Australian
Finance
Industry
Association

31 March 2023

Ms Julia Galluccio

Assistant Secretary, Information Law Branch

Attorney-General's Department

Submitted via email to: privacyactreview@ag.gov.au

Dear Ms Galluccio,

Re: The Government's Response to the Privacy Act Review Report

The Australian Finance Industry Association (AFIA) is the only peak body representing the entire finance industry in Australia.[1] We appreciate the opportunity to respond to the Attorney-General's Department's consultation on the Government's Response to the Privacy Act Review Report.[2]

We represent over 150 members, including bank and non-bank lenders, finance companies, fintechs, providers of vehicle and equipment finance, car rental and fleet providers, and service providers in the finance industry. We are the voice for advancing a world-class finance industry and our members are at the forefront of innovation in consumer and business finance in Australia. Our members finance Australia's future.

We collaborate with our members, governments, regulators and customer representatives to promote competition and innovation, deliver better customer outcomes and create a resilient, inclusive and sustainable future. We provide new policy, data and insights to support our advocacy in building a more prosperous Australia.

[1] Australian Finance Industry Association (afia.asn.au).
[2] https://consultations.ag.gov.au/integrity/privacy-act-review-report/.

Australian Finance Industry Association
ABN 13 000 493 907

INTRODUCTORY COMMENTS

On 16 February 2023, the Attorney-General of Australia, the Hon. Mark Dreyfus KC MP, released the *Privacy Act Review Final Report December 2022: Achieving a Just and Secure Society* ('the Review').[3]

AFIA supports the aims of these reforms to improve consumer safeguards, but we want to ensure any changes are implemented in a manner that most effectively achieves their objectives without inadvertently creating other risks and complexities for Australians and Australian businesses.

AFIA recognises that our privacy laws must evolve along with the changes across our economy and society. We agree with the Attorney-General that having sound privacy laws are important to the protect consumers. In releasing the Review, the Attorney-General said:[4]

> *Strong privacy laws are essential to Australians' trust and confidence in the digital economy and digital services provided by governments and industry.*

However, the Attorney-General also indicated the importance of consulting industry and relevant stakeholders prior to committing to any further changes in Australia's privacy laws. In releasing the Review, the Attorney-General said:

> *The Government is now seeking feedback on the 116 proposals in this report* ***before deciding what further steps to take****.*

As the Review acknowledges, many of the 116 proposals would, if adopted, change substantial aspects of Australia's privacy laws. This will have significant consequences for businesses and their customers.[5] As the Department recognises, many modern Australian companies operate globally or across many different jurisdictions.[6] In this context, it is essential to streamline and harmonise legal regimes as much as possible to facilitate compliance.

AFIA proudly represents Australia's entire finance sector, which contributes approximately $185.1 billion to Australia's Gross Domestic Product (GDP).[7] Our members have significant interactions with the *Privacy Act 1988* (Cth) ('the Act') and associated laws. For example, via the Privacy (Credit Reporting) Code 2014.[8]

[3] The full document referred to throughout this submission is here.
[4] Mark Dreyfus (Attorney-General of Australia), '*Landmark Privacy Act Review report released*' (16 February 2023).
[5] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 12, 72-8.
[6] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 282.
[7] IBIS World, *Finance in Australia* (31 March 2022): Finance in Australia - Market Size | IBISWorld.
[8] Office of the Australian Information Commissioner (OAIC), '*2021 Independent review of the Privacy (Credit Reporting) Code 2014*' (released 20 September 2022).

AFIA supports privacy laws that are appropriately tailored to maximise the safety and security of customers personal information. However, we note the Review recognises that often the right to privacy must be balanced against other competing and equally important legal rights, such as freedom of expression; law enforcement and the upholding of contractual obligations or the protection of commercially sensitive information or intellectual property.[9]

Hence, any changes to privacy laws should carefully balance the regular tensions between these foundational, complex, interrelated and often competing legal values and principles.[10]

In **Attachment A**, we respond in detail to all 116 proposals of the Review. Some of the proposals AFIA members think require the most careful consideration include:

1. Proposal 4.1's suggested changes to the definition of the term 'personal information' in the Act, including the addition of 'inferred' and 'generated' information.[11]
2. Proposal 7.1's suggested changes to the employee records exemption.[12]
3. Proposal 18.1 to 18.5's suggested introduction of five separate 'rights of the individual' to the Act, subject to the exceptions in Proposal 18.6.[13]
4. Proposal 19.1's suggested changes to automated decision making.[14]
5. Proposal 20.1's suggested changes on 'direct marketing, targeting and trading'.[15]
6. Proposal 25's suggested changes to enforcement approaches.[16]
7. Proposal 26's suggested new direct right of action for interferences with privacy.[17]
8. Proposal 27's suggested statutory tort of privacy, on pages 338 to 339 of the Review.[18]

The eight proposals outlined above would impose new legal obligations and regulatory burdens on entities covered by the Act.

AFIA supports updating privacy laws to ensure optimal consumer protections. However, we suggest any reforms should recognise the compelling legal interests that often compete with privacy and the importance of harmonising compliance obligations for global companies.[19] Any new legal rights adopted under Proposals 18.1 to 18.5, 25.1, 26.1 or 27.1 should recognise these legitimate competing interests and be subject to limitations on damages and statutory limitation periods.[20]

---

[9] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 18, 218-222.
[10] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 324-328.
[11] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 10, 27-29 and 38.
[12] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 12, 90-1.
[13] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 218-22.
[14] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 18 and 223.
[15] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 256-8.
[16] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 22-3 and 304-305.
[17] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 330.
[18] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 338 and 342.
[19] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 10, 27-29 and 218-22.
[20] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 218-22. See too Commonwealth Parliamentary Library, '*Legal actions and limitation periods*' (accessed on 24 March 2023).

AFIA also notes consideration must be given to the impact Proposal 6, removing the small business exemption to the *Privacy Act*, may have only SMEs with fewer resources.[21] If this is pursued, a phased approach would be required.

AFIA supports laws recognising privacy's importance. Yet we remain cognisant of the complex and interrelated nature of other legal rights that intersect with privacy.[22]

We support strengthening privacy laws in a way which is considered, measured, and balanced. Any changes should be targeted, proportionate, scalable and commensurate with the risk involved in the activity which is being regulated.

We look forward to working with the Government as it consults industry on the best path forward. Each of these 116 proposals must be considered on its merits and adopted in ways which will practically achieve the underlying objectives sought.

CLOSING COMMENTS

We would appreciate the opportunity to discuss our recommendations and provide further information.

Please feel free to contact AFIA's Senior Policy Adviser, Sebastian Reinehr at sebastian.reinehr@afia.asn.au.

Yours sincerely

Roza Lozusic
Executive Director, Policy and Public Affairs

[21] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 12, 66.
[22] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 218-22.

