style roles. To avoid unnecessary complexity, the Australian framework should align closely with GDPR concepts, unless a deliberate policy difference is intended.

Even with alignment to GDPR style concepts, implementation will still require significant uplift. Organisations will need to confirm controller and processor roles across intra-group arrangements, outsourced administration, technology providers and other third-party servicing models, and then reflect those roles in contracts, documented instructions and governance processes.

Recommendations:

- Align the controller and processor framework as closely as possible with the GDPR, and clearly identify any intended differences.
- Clarify whether existing GDPR style assessments and documentation can be relied

upon to establish compliance with the proposed reforms (for example, GDPR controller / processor determinations).

- OAIC guidance should address role allocation, including handling of complex arrangements such as multi-party processing, documented instructions and the consequences where a processor acts beyond its instructions.

7. The "fair and reasonable" test

While the new test is intended to simplify key principles, in practice the test imposes a significant compliance burden on organisations' day-to-day activities, particularly where pro-active consideration of all factors identified in APP 3.2 is required before any collection, use or disclosure (including use or disclosure of existing personal information datasets). A stronger carve-out for exemption cases would assist in reducing unnecessary compliance overload. The current exemption for conduct required or authorised by Australian law or a court/tribunal order is too narrow, as legal obligations frequently arise from regulatory "soft law" (for example, APRA or ASIC guidance or regulator expectations).

The 'genuine choice' factor (APP 3.2(e)), which considers whether an individual is provided with genuine choice in relation to the collection, use or disclosure of their personal information, may have the unintended effect of suggesting that processing necessary to meet regulatory or contractual requirements is not fair or reasonable solely because the individual lacks a meaningful ability to withhold consent.

Recommendations:

- Broaden the exemptions to cover collection, use and disclosure of personal information for 'soft law' compliance obligations. Organisations would also benefit from guidance from the OAIC as to how this test is to be applied, including comparison with well-known international standards such as GDPR's legitimate-interest assessment.
- Provide clear guidance on how the factors in APP 3.2 should be weighted.
- Clarify that a lack of genuine choice arising solely from a regulatory or contractual requirement should not result in a finding that the collection, use or disclosure was not fair or reasonable under APP 3.2(e).

8. Requirement to consider destruction of personal information

While we consider it sensible for organisations to be required not to retain personal information once it is no longer needed for any purpose, we are concerned that the standalone requirement in APP 11.2(a) to 'consider whether to destroy' personal information adds a compliance and documentation burden without altering the substantive obligation already imposed by APP 11.2(b), which requires an entity to take reasonable steps to either destroy or de-identify the information. Organisations should retain discretion as to whether destruction or de-identification is the more appropriate outcome in the circumstances, having regard to the practicalities of each case.

Recommendation:

- Remove APP 11.2(a) “consider whether to destroy the personal information” and retain APP 11.2(b).

9. Data access

We are supportive of the new APP 12.3A access request exception for responding to access requests involving legacy archives, backups and immutable records.

10. Right to erasure and definition of Large Digital Platform

Definition of Large Digital Platform

The proposed definition of 'large digital platform' may capture a large number of organisations that do not operate the kind of 'platform' the explanatory information appears intended to capture (social media, messaging, email, gaming and streaming services or platforms).

The inclusion of 'designated internet service', which captures services that enable end-users to access or deliver material via the internet would capture most types of website, including financial services platforms. It also does not appear limited to consumer-focused services, given the broad meaning that could be attributed to 'end-user'. We are concerned that 'designated internet service' has no size, revenue, commercial-purpose or content threshold, and the eSafety Commissioner has described it as covering most apps and websites. The only relevant exclusion applies where no material is accessible to Australian end-users.

The proposed definition may unintentionally capture financial services client portals. For example, an authenticated investor portal for statements, holdings data and reports may fall within this definition. The revenue test would then be met automatically by most global financial institutions because section 6EB(3) aggregates group revenue, regardless of Australian source. This could regulate a wholesale investment manager with no consumer digital platform business as a large digital platform.

Further, the Exposure Draft does not provide clarity around who the 'provider' is where an outsourced portal is presented under the fund manager's brand.

Given the proposed APP 14.1 applies at the organisation level, this may have unintended effects (eg, if a particular portal triggers classification, the erasure right would extend to records unrelated to the portal/across the organisation's entire data holdings). Given the broad extra-territorial application of the Privacy Act, this could have significant unintended consequences for the application of the Privacy Act far beyond Australia and information collected from or related to individuals in Australia.

New APP 14

APP 14.1 should be clarified to confirm that it does not apply to information already de-identified under section 6FG, since it no longer relates to an identifiable individual. This would remove uncertainty in relation to anonymisation based retention programs.

We are supportive of the exceptions in proposed APP 14.3(c) and (e) and consider those exceptions are essential. They should not be narrowed.

The exception in APP 14.3 does not sufficiently capture the myriad of circumstances where financial services organisations may be *authorised* to retain personal information, or where an organisation may be expected to retain such information for legitimate business operation purposes (eg, for fulfilling contractual obligations with individual or corporate clients, or for initiating or defending legal claims within the relevant statutory limitation periods), or as part of managing compliance and risk associated with its legal and regulatory obligations for

example to mitigate fraud and scams.

Finally, whilst APP 11.2(b) permits destruction or de-identification of personal information, APP 14.1 requires an organisation to destroy personal information. There is no ability to de-identify such information instead. This creates an unexplained inconsistency, disadvantages entities relying on de-identification, and may force destruction where de-identification would achieve the same privacy outcome while preserving transactional and registry integrity.

