

18 September 2026

Privacy Reform

Attorney-General's Department

Submitted online

Dear Attorney-General's Department,

Consultation on the Privacy Amendment (Personal Data Protection) Bill 2026

The Financial Advice Association Australia (FAAA)¹ welcomes the opportunity to comment on the Privacy Amendment (Personal Data Protection) Bill 2026 (Exposure Draft Bill) and accompanying Privacy Reform Consultation Paper, released by the Attorney-General's Department on 31 August 2026.

The FAAA is the largest professional body representing financial advisers in Australia, with more than 10,000 members. Financial advisers routinely collect, use and retain some of the most personal information individuals share with any professional adviser, including identification documents, health information, family and relationship circumstances, estate planning matters, and detailed financial information. Strong and effective privacy protections are therefore fundamental to maintaining trust in the financial advice profession.

In preparing this submission, the FAAA sought input from members through a dedicated working group to understand how the proposed reforms would operate in financial advice practices, and identify practical implementation issues for advisers, licensees and their clients.

The FAAA supports the Government's objective of strengthening privacy protections and enhancing consumer trust in the handling of personal information. Our member feedback highlights the need to ensure the reforms also operate coherently alongside existing financial services, AML/CTF, dispute resolution and record-keeping obligations. Accordingly, this submission focuses on practical measures to improve clarity and implementation, including: guidance on the fair and reasonable handling test, consent in ongoing advice relationships, data minimisation and retention requirements, referral arrangements, data breach notification obligations, dispute resolution processes and the growing use of artificial intelligence.

Our analysis and recommendations are set out below.

¹ The Financial Advice Association of Australia (FAAA) is the largest association representing the financial advice profession in Australia, with over 10,000 members. FAAA advocates for the interests of financial advisers and their clients across the country.

1. Fair and reasonable handling, consent and notice requirements

1.1 Interaction with record-keeping, best interests and ongoing monitoring obligations under financial services law

The proposed new framework would introduce a principles-based 'fair and reasonable' test through proposed APP 3.1 and APP 3.2, requiring the collection, use and disclosure of personal information to be fair and reasonable in the circumstances having regard to factors including reasonable expectations, the relationship to the entity's functions or activities, transparency, data minimisation, genuine choice, and proportionality of privacy impacts.

One of the key issues for the financial advice profession is the interaction between the proposed fair and reasonable test and advisers' existing legal obligations under the Corporations Act, AML/CTF Act, AFCA dispute resolution framework and licensee compliance requirements. Financial advisers are already subject to extensive statutory and professional obligations that require them to collect, verify, retain and use personal information throughout the adviser-client relationship. In particular, the Best Interests Duty in section 961B of the Corporations Act requires advisers to identify and understand a client's objectives, financial situation and needs, make reasonable inquiries where information is incomplete or inaccurate, and obtain information necessary to provide advice that is appropriate to the client's circumstances. These obligations cannot be discharged without collecting and using extensive personal information. Most client relationships with financial advisers are ongoing relationships, meaning that further advice is provided progressively over time. Each time that further advice is provided, the adviser needs to rely upon both information previously collected and new information that becomes relevant.

The legislation should therefore make clear that the collection, use, disclosure and retention of personal information that is reasonably necessary to comply with statutory, regulatory, professional and dispute-resolution obligations will generally be regarded as fair and reasonable. This is particularly important in the context of ongoing advice relationships, where advisers may need to access historical client information years after it was originally collected, to: provide further advice, review existing strategies, manage insurance claims, assist in the administration of estates, or to satisfy regulatory and record-keeping requirements. In limited circumstances a financial adviser may also need to refer to that information in responding to complaints.

Members are concerned that the breadth and contextual nature of the proposed test may create uncertainty for advice practices seeking clear and repeatable compliance processes. This is particularly relevant given the sensitive and diverse information advisers routinely handle, and the fact that information that may not appear relevant at the commencement of an engagement can become relevant as advisers investigate a client's circumstances and develop appropriate advice strategies. An overly narrow interpretation of the data minimisation requirement could discourage appropriate fact-finding and create uncertainty about the information advisers can reasonably collect to satisfy their obligations under the Best Interests Duty and the Financial Planners and Advisers Code of Ethics, both of which require advisers to obtain and consider sufficient information about the client before providing advice.

Recommendation 1: Amend the proposed legislation to expressly confirm that collection, use, disclosure, access and retention undertaken to comply with statutory obligations, including obligations under financial services and AML/CTF legislation, satisfy the fair and reasonable test and fall within the

exception for conduct required or authorised by law. The OAIC should develop worked examples specific to the financial advice lifecycle, including ongoing service arrangements, inactive and returning clients, insurance claims, estate administration and long-term record retention.