ATTACHMENT A – AFIA's RESPONSE TO THE PRIVACY ACT REVIEW REPORT

TABLE 1 – AFIA's Detailed Response to Recommendations from the *Privacy Act Review (Final Report)*

Recommendation	AFIA Member Feedback
3. Objects of the Act **Proposal 3.1** Amend the objects of the Act to clarify that the Act is about the protection of personal information. **Proposal 3.2** Amend the objects of the Act to recognise the public interest in protecting privacy.	• AFIA understands the importance of protecting privacy. Yet, there are potential unintended consequences of amending the objects of the Act to recognise a 'public interest in protecting privacy' per Proposal 3.2.[23] • Such a change will impact how all other provisions of the Act must be interpreted, given the basic legal principle that the words of specific legislative provisions must be interpreted in accordance with a legislative instrument's purposes.[24] • Significant consultation should be undertaken on the specific legislative definition of any such 'public interest' object of the Act.[25] • This is important due to the amorphous nature of the 'public interest'. The Office of the Australian Information Commissioner (OAIC) has acknowledged proposal 3.2 is questionable as: 'it is open to interpret the public interest in the economic wellbeing of the country as conceivably capturing any commercial practices, which may undermine the benefits of the proposal'.[26] • The Review raises concern about how this new 'public interest' object of the Act might interact with other proposals, such as proposal 12.1's introduction of a legislated 'requirement that the collection, use and

[23] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 10, 27-29.
[24] *Acts Interpretation Act 1901* (Cth), s 15AA.
[25] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 10, 27-29.
[26] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 27.

	disclosure of personal information must be fair and reasonable in the circumstances'.[27] • The Review acknowledges there are 'countervailing' or 'competing' public interests that could be applied to the same case.[28]
4. Personal Information **Proposal 4.1** Change the word 'about' in the definition of personal information to 'relates to'. Ensure the definition is appropriately confined to where the connection between the information and the individual is not too tenuous or remote, through drafting of the provision, explanatory materials and OAIC guidance. **Proposal 4.2** Include a non-exhaustive list of information which may be personal information to assist APP entities to identify the types of information which could fall within the definition. Supplement this list with more specific examples in the explanatory materials and OAIC guidance. **Proposal 4.3** Amend the definition of 'collection' to expressly cover information obtained from any source and by any means, including inferred or generated information. **Proposal 4.4** 'Reasonably identifiable' should be supported by a non-exhaustive list of circumstances to which APP entities will be expected to have regard in their assessment. **Proposal 4.5** Amend the definition of 'de-identified' to make it clear that de-identification is a process, informed by best available practice, applied to	• AFIA seeks more information on how changes to the phrases 'relates to' and 'too tenuous or remote' in Proposal 4.1 may affect existing data sets.[29] Greater clarity is sought on how these definitional changes materially change the existing definitions of personal information. • AFIA supports Proposal 4.2's suggested list of specific examples in the explanatory materials and OAIC guidance.[30] We specifically ask that any such guidance be released in advance for public consultation and contain significant examples relevant to the financial services sector. For example, guidance for credit providers, debt collectors, banking and other similar activities. • AFIA seeks further information and consultation on the specific proposed definitions of information which is 'inferred' or 'generated' under Proposal 4.3. The explanatory materials accompanying such proposals should provide clear examples of inferred and generated information types and how they apply to the financial services sector.[31] This proposal could potentially impose significant obligations on APPs regarding a much wider range of data, which could have unintended regulatory and compliance consequences.

[27] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 143 and 148.
[28] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 8 and 18.
[29] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 10, 27-29.
[30] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 10, 39.
[31] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 10, 38.

personal information which involves treating it in such a way such that no individual is identified or reasonably identifiable in the current context. Proposal 4.6 Extend the protections of the Act to de-identified information: (a) APP 11.1 – require APP entities to take such steps as are reasonable in the circumstances to protect de-identified information: (a) from misuse, interference and loss; and (b) from unauthorised re-identification, access, modification or disclosure. (b) APP 8 – require APP entities when disclosing de-identified information overseas to take steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles in relation to de-identified information, including ensuring that the receiving entity does not re-identify the information or further disclose the information in such a way as to undermine the effectiveness of the de-identification. (c) Targeting proposals – the proposed regulation of content tailored to individuals should apply to de-identified information where it is used in that act or practice. Proposal 4.7 Consult on introducing a criminal offence for malicious re-identification of de-identified information where there is an intention to harm another or obtain an illegitimate benefit, with appropriate exceptions. Proposal 4.8 Prohibit an APP entity from re-identifying de-identified information obtained from a source other than the individual to whom the information relates, with appropriate exceptions. In addition, the prohibition should not apply where:	• If Proposal 4.4's is adopted, we supports the development of a non-exhaustive list of circumstances to guide APP's assessment of when a person is 'reasonably identified' based off particular information, to help guide compliance with the Act's requirements for the protection of personal information.[32] • However, a simpler approach would be to define 'identifiable' under Proposal 4.4 as information making an individual 'capable of being distinguished from all others, even if their identity is not known'.[33] • AFIA seeks clarity on Proposal 4.5's suggested change to the definition of 'de-identified', to clarify that de-identification requires 'best available practice' be used. Guidance is needed on how the term 'best available practice' accords with the 'reasonable steps' test in Proposal 4.6 on de-identified information.[34] • AFIA members seek further explanation of what be required to meet the 'reasonable steps' test which is suggested in Proposal 4.6 regarding the protection of 'de-identified information', as defined under s 6 of the Act.[35] AFIA members request that any specific regulatory changes to APP 11.1 or APP 8 be the subject of separate consultation.[36] • AFIA members have suggested Proposal 4.6(a) may create undesirable complexity in creating three categories of information – personal information, de-identified personal information, and all other forms of information. Members have suggested the Review's concern to protect

[32] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 10, 44-5. See too the definition of 'personal information in s 6 of the *Privacy Act*, which includes the as yet undefined term 'reasonably identifiable'.
[33] Anna Johnston and Alex Kotova, *Submission to the Attorney-General Department's Consultation on the Review of the Privacy Act: Final Report* (31 March 2023), 5.
[34] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 10, 50-2.
[35] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 10, 50-2.
[36] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 10, 49-50.

(a) the re-identified information was de-identified by the APP entity itself - in this case, the APP entity should simply comply with the APPs in the ordinary way. (b) the re-identification is conducted by a processor with the authority of an APP entity controller of the information. **Proposal 4.9** (a) Amend the definition of sensitive information to include 'genomic' information. (b) Amend the definition of sensitive information to replace the word 'about' with 'relates to' for consistency of terminology within the Act. (c) Clarify that sensitive information can be inferred from information which is not sensitive information. **Proposal 4.10** Recognise collection, use, disclosure and storage of precise geolocation tracking data as a practice which requires consent. Define 'geolocation tracking data' as personal information which shows an individual's precise geolocation which is collected and stored by reference to a particular individual at a particular place and time, and tracked over time.	de-identified information is well placed. However, if de-identified information is at risk of re-identification, it should not be treated as de-identified and instead continue to be treated as personal information, to avoid the introduction of a third tier. • AFIA members seek clarity regarding how this 'such reasonable steps' test would cohere with the 'best available practice' standard suggested in proposal 4.5.[37] • AFIA supports Proposal 4.8, if our alternative Proposal 4.4 is not adopted.[38] • AFIA members have expressed a desire to see more information related to Proposal 4.10's suggested inclusion of 'geolocation tracking data' within s 6's definition of personal information.[39]

[37] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 10, 48.
[38] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 10-11, 52. For our preferred approach, see Anna Johnston and Alex Kotova, *Submission to the Attorney-General Department's Consultation on the Review of the Privacy Act: Final Report* (31 March 2023), 5.
[39] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 11, 57-9.