Recommendations:

In relation to the definition of 'Large Digital Platform':

- Financial services entities should be exempt from the large digital platform thresholds, as financial institutions are already heavily regulated by sector regulators, with multinational firms already complying with multiple sector-regulator regimes.
- Should the provision continue to apply to financial services, further consideration needs to be given to the exceptions to actioning a right to erasure. We strongly recommend that the Act permit the creation of additional exceptions, by regulation, to ensure that the framework is appropriately tailored to the financial services industry.
- If the definition of 'Large Digital Platform' is retained:
    (i) The end-user test and gross-revenue tests should (i) apply only to activities conducted directly in Australia and (ii) be conjunctive, rather than distinctive.
    (ii) The definition should exclude platforms that are predominantly business-to-business or do not offer services to the public at large.
    (iii) The definition should clarify the operation of the definition where outsourced administrators operate the relevant service.

In relation to the substance of APP 14:

- APP 14 should not apply to information that has already been de-identified within the meaning of s 6FG.
- APP 14 should permit de-identification or destruction (at the organisation's election).
- The exceptions to destruction should be broader to enable platforms to retain information where it is authorised by law or reasonably necessary for legitimate business operations (including managing risk of claims by retaining information for statutory limitation periods) or managing fraud and scam prevention and legal compliance.

11. Overseas transfers, APP 8 and Permitted General Situation (PGS) 4, 5 and 10

Proposed updates to PGS 4, 5 and 10 restrict disclosures to recipients that are not overseas recipients. These permitted general situations facilitate cross-border transfers by multinational corporations whose operations and regulatory obligations necessitate such transfers. In practice, the proposed restrictions may render these PGS's unusable by global

financial institutions, whose global operations mean that they are likely to have to disclose information to overseas recipients for purposes of legal claims, alternative dispute resolution or enforcement bodies.

We note that the 2024 Privacy Act reforms introduced a whitelisting mechanism empowering the prescription, by regulation, of countries or binding schemes providing privacy protections substantially similar to the APPs and appropriate enforcement mechanisms. This power has not yet been exercised.

Recommendations:

- Reinstate PGS 4, 5 and 10 to their current form by removing the proposed condition that disclosures may only be made to recipients who are not overseas recipients.
- The Government prescribe whitelisted countries under the existing regulatory power to provide certainty for cross-border disclosures.

12. Permitted General Situation (PGS) item 2

The inclusion of 'precise geolocation tracking data' into the definition of 'sensitive information' will impose significant limitations on the use of such data, particularly in relation to fraud and scam prevention. Requiring consent would materially impact the ability for organisations to proactively monitor and detect potential fraudulent, scam or illegal activity.

Recommendation:

PGS 2 should be further updated to permit personal information (including sensitive information) to be collected, used and disclosed for pre-emptive security measures (eg, fraud and scam monitoring) without requiring the consent of the relevant individual.

13. 72-hour notification for eligible data breaches

We do not oppose a 72-hour notification period and it is, in principle, consistent with GDPR requirements. However, we consider that the threshold for incomplete reporting is too low (ie, it is required where full reporting is 'impossible or impracticable'). Early forensic uncertainty is routine, especially when scoping affected individuals, data elements and serious harm, or when dependent on third-party or offshore investigations.

Further, partial notification to individuals, in such a short time following an incident, may generate additional harms for individuals (such as anxiety) as well as generate unnecessary activities for the organisation and others (for example, individuals may try to cancel government identification documents unnecessarily). We suggest that the period for notifying the OAIC is decoupled from the period for notifying individuals.

Recommendations:

- Replace 'impossible or impracticable' with 'not reasonably possible' in section 26WK(5)(a) (in alignment with Article 33(4) of the GDPR).
- Decouple the period for notifying the OAIC with the period for notifying individuals.

- Clarify the interaction between, and effect of, the new suspicion-based mitigation duty in section 26WDB and the section 26WH assessment period.
- Clarify whether a report can cover affected group entities.
- Confirm whether a streamlined means of lodging a single comprehensive report for eligible data breaches which may also be reported to other regulators, such as ASIC and APRA, will be available to mitigate the operational burden of multiple reporting requirements for the same incident.

14. Implementation timeline

Given the breadth and complexity of the proposals, implementation will take significant time and resources. For global groups, implementation will not be limited to Australian systems, as records and data often sit on shared global platforms, and breach response, retention and deletion processes operate group-wide. The changes required to achieve compliance will require cross-jurisdictional coordination to review and change process and system settings, including retention and destruction settings, incident procedures, intra-group arrangements, as well as engage with third party vendors. The technical and operational changes required to identify and assess existing datasets pursuant to the new definition of personal information, as well as the fair and reasonable test, along with changes to give effect to the right to erasure, should not be underestimated. The Government must give organisations sufficient time to review existing information held and uplift internal processes and technical systems.

Recommendation:

Given the significant activities required for implementation, the implementation period should be no less than 24 months. If commencement is staged, dates should be settled in the Bill as introduced so organisations can plan and resource with certainty.

Next steps

ASIFMA members would be happy to provide further information or clarification on this submission. Should you have any questions, please contact **Ms. Diana Parusheva-Lowery, Managing Director, Head of Public Policy and Sustainable Finance at ASIFMA**, at [dparusheva@asifma.org]. This submission was prepared based on feedback from the wider ASIFMA membership.

Yours faithfully



Diana Parusheva-Lowery
Managing Director – Head of Public Policy and Sustainable Finance
Asia Securities Industry & Financial Markets Association (ASIFMA)
www.asifma.org