1.2 'Specific' and 'unambiguous' consent in an ongoing advice relationship

The FAAA supports the objective of ensuring client consent is genuine and informed. However, the financial advice relationship is fundamentally an ongoing professional relationship rather than a series of discrete transactions. Advisers are subject to statutory and professional obligations that require client information to be collected, used and retained throughout the lifecycle of that relationship.

In particular, the Best Interests Duty in section 961B of the Corporations Act requires advisers to identify and understand a client's objectives, financial situation and needs, make reasonable inquiries where information is incomplete or inaccurate, and base advice on the client's relevant circumstances. The safe harbour steps in section 961B(2) recognise that advisers must undertake comprehensive fact-finding and collect sufficient information before advice can be provided. Information obtained at one point in time may also need to be revisited and relied upon for future reviews, implementation activities, insurance claims, estate planning matters and other advice interactions. Similarly, the Code of Ethics contemplates ongoing access to client information to enable advisers to act in their clients' best interests and provide professional services competently.

In this context, the proposed requirement that consent be voluntary, informed, current, specific and unambiguous creates uncertainty as to whether advisers will need to obtain fresh consent whenever personal information is used for a review, implementation activity or related advice purpose. We are concerned that this obligation reflects a transactional relationship rather than an ongoing professional relationship, creating additional compliance costs and client friction without necessarily improving privacy outcomes. The framework should recognise that, where a client enters into an ongoing advice relationship, consent can be obtained at the commencement of the engagement for reasonably foreseeable advice, implementation and review activities. Renewed specific consent should only be required where there is a material change in purpose, scope or parties involved.

Recommendation 2: Amend the legislation or accompanying guidance to expressly recognise enduring consent within an ongoing professional advice relationship, allowing advisers to obtain consent at the commencement of an engagement for reasonably foreseeable advice, implementation and review activities. The OAIC should provide worked examples demonstrating when existing consent remains effective and when fresh consent is required due to a material change in purpose or scope.

1.3 Consent to trade personal information - referral arrangements

The Bill introduces a new requirement through proposed APP 4.2 for consent before an organisation 'trades' personal information. Proposed section 6FC defines a trade to include disclosures for money or other consideration, or for the purposes of direct marketing, subject to specified exceptions, including where the disclosure is for the recipient to provide a product or service requested by the individual. Holistic financial advice frequently involves an adviser referring client information to another specialist financial adviser such as a risk adviser for life insurance advice, a mortgage broker for a home loan, an accountant for tax advice, or an aged care specialist for placement advice, referrals that are made

because the client has asked the adviser to help arrange these services. We would not describe this as a trade; however, we are concerned about what might be captured under this term.

Recommendation 3: Clarify, through guidance or drafting refinement, that referrals made by a financial adviser to other professionals, for the purpose of delivering the holistic advice or service the client has requested, fall within the existing carve-outs to the definition of ‘trade’ and do not require separate consent to ‘trade’.

2. Handling of personal information

The FAAA supports the proposed amendment to Permitted General Situation 2 and the consequential amendment to APP 12.3(h), broadening its application from ‘misconduct of a serious nature’ to ‘wrongdoing of a serious nature’, including conduct by a person acting in a private capacity, such as exploitation of a customer’s vulnerability or misuse of an enduring power of attorney. Financial advisers, by virtue of their close and ongoing relationship with clients (particularly older clients and those with complex family circumstances), are well placed to identify early warning signs of potential financial abuse, coercive control or exploitation. A clearer and broader basis for advisers and licensees to collect, use or disclose personal information in order to take appropriate protective action in these circumstances is a welcome development.

The FAAA seeks further guidance on how this expanded PGS is intended to interact with an adviser’s existing legal duties of confidentiality, and with any state, territory or sector-specific safeguarding protocols that may also apply where financial abuse or exploitation is suspected. Clear, practical guidance would assist advisers to act confidently and appropriately in these sensitive situations, rather than being deterred from acting for fear of breaching either their duty of confidentiality or the Privacy Act.

Recommendation 4: Develop OAIC guidance on the practical application of the broadened PGS 2 to adviser detection of suspected financial abuse, including its interaction with financial advisers’ legal duties of confidentiality and other safeguarding obligations.

3. Data minimisation, de-identification and client portals

3.1 Application to advice records and client-controlled systems

The FAAA supports reducing unnecessary holdings of personal information. In financial advice, however, it is not always possible to determine whether information is relevant until inquiries and analysis have been completed. Under the law, advisers must usually collect a broad fact base before identifying which information is necessary for the advice, implementation, compliance review or a later insurance claim. As noted previously, financial advice is typically provided as part of an ongoing relationship, where reliance upon previously collected information is often essential. The proposed reform could therefore inadvertently discourage appropriate fact-finding or create pressure to delete information that remains important to the adviser’s ability to provide further financial advice that meets the Best Interest Duty in the Corporations Act.