5. Flexibility of the APPs **Proposal 5.1** Amend the Act to give power to the Information Commissioner to make an APP code where the Attorney-General has directed or approved that a code should be made: (a) where it is in the public interest for a code to be developed, and (b) where there is unlikely to be an appropriate industry representative to develop the code. In developing an APP code, the Information Commissioner would: (a) be required to make the APP Code available for public consultation for at least 40 days, and (b) be able to consult any person he or she considers appropriate and to consider the matters specified in any relevant guidelines at any stage of the code development process. **Proposal 5.2** Amend the Act to enable the Information Commissioner to issue a temporary APP code for a maximum 12-month period on the direction or approval of the Attorney-General if it is urgently required and in the public interest. **Proposal 5.3** Amend the Act to enable Emergency Declarations to be more targeted by prescribing their application in relation to: (a) entities, or classes of entity (b) classes of personal information, and (c) acts and practices, or types of acts and practices. **Proposal 5.4** allow Emergency Declarations in relation to ongoing emergencies. **Proposal 5.5** Amend the Act to permit organisations to disclose personal information to state and territory authorities under an Emergency Declaration, provided the state or territory has enacted comparable privacy laws to the Commonwealth.	• AFIA supports Proposals 5.1's capacity for the Information Commission to make an APP Code, as directed by the Attorney-General.[40] • However, AFIA members recommend any such Codes the Attorney-General may make must be available for a consultation of at least 60 days, not the 40 days suggested in the review, to give industry appropriate time to respond.[41] • Any Code developed at the direction of the Attorney-General under Proposal 5.1 must be subject to the normal rules for the disallowance of regulations under the *Legislation Act 2003* (Cth), or such equivalent oversight legislation as may be in existence.[42] • Any Code developed under Proposal 5.1 must also be subject to parliamentary oversight and review by the Senate Standing Committee for the Scrutiny of Delegated Legislation or equivalent and the Parliamentary Joint Committee on Corporations and Financial Services.[43] • AFIA notes Proposals 5.2 to 5.5 insofar would allow for APP Codes to be made without the oversight mechanisms discussed with reference to Proposal 5.1. Any pursuit of these proposals must include provisions for any regulations made under Proposals 5.2 to 5.5 to be: 1. Subject to mandatory consultation periods, and/or;[44] 2. Subject to parliamentary scrutiny and disallowance.[45]

[40] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 11, 60.
[41] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 11, 61.
[42] Parliament of Australia, *Guides to Senate Procedure: Disallowance* (July 2022), 1.
[43] Parliament of Australia, *Guides to Senate Procedure: Disallowance* (July 2022), 1.
[44] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 11, 61.
[45] Parliament of Australia, *Guides to Senate Procedure: Disallowance* (July 2022), 1

6. Small business exemption **Proposal 6.1 Remove the small business exemption, but only after:**[46] (a) an impact analysis has been undertaken to better understand the impact removal of the small business exemption will have on small business - this would inform what support small business would need to adjust their privacy practices to facilitate compliance with the Act (b) appropriate support is developed in consultation with small business (c) in consultation with small business, the most appropriate way for small business to meet their obligations proportionate to the risk, is determined (for example, through a code), and (d) small businesses are in a position to comply with these obligations. **Proposal 6.2 In the short term:** (a) prescribe the collection of biometric information for use in facial recognition technology as an exception to the small business exemption, and (b) remove the exemption from the Act for small businesses that obtain consent to trade in personal information.	• AFIA notes complexities regarding the removal of the small business exemption in Proposals 6.1 to 6.2.[47] Removing the small business exemption will increase the regulatory burden on small businesses. Sufficient transition time will be needed for small businesses to prepare for such a change.

[46] OAIC, 'Does the Privacy Act Cover Your Business' (accessed on 22 March 2023): A small business is defined as having an annual turnover of $3 million or less.
[47] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 12, 72-8.

7. Employee records exemption **Proposal 7.1** Enhanced privacy protections should be extended to private sector employees, with the aim to: a) provide enhanced transparency to employees on what their personal and sensitive information is being collected and used for b) ensure employers have adequate flexibility to collect, use and disclose employees' information reasonably necessary to administer the employment relationship, including addressing the appropriate scope of individual rights and the issue of if consent should be required to collect employees' sensitive information c) ensuring that employees' personal information is protected from misuse, loss or unauthorised access and is destroyed when it is no longer required, and d) notifying employees and the Information Commissioner of any data breach involving employee's personal information which is likely to result in serious harm. Further consultation should be undertaken with employer and employee representatives on how the protections should be implemented in legislation, including how privacy and workplace relations laws should interact. The possibility of privacy codes of practice developed through a tripartite process to clarify obligations regarding collection, use and disclosure of personal and sensitive information should also be explored.	• On Proposal 7.1, we seek clarification of the term 'reasonably necessary to administer the employment relationship'.[48] • It is unclear if the phrase above includes actions that may have to be taken with respect to potential employees or former employees prior to commencement or after their leaving a financial institution. • AFIA seeks clarification on how the team 'reasonably necessary' may be applied in a financial services context, for example the need to share information and check references in banking. • AFIA members noted the implications of any changes to this exemption must be considered against the context of any reference checking requirements under relevant industry codes. • Therefore, AFIA members cannot confirm our position on Proposal 7.1. However, we agree with the review that any changes to the employee records exemption must 'ensure employers adequate flexibility to collect, use and disclose employees' information'.[49] • AFIA members have also indicated that any changes to this exemption should be made with an understanding of the following relevant sources and authorities on this topic: 1. The narrow interpretation already being applied to this exemption by Australian employment tribunals, including the Full Bench of the Fair Work Commission.[50] 2. Guidance from the Fair Work Ombudsman.

[48] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 12, 90-1.
[49] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 12, 91.
[50] See for example, *Lee v Superior Wood Pty. Ltd.* [2019] FWCFB 2946.

	3. The 2008 Australian Law Reform Commission Report.[51] 4. The Australian Government Agencies Privacy Code.[52] 5. The 'legitimate interests' test for employee data under the European *General Data Protection Regulation 2018* (GDPR). 6. The Information Commissioner (UK)'s guidance on confidential references.
8 Political exemption **Proposal 8.1** Amend the definition of 'organisation' under the Act so that it includes a 'registered political party' and include registered political parties within the scope of the exemption in section 7C. **Proposal 8.2** Political entities should be required to publish a privacy policy which provides transparency in relation to acts or practices covered by the exemption. **Proposal 8.3** The political exemption should be subject to the following requirements: (a) Political acts and practices covered by the exemption must be fair and reasonable. (b) Political entities must not engage in targeting based on sensitive information or traits which relates to an individual, with an exception for political opinions, membership of a political association, or membership of a trade union. The political exemption should include a savings clause as per Recommendation 41-2 of ALRC Report 108. **Proposal 8.4** The political exemption should be subject to a requirement that individuals must be provided with the means to:	• No comment[53]

[51] Australian ALRC, *For Your Information: Australian Privacy Law and Practice (ALRC Report 108)* (May 2008), 1363.
[52] Which commenced on 1 July 2018 and applies to all Australian Government agencies subject to the *Privacy Act*, except Ministers.
[53] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 12-13 and 92-105.

(a) opt-out of their personal information being used or disclosed for direct marketing by a political entity, and (b) opt-out of receiving targeted advertising from a political entity. Proposal 8.5 The political exemption should be subject to a requirement that political entities must: (a) take reasonable steps to protect personal information held for the purpose of the exemption from misuse, interference and loss, as well as unauthorised access, modification or disclosure (b) take reasonable steps to destroy or de-identify the personal information it holds once the personal information is no longer needed for a purpose covered by the political exemption, and (c) comply with the NDB scheme in relation to an eligible data breach involving personal information held for a purpose covered by the political exemption. Proposal 8.6 The OAIC should develop further guidance materials to assist political entities to understand and meet their obligations.	

9. Journalism exemption Proposal 9.1 To benefit from the journalism exemption a media organisation must be subject to: (a) privacy standards overseen by a recognised oversight body (the ACMA, APC or IMC), or (b) standards that adequately deal with privacy. Proposal 9.2 In consultation with industry, and the ACMA, the OAIC should develop and publish criteria for adequate media privacy standards and a template privacy standard that a media organisation may choose to adopt. Proposal 9.3 An independent audit and review of the operation of the journalism exemption should be commenced three years after any amendments to the journalism exemption come into force. **Proposal 9.4** Require media organisations to comply with security and destruction obligations in line with the obligations set out in APP 11. **Proposal 9.5** Require media organisations to comply with the reporting obligations in the NDB scheme. There will need to be some modifications so that a media organisation would not need to notify an affected individual if the public interest in journalism outweighs the interest of affected individuals in being notified.	• No comment.[54]

[54] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 13-14 and 106-116.

10. Privacy policies and collection notices **Proposal 10.1** Introduce an express requirement in APP 5 that requires collection notices to be clear, up-to-date, concise and understandable. Appropriate accessibility measures should also be in place. **Proposal 10.2** The list of matters in APP 5.2 should be retained. OAIC guidance should make clear that only relevant matters, which serve the purpose of informing the individual in the circumstances, need to be addressed in a notice. The following new matters should be included in an APP 5 collection notice: (a) if the entity collects, uses or discloses personal information for a high privacy risk activity —the circumstances of that collection, use or disclosure (b) that the APP privacy policy contains details on how to exercise any applicable Rights of the Individual, and (c) the types of personal information that may be disclosed to overseas recipients. **Proposal 10.3** Standardised templates and layouts for privacy policies and collection notices, as well as standardised terminology and icons, should be developed by reference to relevant sectors while seeking to maintain a degree of consistency across the economy. This could be done through OAIC guidance and/or through any future APP codes that may apply to particular sectors or personal information-handling practices.	• AFIA seeks guidance on how the terms: 'clear', 'concise' and 'understandable' would apply under Proposal 10.1.[55] • AFIA seeks information on the definition of the term 'such steps as are reasonable in the circumstances' under APP 5, regarding matters individuals must be made aware of in collection notices.[56] • AFIA agrees with proposal 10.2's suggested OAIC guidance on this topic. We support the limitation that only 'relevant matters' must be in collection notices under APP 5.2.[57] Such OAIC guidance must be subject to public consultation with industry. • AFIA seeks clarity on how the additional matters to be included in APP 5.2 under Proposal 10.2 interact with Proposal 4.1's suggested amended definition of personal information.[58] We also seek clarity on how Proposal 10.2's changes would interact with any amended definition of 'collection' under proposal 4.3.[59] • AFIA members support Proposal 10.3's suggested 'standardised templates' for privacy policies and collection notices.[60] Such templates should only serve as guides and provision of information in variant or amended forms should not have legal consequences, given the need to allow flexibility to respond to a range of circumstances. • Such templates should be developed in consultation with industry and finalised well in advance of new obligations taking effect.

[55] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 14 and 121.
[56] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 121.
[57] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 123.
[58] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 10.
[59] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 10.
[60] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 14 and 124-5.

	• AFIA seeks a legislative definition and OAIC guidance for the term 'high privacy risk' under proposal 10.2.[61] • Information Proposals 10.1 to 10.3's should be given on interactions between Proposals 13.1 to 13.3, which strengthen Privacy Impact Assessments.[62] • Clarification is sought regarding the additional matters in Proposal 10.2 6 their connections to Proposal 10.1. This is because longer collection notices are unlikely to be more clear or concise. AFIA members query if the additional details are required (particularly 10.2(b) as detailed below). • AFIA members seek clarity on the meaning of 'details on how to exercise any applicable rights', under Proposal 10.2(b).[63] Is this intended to be limited to the contact within the organisation who can assist with an exercise of rights, rather than a fulsome list of the means by which a consumer could take action? Members have suggested the latter would be difficult for businesses (particularly small businesses) to define, as it is highly context-driven and difficult to prescribe in a collection notice. Furthermore, a business cannot and should not be providing legal advice to consumers in these contexts. Information of this nature generally should be issued by OAIC, not individual businesses. • Further information is sought in relation to whether Buy Now, Pay Later (BNPL) services would be designated as a 'high privacy risk activity' under Proposal 10.2(a), as indicated in the previous Discussion Paper. If so, further explanation is sought as to why this is an appropriate designation, given BNPL providers use the same security safeguards as other industries.[64]

[61] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 14 and 123.
[62] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 15-6, 155-7.
[63] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 15.
[64] Attorney-General's Department, *Privacy Act Review: Discussion Paper* (December 2021), 47.

11. Consent and privacy default settings **Proposal 11.1** Amend the definition of consent to provide that it must be voluntary, informed, current, specific, and unambiguous. **Proposal 11.2** The OAIC could develop guidance on how online services should design consent requests. This guidance could address whether particular layouts, wording or icons could be used when obtaining consent, and how the elements of valid consent should be interpreted in the online context. Consideration could be given to further progressing standardised consents as part of any future APP codes. **Proposal 11.3** Expressly recognize the ability to withdraw consent, and to do so in a manner as easily as the provision of consent. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. **Proposal 11.4** Online privacy settings should reflect the privacy by default framework of the Act. APP entities that provide online services should be required to ensure that any privacy settings are clear and easily accessible for service users.	• AFIA seeks clarification on how the amended definition of consent of Proposal 11.1 will affect existing information held by APP entities.[65] • AFIA notes this emphasis on consent which is 'voluntary, informed, **current**, specific and **unambiguous**' is the same formulation the standard under both Article 7 and recital 32 of the GDPR.[66] • A slightly different standard of consent also applies under the Consumer Data Right (CDR) in Australia, which requires consent to be: 'voluntary, **express**, informed, specific as to purpose, **time limited and easily withdrawn**'.[67] • AFIA recommends a consistent definition of consent throughout relevant Australian laws, which is harmonised with international approaches, to facilitate ease of compliance. • AFIA seeks clarification as to how this new definition of explicit consent would interact with the definition of personal information which is 'collected' in an 'inferred' way under Proposals 4.3.[68] • The use of the term 'unambiguous' in Proposal 11.1 is a very high standard, which may rule out implied consent in almost all cases.[69] • The removal of implied consent must be reconciled with the *Spam Act 2003* (Cth), which allows for inferred consent to be inferred.[70] It is unclear how these concepts can be reconciled, or which will take precedence.

[65] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 14, 127-130.
[66] Intersoft Consulting, 'GDPR Consent' (accessed on 23 March 2023).
[67] Australian Competition and Consumer Commission (ACCC), Consumer Data Rights: Rules Outline, 21
[68] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 10-11 and 57-9.
[69] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 14, 127.
[70] *Spam Act 2003* (Cth), ss 4-5.