We recognise that different considerations apply to current and former clients. For current clients, retaining historical information is often necessary to provide ongoing advice, meet the Best Interests

Duty, and assess changes in a client's circumstances overtime. For former clients, information may still be needed to be retained to satisfy record-keeping obligations, for audit purposes, or responding to complaints or AFCA disputes. While the rationale for record retention differs, the practical challenges associated with determining appropriate retention periods remains.

Member feedback also highlighted the difficulty of reconciling minimisation and deletion requirements with overlapping retention obligations under financial services, AML/CTF, dispute resolution and evidentiary frameworks. In some cases, different categories of information are subject to different retention requirements, creating uncertainty regarding when information can be deleted or de-identified. This is further complicated by client portals and document-storage tools. A portal may be established by an adviser but understood and used by the client as the client's own information repository. The adviser may have technical access to documents that were not requested, reviewed or used by the adviser. The reforms should clarify when information available through such a portal is taken to have been collected or held by the adviser or licensee, and where responsibility for data security and minimisation sits between the advice practice, client, and portal service provider.

Recommendation 5: Clarify that APP 11 does not require the collection, retention or deletion of information in a manner that compromises compliance with obligations under the Corporations Act, AML/CTF laws, dispute resolution requirements or other record-keeping obligations. Provide guidance on the treatment of information accessible through client portals and similar platforms.

3.2 De-identification and secure point-in-time access

Members expressed concern that de-identification is not necessarily a one-off or practical solution for advice records. Retrospective review and redaction of large record sets would impose substantial technology and compliance costs, particularly on small financial advice practices. Government should also consider whether privacy risk can be reduced by enabling advisers, with client authority, to verify high-risk information through secure government or trusted digital identity services at the point it is needed, rather than requiring clients and practices to repeatedly transmit and store copies. No access method is completely secure, but a point-in-time verification model may reduce unnecessary duplication of highly sensitive information.

Further guidance is also required regarding how data minimisation and deletion requirements are intended to operate where records may be needed for further advice, future claims, disputes, investigations or legal proceedings, and where retention periods differ across categories of information.

Recommendation 6:

- Clarify how data minimisation and the definition of collection apply where information is accessible through a client-controlled portal provided by the adviser, but has not been requested or used by the adviser.
- Provide proportionate, risk-based guidance on retention, destruction and de-identification, including examples for high-risk identifiers, insurance records, AML/CTF obligations and documents subject to extended legal retention requirements.
- Government should explore secure point-in-time verification mechanisms that reduce the need for advice practices to hold duplicate copies of high-risk personal information.

- Clarify the intended operation of proposed APP 11.2, including the requirement to consider whether to destroy personal information and to take reasonable steps to destroy or de-identify it, and how that obligation is intended to operate alongside the proposed exception in APP 11.3 for information required to be retained under Australian law.

4. Notifiable data breaches

4.1 The 72-hour notification requirement and small business capacity

The FAAA acknowledges the rationale for the proposed 72-hour notification requirement in section 26WK, which aligns the Privacy Act's data breach reporting framework with the reporting timeframes under the Security of Critical Infrastructure Act 2018 (Cth) and the Cyber Security Act 2024 (Cth). However, we note that a large majority of financial advice licensees and practices are small businesses without dedicated IT, security, legal or communications teams. A fixed 72-hour deadline to notify the Commissioner of an eligible data breach, even on an incomplete-statement basis, represents a significant operational challenge for a small practice, particularly where the practice must first establish the nature and scope of a breach that may have originated in a third-party system.

Member feedback indicates that the practical difficulty lies not only in preparing a notification, but in determining within 72 hours whether an incident is reportable. A practice may become aware late in the reporting period, including on a Friday afternoon, and may need information from its licensee, technology provider, platform or product provider before it can assess scope and eligibility. In some cases, the responsible provider may not confirm what occurred until much of the 72-hour period has elapsed, or indeed after it, especially if the provider is offshore. While proposed subsections 26WK(5) and (6) permit an incomplete statement to be provided where it is impossible or impracticable to provide all required information within 72 hours, further guidance would assist smaller businesses in understanding when those provisions can appropriately be relied upon. As an example of the timeframe required in other breach reporting regimes, Australian Financial Services Licensees have 30 days to report to ASIC under the Corporations Act.

Recommendation 7: Review the application of a 72-hour deadline for small businesses and clarify when the 72-hour notification period commences. Provide guidance on the circumstances in which entities may rely on the incomplete notification provisions in proposed subsections 26WK(5) and (6), including where information must be obtained from third-party providers.