	• It should be noted Canada's *Personal Information Protection and Electronic Documents Act 2000* also allows implied consent, where individuals are well informed.[71] Similarly, in Europe under GDPR, consent is not required where a provider can rely on 'legitimate interests' as a basis for direct marketing.[72] • Implied consent also operates to support accessibility. For example, for people with disabilities to use assistive services and/or third parties to help them conduct their banking and financial transactions. • AFIA supports proposal 11.2's suggested OAIC guidance on obtaining valid consent. However, we emphasise there should be public consultation undertaken on this guidance.[73] Guidance should not be mandatory (in substance or form) and should provide flexibility to individual businesses. • AFIA seeks further consultation on the consequences of what would occur after consent is withdrawn, under proposal 11.3.[74] • AFIA members seek guidance on how this would impact other activities in the financial services industry, including internal evaluation of credit portfolio performance (i.e. use of information regarding identifiable loans, which may include personal information, on a portfolio level as part of performance, risk, fraud or other evaluation). • AFIA members would support in the introduction of a safe harbour for financial services businesses, or alternatively a legitimate business purposes test. • AFIA members have noted that 'bundled consent' can often be an effective way to provide customers all the

[71] Office of the Privacy Commissioner of Canada, *Guidelines for obtaining meaningful consent* (revised 13 August 2021).
[72] Information Commissioner's Office (UK), *When can we rely on legitimate interests?* (accessed March 30 2023).
[73] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 14 and 127-131.
[74] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 14 and 132-3.

	information they want without giving them 'consent fatigue' through repetition of similar processes. Proposal 11.1 should be implemented with consideration of its implications for these arrangements.[75]
12. Fair and reasonable personal information handling Proposal 12.1 Amend the Act to require that the collection, use and disclosure of personal information must be fair and reasonable in the circumstances. It should be made clear that the fair and reasonable test is an objective test to be assessed from the perspective of a reasonable person. Proposal 12.2 In determining whether a collection, use or disclosure is fair and reasonable in the circumstances, the following matters may be taken into account: (a) whether an individual would reasonably expect the personal information to be collected, used or disclosed in the circumstances (b) the kind, sensitivity and amount of personal information affected (c) whether the collection, use or disclosure is reasonably necessary for the functions and activities of the organisation or is reasonably necessary or directly related for the functions and activities of the agency (d) the risk of unjustified adverse impact or harm (e) whether the impact on privacy is proportionate to the benefit (f) if the personal information relates to a child, whether the collection, use or disclosure of the personal information is in the best interests of the child, and (g) the objects of the Act.	• On Proposal 12.1, we note complexities related to the potential unintended consequences flowing from an express requirement that the 'collection, use and disclosure' of 'personal information' must be 'fair and reasonable in the circumstances'.[76] • In principle, if such a proposal is to be adopted, we support the Review's suggestion the test be objective, not subjective, per tests in Canada, Singapore and other Australian privacy laws.[77] • AFIA seeks clarification on how Proposal 12.2's extension of factors relevant to the collection of personal information accord with the new definition of the term 'collect' in Proposal 4.3.[78] • On Proposal 12.2, AFIA members support a temporal element being made express in any legislated test, so the relevant conduct has to do with the **time at which** the 'collection, use or disclosure' occurred and not **any subsequent or preceding time period**. • AFIA members would ask the Department to especially consider factors (d)-(e) of Proposal 12.2 and provide further guidance.[79]

[75] In the context of bundled consent arrangements, the Department may consider how Proposal 11.1 would interact with Proposal 4.3 on generated information and Proposal 15.1 on secondary purposes.
[76] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 143-4.
[77] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 141.
[78] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 10-11 and 57-9.
[79] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 146-7.

The EM would note that relevant considerations for determining whether any impact on an individual's privacy is 'proportionate' and could include: (a) whether the collection, use or disclosure intrudes upon the personal affairs of the affected individual to an unreasonable extent (b) whether there are less intrusive means of achieving the same ends at comparable cost and with comparable benefits, and (c) any actions or measures taken by the entity to mitigate the impacts of the loss of privacy on the individual. Proposal 12.3 The requirement that collection, use and disclosure of personal information must be fair and reasonable in the circumstances should apply irrespective of whether consent has been obtained. The requirement that collection, use and disclosure of personal information must be fair and reasonable in the circumstances should not apply to exceptions in APPs 3.4 and 6.2. The reference to a 'fair means' of collection in APP 3.5 should be repealed	• The term **'unjustified adverse impact or harm'**, under Proposal 12.2(d), requires further definition.[80] • The factor **'whether the impact on privacy is proportionate to the benefit'** in proposal 12.2(e), is subject to of multiple reasonable interpretations. we seek further consultation on this term.[81] • Proposal 12.2(g)'s implications should be considered with Proposal 3.2's suggested expansion of the Act's objects to include the 'public interest'. We seek guidance on how the other factors in Proposal 12.2 will be balanced against 12.2(g). We note our comments outlined specifically regarding Proposal 3.2 of the Review.

[80] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 146-7.
[81] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 147-8.

13. Additional protections **Proposal 13.1** APP entities must conduct a Privacy Impact Assessment for activities with high privacy risks. (a) A Privacy Impact Assessment should be undertaken prior to the commencement of the high-risk activity. (b) An entity should be required to produce a Privacy Impact Assessment to the OAIC on request. The Act should provide that a high privacy risk activity is one that is 'likely to have a significant impact on the privacy of individuals'. OAIC guidance should be developed, articulating factors that may indicate a high privacy risk, and provides examples of activities that will generally require a Privacy Impact Assessment to be completed. Specific high risk practices could also outlined in the Act. **Proposal 13.2** Consider how enhanced risk assessment requirements for facial recognition technology and other uses of biometric information may be adopted as part of the implementation of Proposal 13.1 to require Privacy Impact Assessments for high privacy risk activities. This work should be done as part of a broader consideration by government of the regulation of biometric technologies. **Proposal 13.3** The OAIC should continue to develop practice-specific guidance for new technologies and emerging privacy risks. Practice-specific guidance could outline the OAIC's expectations for compliance with the Act when engaging in specific high-risk practices, including compliance with the fair and reasonable personal information handling test.	• On Proposal 13.1, AFIA members have suggested guidance on Privacy Impact Assessments should be in the Act itself. AFIA members suggest the term 'significant impact on privacy' is quite broad and lacks prior judicial consideration in Australia. Instead, AFIA members have suggested the term 'risk of serious harm' should be adopted for Privacy Impact Assessments, noting this term is used in the Notifiable Data Breach scheme.[82] • AFIA agrees with Proposal 13.2 that OAIC should provide specific guidance on the definition of the term 'likely to have a significant impact on the privacy of individuals', with recognition that this term will likely evolve over time.[83] Any such guidance should include provision of specific examples relevant to the financial services sector.[84] • AFIA agrees with Proposal 13.3 that OAIC should provide specific guidance on when entities must conduct a Privacy Impact Assessment for 'specific high risk practices' (a term which is requires further defintion). Such guidance should define this term and furnish examples relevant to financial services.[85] • AFIA seeks further information on Proposal 13.4's suggested changes to APP 3.6's requirements regarding information not collected directly from an individual. Guidance on this topic should include what constitutes 'reasonable steps', specific examples of scenarios relevant to the financial services sector and guidance on 'reasonable steps' to be taken in those example scenarios to meet obligations.[86]

[82] OAIC, '*What is a notifiable data breach?*' (accessed on 23 March 2023).
[83] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 15, 154.
[84] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 15, 155-6.
[85] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 15, 157-8.
[86] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 15, 161-3.

Proposal 13.4 Include an additional requirement in APP 3.6 to the effect that where an entity does not collect information directly from an individual, it must take reasonable steps to satisfy itself that the information was originally collected from the individual in accordance with APP 3. OAIC guidelines could provide examples of reasonable steps that could be taken.	• On Proposals 13.1 to 13.4, and all other relevant Proposals, there should be safe-harbour provisions to ensure that, where an APP entity has undertaken best endeavours to meet its obligations with respect to Privacy Impact Assessments, it avoids liability. • Clarification is required as to when entities may be prevented from using Facial Recognition Technology (FRT) for assessments under Proposals 13.1 and 13.2. FRT is a key tool for fraud prevention and without this technology, entities could be open to higher fraud risks.[87]
14. Research **Proposal 14.1** Introduce a legislative provision that permits broad consent for the purposes of research: (a) Broad consent should be available for all research to which the research exceptions in the Act (and proposed by this chapter) will also apply. (b) Broad consent would be given for 'research areas' where it is not practicable to fully identify the purposes of collection, use or disclosure of personal or sensitive information at the point when consent is being obtained. **Proposal 14.2** Consult further on broadening the scope of research permitted without consent for both agencies and organisations. **Proposal 14.3** Consult further on developing a single exception for research without consent and a single set of guidelines, including considering the most appropriate body to develop the guidelines.	• No comment.[88]

[87] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 15.
[88] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 16, 164-171.

15. Organisational Accountability **Proposal 15.1** An APP entity must determine and record the purposes for which it will collect, use and disclose personal information at or before the time of collection. If an APP entity wishes to use or disclose personal information for a secondary purpose, it must record that secondary purpose at or before the time of undertaking the secondary use or disclosure. **Proposal 15.2** Expressly require that APP entities appoint or designate a senior employee responsible for privacy within the entity. This may be an existing member of staff of the APP entity who also undertakes other duties.	• AFIA members have sought clarification with to Proposal 15.1. Specifically, AFIA members seek clarification regarding:[89] 1. Whether Proposal 15.1 records would belong to the individual subject and therefore be deemed 'personal information' **OR** 2. Be deemed an organisation record for compliance purposes. • AFIA members suggest the latter approach is preferable. • AFIA members seek clarification on Proposal 15.2's requirement for there to be a single senior employee responsible for privacy across an APP entity, especially given the difficulties of implementing end to end responsibility in some contexts.[90]
16. Children **Proposal 16.1** Define a child as an individual who has not reached 18 years of age. **Proposal 16.2** Existing OAIC guidance on children and young people and capacity15 should continue to be relied upon by APP entities. An entity must decide if an individual under the age of 18 has the capacity to consent on a case-by-case basis. If that is not practical, an entity may assume an individual over the age of 15 has capacity, unless there is something to suggest otherwise. The Act should codify the principle that valid consent must be given with capacity. Such a provision could state that 'the consent of an individual is only valid if it is reasonable to expect that an individual to whom the APP entity's activities are directed would understand the nature, purpose and	• No comment.[91]

[89] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 16, 175-6.
[90] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 16, 177.
[91] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 16, 179-192.

consequences of the collection, use or disclosure of the personal information to which they are consenting.' Exceptions should be provided for circumstances where parent or guardian involvement could be harmful to the child or otherwise contrary their interests (including, but not limited to confidential healthcare advice, domestic violence, mental health, drug and alcohol, homelessness or other child support and community services). Proposal 16.3 Amend the Privacy Act to require that collection notices and privacy policies be clear and understandable, in particular for any information addressed specifically to a child. In the context of online services, these requirements should be further specified in a Children's Online Privacy Code, which should provide guidance on the format, timing and readability of collection notices and privacy policies. Proposal 16.4 Require entities to have regard to the best interests of the child as part of considering whether a collection, use or disclosure is fair and reasonable in the circumstances. Proposal 16.5 Introduce a Children's Online Privacy Code that applies to online services that are 'likely to be accessed by children'. To the extent possible, the scope of an Australian children's online privacy code could align with the scope of the UK Age Appropriate Design Code, including its exemptions for certain entities including preventative or counselling services. The code developer should be required to consult broadly with children, parents, child development experts, child-welfare advocates and industry in developing the Code. The eSafety Commissioner should also be consulted. The substantive requirements of the Code could address how the best interests of child users should be supported in the design of an online service.	

17. People experiencing vulnerability **Proposal 17.1** Introduce, in OAIC guidance, a non-exhaustive list of factors that indicate when an individual may be experiencing vulnerability and at higher risk of harm from interferences with their personal information. **Proposal 17.2** OAIC guidance on capacity and consent should be updated to reflect developments in supported decision-making. **Proposal 17.3** Further consultation should be undertaken to clarify the issues and identify options to ensure that financial institutions can act appropriately in the interests of customers who may be experiencing financial abuse or may no longer have capacity to consent.	• AFIA supports Proposal 17.1's suggestion that OAIC should provide guidance on vulnerability, noting the definition of vulnerability must be consistent with definitions of this term in guidance already provided by other regulators such as ASIC.[92] • Any definitions of vulnerability should account for definitions of the term used in existing industry codes. • The Department should consider how Proposal 17.2, on updating guidance on consent, interacts with Proposal 11.1's suggestion that the definition of consent be amended so consent must be: **'voluntary, informed, current, specific, and unambiguous'.**[93] • AFIA supports Proposal 17.3's suggested specific consultation with financial institutions on vulnerability.[94]

[92] Sean Hughes (ASIC Commissioner), 'ASIC's expectations for protecting vulnerable customers' (26 November 2020).
[93] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 14, 127-130.
[94] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 17, 200-201.

18. Rights of the Individual **Access and Explanation** **Proposal 18.1** Provide individuals with a right to access, and an explanation about, their personal information if they request it, with the following features: (a) an APP entity must provide access to the personal information they hold about the individual (this reflects the existing right under the Act) (b) an APP entity must identify the source of the personal information it has collected indirectly, on request by the individual (c) an APP entity must provide an explanation or summary of what it has done with the personal information, on request by the individual (d) the entity may consult with the individual about the format for responding to a request, and the format should reflect the underlying purpose of ensuring the individual is informed, as far as is reasonable, about what is being done with their information (e) an organisation may charge a 'nominal fee' for providing access and explanation where the organisation has produced a product in response to an individual	• The breadth and application of 'rights of the individual' proposed in Chapter 18 is significant.[95] • The Review proposes five specific privacy rights: 1. A right of access and explanation of personal information.[96] 2. A right of objection to collection, use or disclosure of personal information.[97] 3. A right to the erasure of personal information.[98] 4. A right to the correction of personal information in 'generally available publications online' controlled by AFPs.[99] 5. A right to de-index certain personal information from online search results.[100] The Review also suggests three exceptions to all the individual privacy rights outlined above, these are outlined in Proposal 18.6 and include:[101] • Competing public interests which need to be weighed against the individual privacy rights, including 'freedom of expression' and 'law enforcement'.[102] • 'Relationships of a legal character' – including where complying with a request to enforce a privacy right would contradict another law or contract.[103]

[95] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 17, 203-27.
[96] Attorney-General's Department, *Privacy Act Review Report* (December 2022), Proposal 18.1, discussed at 17-18, 205, 209.
[97] Attorney-General's Department, *Privacy Act Review Report* (December 2022), Proposal 18.2, discussed at 18, 210-11.
[98] Attorney-General's Department, *Privacy Act Review Report* (December 2022), Proposal 18.3, discussed at 18, 211-14.
[99] Attorney-General's Department, *Privacy Act Review Report* (December 2022), Proposal 18.4, discussed at 18, 215.
[100] Attorney-General's Department, *Privacy Act Review Report* (December 2022), Proposal 18.5, discussed at 18, 216-18.
[101] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 18, 218-222.
[102] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 18, 219-220.
[103] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 220-21.