4.2 Layered data chains - advisers, licensees, platforms and product providers

Client information handled in the course of financial advice typically passes through multiple hands - the adviser, the AFSL, financial planning software providers, investment and superannuation platforms, and other product providers such as insurers and fund managers. A data breach may originate at any point in this chain, and it will not always be immediately apparent to the adviser or licensee whose personal information has been affected, or the extent of the affected data set, particularly where the breach occurs at a platform or product provider that the client interacts with only indirectly. The Bill's obligations apply separately to each entity that holds the affected information, creating a real risk of duplicated, inconsistent or confusing notifications being received by the same client from multiple entities in the same distribution chain.

Recommendation 8: Simplify and make clear how responsibility and client notification should be coordinated across the data chain to avoid duplication and confusion.

5. Right to erasure on large digital platforms

The FAAA notes the proposed new APP 14 right to erasure applying to large digital platforms, with proposed section 6EB defining a large digital platform by reference to specified service types and revenue or end-user thresholds. While this obligation is directed at large digital platforms rather than financial advice licensees themselves, we note that some advice practices rely on platforms, portals or client-facing digital tools provided by larger technology or financial services groups that could potentially meet the large digital platform threshold. Where a client makes an erasure request directly to such a platform in relation to information that also forms part of an adviser's or licensee's statutory advice record, it is important that the proposed exceptions, including the exception for information required to be retained under Australian law, and the exception for information strictly necessary to continue providing an advice service, are interpreted and understood to protect the integrity of financial services record-keeping obligations.

Members also queried how an advice practice could verify that information had in fact been erased and how it would know whether a technology provider met the large digital platform threshold. Responsibility should not fall on advice practices to investigate platform status or infer the consequences of an erasure request from general terms and conditions. Instead, the Government should maintain a publicly accessible register of entities that meet the large digital platform definition. This would provide greater certainty for businesses that rely on those platforms and enable advice practices to understand when the APP 14 right to erasure may apply without undertaking their own legal or technical assessment.

Recommendation 9: Confirm that the right to erasure on large digital platforms does not override, and cannot be used to circumvent, a licensee's obligation to retain advice records. Establish a publicly accessible register of large digital platforms so that businesses can readily determine whether APP 14 applies to a particular provider, and provide a mechanism for advisers and licensees to identify information that must be preserved under Australian law or for the provision of an advice service.

6. OAIC powers and efficiency - dispute resolution

The Consultation Paper proposes that individuals generally be required to first raise privacy concerns with the relevant APP entity, with that entity required to provide accessible complaint mechanisms and respond within 60 days, before a complaint proceeds to the OAIC. Financial advice licensees are already subject to detailed internal dispute resolution (IDR) requirements under ASIC Regulatory Guide 271, and to external dispute resolution (EDR) through the Australian Financial Complaints Authority (AFCA), including prescribed response timeframes that differ from the proposed 60-day privacy complaint-handling timeframe. A single client complaint may raise both a financial advice quality issue and a privacy issue (for example, a complaint that a client's sensitive information was mishandled in the course of providing advice). Without clear guidance on how these two complaint-handling regimes interact, licensees risk running parallel, and potentially inconsistent, complaint processes for a single grievance.

Recommendation 10: Clarify how the proposed requirement to first raise privacy complaints with the entity, and the entity's 60-day response obligation, are intended to interact with existing IDR obligations under ASIC RG 271 and EDR through AFCA, to avoid parallel or conflicting complaint-handling processes for a single client complaint with both advice and privacy dimensions.

7. Emerging technology and artificial intelligence

Members noted the rapid expansion of AI-enabled services throughout financial services distribution chains, including platforms, product providers, software vendors and outsourced service providers. As advice businesses increasingly rely on third-party AI functionality, uncertainty can arise regarding: which entity controls personal information, whether providers use information for their own purposes, responsibility for responding to privacy requests or data breaches, and how information is handled following contract termination.

Recommendation 11: Develop practical OAIC guidance for businesses using AI-enabled services, including criteria for determining responsibility between businesses and technology providers, due diligence considerations, incident reporting responsibilities and controls governing the use of personal information for AI, analytics and service development.

Conclusion

The FAAA strongly supports the Government's objective of modernising Australia's privacy laws to reflect contemporary data practices and community expectations, and recognises the significant public benefit in strengthening consumer trust in the handling of personal information. Financial advisers are entrusted with some of the most sensitive information Australians hold, and a modern, workable privacy framework is squarely in the interests of the advice profession and its clients.

However, the FAAA considers that the reforms, as currently drafted, would benefit from further clarification of how the new principles-based standards are intended to interact with the extensive, pre-existing regulatory obligations that already govern the collection, use, disclosure and retention of client information in fields such as financial advice. Without this clarity, there is a real risk of unnecessary regulatory duplication and uncertainty, without a commensurate improvement in privacy outcomes for clients.

If you have any questions about our feedback, please do not hesitate to contact me on 02 9220 4500 or sarah.abood@faaa.au.

Yours sincerely,



Sarah Abood

Chief Executive Officer

Financial Advice Association Australia (FAAA)