Objection **Proposal 18.2** Introduce a right to object to the collection, use or disclosure of personal information. An APP entity must provide a written response to an objection with reasons. **Erasure** **Proposal 18.3** Introduce a right to erasure with the following features: (a) An individual may seek to exercise the right to erasure for any of their personal information. (b) An APP entity who has collected the information from a third party or disclosed the information to a third party must inform the individual about the third party and notify the third party of the erasure request unless it is impossible or involves disproportionate effort. In addition to the general exceptions, certain limited information should be quarantined rather than erased on request, to ensure that the information remains available for the purposes of law enforcement. **Correction** **Proposal 18.4** Amend the Act to extend the right to correction to generally available publications online over which an APP entity maintains control. **De-indexing** **Proposal 18.5** Introduce a right to de-index online search results containing personal information which is: (a) sensitive information [e.g. medical history], or (b) information about a child, or (c) excessively detailed [e.g. home address and personal phone number], or	• 'Technical exceptions' – such as where comply with a request to enforce a privacy right would be 'technically impossible' or 'unreasonable and frivolous or vexatious'.[104] • AFIA seeks clarification on whether all individual rights in Chapter 18 would apply to all businesses, given Proposal 6.1's suggested removal of the small business exemption.[105] • AFIA members have also noted that in other jurisdictions, like California, the financial services sector is specifically excluded from similar individual privacy rights, owing to the inherently complex characteristics of the sector. Instead, financial services is dealt with via bespoke approaches. We advocate similar tailoring in Australia.[106] • AFIA members have noted such rights may specifically be hard to apply in a financial services context, given information is often commercially sensitive and can include valuable intellectual property. For example, explaining credit scoring output that is generated by a company's internal scorecard system may both publicise commercially sensitive information and expose a company's intellectual property to its competitors and the marketplace at-large. • To limit uncertainty, we seek express statutory limitation periods on all rights outlined in Chapter 18, so requests may only be made within three years, as is common in other legal contexts.[107] • AFIA emphasises that, if adopted, all these rights must be subject to the exceptions outlined in Proposal 18.6.[108]

[104] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 221
[105] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 12.
[106] Clarip, 'GLBA Exemption in California Consumer Privacy Act (CCPA)' (accessed on 21 March 2023). This partial exemption is connected to the *Gramm-Leach-Bliley Act 1999* (US) (GLBA).
[107] Commonwealth Parliamentary Library, '*Legal actions and limitation periods*' (accessed on 24 March 2023).
[108] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 18, 218-222.

(d) inaccurate, out-of-date, incomplete, irrelevant, or misleading. The search engine may refer a suitable request to the OAIC for a fee. The right should be jurisdictionally limited to Australia. **Exceptions** **Proposal 18.6** Introduce relevant exceptions to all rights of the individual based on the following categories: (a) Competing public interests: such as where complying with a request would be contrary to public interests, including freedom of expression and law enforcement activities. (b) Relationships with a legal character: such as where complying with the request would be inconsistent with another law or a contract with the individual. (c) Technical exceptions: such as where it would be technically impossible, or unreasonable, and frivolous or vexatious to comply with the request. **Response** **Proposal 18.7** Individuals should be notified at the point of collection about their rights and how to obtain further information on the rights, including how to exercise them. Privacy policies should set out the APP entity's procedures for responding to the rights of the individual. **Proposal 18.8** An APP entity must provide reasonable assistance to individuals to assist in the exercise of their rights under the Act. **Proposal 18.9** An APP entity must take reasonable steps to respond to an exercise of a right of an individual. Refusal of a request should be accompanied by an explanation for the refusal and information on how an individual may lodge a complaint regarding the refusal with the OAIC.	• These exceptions must be worded so where is a conflict between the right asserted and an equally compelling exception, the exception should prevail. • AFIA seeks further clarity on the direct relationship between the rights outlined in these proposals and the 'direct right of action' for alleged 'interferences with privacy' under Proposal 26. • AFIA members specifically note Proposals 18.1(b) and 18.1(c). These are access right obligations that will significantly increase the level of resourcing, storage and technology investment requirement to respond to access requests. These new obligations first require APP entities to **identify the source** of personal information, then to **explain** what the APP entity has done with the information.[109] • Identifying the source of data will require data holders to collect and retain more information than it would otherwise (namely, source information). Collecting, coding and storing this information in existing systems will be a significant cost. • A data holder is already required to provide a Notice at the point of data collection explaining how the data holder will process information. This introduces a duplicative obligation to provide a further explanation, after the fact of processing. There is no equivalent requirement in EU or California, where a data holder is only required to provide the raw information. • Further information is required on how such an explanation should be provided or whether capabilities exist to support such explanations. • On Proposal 18.1(e), we support the concept that, if a right of 'access and explanation' is to be instituted, APP entities

[109] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 17-18.

Proposal 18.10 An organisation must acknowledge receipt of a request to exercise a right of an individual within a reasonable time and provide a timeframe for responding. An agency and organisation must respond to a request to exercise a right within a reasonable timeframe. In the case of an agency, the default position should be that a reasonable timeframe is within 30 days, unless a longer period can be justified.	must be able to charge a 'nominal fee' for responding to requests.[110] This is appropriate, to allow for the resources which will be needed and disincentivise vexatious or excessive requests. • On Proposal 18.2, regarding individuals' right to object to APPs collecting, using or disclosing personal information', We suggest that if 'written reasons' must be provided, then templates should be formulated to assist APP entities in doing this.[111] Furthermore, APPs must be given a significant period of time to provide any such reasons. The *Freedom of Information Act 1982* (Cth) ('the FOI Act') allows 30 days to respond to a request. • However, the *FOI Act* relates to Government agencies with significant resources. If Proposal 18.2 is to be adopted, APP entities should be given 60 days to respond to requests, to allow appropriate formulation of responses and allocation of resources. This is especially so if Proposal 6.1's suggested removal of the small business exemption, meaning these rights would apply even to businesses with limited resources.[112] • On Proposal 18.3's suggested right of erasure, and the requirements for APP's to engage with third party entities, except where doing so would require **'disproportionate effort'**.[113] We seek guidance on what would constitute 'disproportionate effort' in this context.[114] We recommend further consultation on this concept. AFIA members have suggested the term 'unreasonable efforts' may be more appropriate in the Australian context, given substantial

[110] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 18, 209-10.
[111] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 18, 211.
[112] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 12.
[113] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 18 and 214.
[114] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 18 and 214.

	prior judicial consideration of the meaning of the term 'reasonableness'. • AFIA members have noted that the right to erasure would need to be workable in practice. For example, it would need to have appropriate carve-outs for system backups. • AFIA members have noted that the right to erasure should be able to be refused in certain limited circumstances, in accordance with Proposal 18.6's exceptions that recognise the need to balance competing legal obligations.[115] For example, credit providers should be able to legitimate refuse requests for the erasure of data where they have applied for credit and want this data removed from the credit providers' or credit bureaus records, to ensure the credit reporting requirements are not undermined. • On Proposal 18.4's right to 'correction' of publications and APP entity 'controls', given the capacity for digital communications to be downloaded and shared prior to such correction, it will be important to specifically define in detail what constitutes 'control' over a publication at any specific point in time.[116] • On Proposal 18.5's suggested right to de-index online search results, We seek further consultation regarding 18.5(c) and 18.5(d), which respectively suggest de-indexation rights regarding information which is respectively 'excessively detailed' **OR** 'inaccurate, out-of-date, incomplete, irrelevant, or misleading'.[117] AFIA members are also uncertain how, if at all, Proposal 18.5 would be intended to apply to financial institutions. • On Proposal 18.7's suggestion that APP entities must 'notify' individuals about their rights 'at the point of

[115] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 18, 218-222.
[116] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 215.
[117] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 218.

	collection', we seek further information on how this interacts with the new definition of 'collection' under Proposal 4.3.[118] Specifically, how would the requirement to 'notify' individuals of their rights apply to information which is either 'inferred' or 'generated'.[119] • On Proposal 18.8's suggestions that APP entities must provide 'reasonable assistance' to individuals seeking to exercise rights proposed in Chapter 18, further guidance will be required on what must be done to meet this test if these rights are adopted.[120] AFIA members have queried if Proposal 18.8 adds anything substantively to the other obligations put forward, given companies have an obligation to comply with the law in any case. Therefore, the term 'reasonable assistance' may not provide much in the way of additional meaning in practice. • AFIA recommends the acknowledgement, response and written reasons requirements of Proposals 18.9 to 18.10 should be subject to a timeframe of 60 days, not 30 days as under the *FOI Act*, noting that it is proposed these rights apply to small businesses under Proposal 6.1, which have substantially fewer resources than the Government agencies under the *FOI Act*.[121] • AFIA members have sought clarification of Proposal 18.1's interaction with Proposal 4.9. Specifically, the regulations should specify the type of detail entities must explain when obtaining consent to collect inferred information (especially inferred information used for fraud or credit risk assessment purposes). Clarification is required to obtain generic consent for this type of collection. Providing further details risks revealing commercially

[118] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 10, 38.
[119] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 10, 38.
[120] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 18 and 223.
[121] Attorney-General's Department, *Privacy Act Review Report* (December 2022), regarding Proposals 18.9-10 see 226-7 and regarding Proposal 6.1 see 12 and 72-8.

	sensitive information. In this context, it is important also to clarify if the exemption for 'commercially sensitive decision making processes' applies to fraud prevention tools.[122]
19. Automated decision making **Proposal 19.1** Privacy policies should set out the types of personal information that will be used in substantially automated decisions which have a legal or similarly significant effect on an individual's rights. **Proposal 19.2** High-level indicators of the types of decisions with a legal or similarly significant effect on an individual's rights should be included in the Act. This should be supplemented by OAIC Guidance. **Proposal 19.3** Introduce a right for individuals to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made. Entities will be required to include information in privacy policies about the use of personal information to make substantially automated decisions with legal or similarly significant effect. This proposal should be implemented as part of the broader work to regulate AI and ADM, including the consultation being undertaken by the Department of Industry, Science and Resources.	• On Proposal 19.1, related to automated decision making, we seek further consultation on the definition of the phrase 'legal or similarly significant effect on an individual's rights', given this phrase is very broad and open to a myriad of reasonable interpretations depending on the context.[123] • In considering Proposal 19.1, the Department should consider carving out disclosures of processes which relate to commercially sensitive information or intellectual property. • AFIA supports Proposal 19.2's suggestion that indicators of what constitutes a 'legal or similarly significant effect' should be included in both the Act and OAIC guidance.[124] • Proposal 19.3's suggested right for customers to 'request meaningful information' about how automated decisions are made should be limited where providing such information may disclose proprietary or commercial sensitive information.[125] • Any such right should be limited and subject to exceptions, as we have advocated in our response to Chapter 18's proposed individual rights. We specifically note Proposal 18.6's recognitions related to: competing public interests, relationships of a legal character and

[122] Attorney-General's Department, *Privacy Act Review Report* (December 2022), at 209 regarding the exemption for commercially-sensitive decision making processes.
[123] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 19, 232.
[124] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 19, 232.
[125] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 19, 233-4.

	technical exceptions.[126] Similar exceptions must be included if Proposal 19.3 is adopted. • While supporting the need to provide more information to customers on automated decisions that have a significant effect, there is ambiguity in the concept of 'meaningful'. It is unclear what level of detail would be required to be provided to individuals under Proposal 19.3. • Decision logic and algorithms are often commercially sensitive. Data holders should not have to detail the weighting of individual elements or components. Consideration should be given to whether it is sufficient for providers to identify the types of data relevant to the decision.
20. Direct marketing, targeting and trading Proposal 20.1 Amend the Act to introduce definitions for: (a) Direct marketing – capture the collection, use or disclosure of personal information to communicate directly with an individual to promote advertising or marketing material. (b) Targeting – capture the collection, use or disclosure of information which relates to an individual including personal information, deidentified information, and unidentified information (internet history/tracking etc.) for tailoring services, content, information, advertisements or offers provided to or withheld from an individual (either on their own, or as a member of some group or class).	• Suggested changes related to direct marketing should consider and not unnecessarily duplicate protections which already exist under the *Australian Competition and Consumer Act 2010* (Cth) ('the ACL') regarding direct sales practices. • Suggested changes on direct marking should also consider the Australian Direct Marketing Association (ADMA)'s *Direct Marking Code of Practice*.[127] Members have also suggested consideration be given to allowing customers to opt out of contact from individual organisations rather than more general opt out provisions. • AFIA members note changes in Proposal 20.1 on direct market, targeting and trading may hamper emerging technologies capacity to make customers aware of services or products they may wish to access.[128]

[126] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 18, 218-222.
[127] ACCC, *Australian Direct Marketing Association (ADMA) - Revocation and substitution - A90876* (29 June 2023).
[128] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 256-8.

(c) Trading – capture the disclosure of personal information for a benefit, service or advantage. Proposal 20.2 Provide individuals with an unqualified right to opt-out of their personal information being used or disclosed for direct marketing purposes. Similar to the existing requirements under the Act, entities would still be able to collect personal information for direct marketing without consent, provided it is not sensitive information and the individual has the ability to opt out. Proposal 20.3 Provide individuals with an unqualified right to opt-out of receiving targeted advertising. Proposal 20.4 Introduce a requirement that an individual's consent must be obtained to trade their personal information. Proposal 20.5 Prohibit direct marketing to a child unless the personal information used for direct marketing was collected directly from the child and the direct marketing is in the child's best interests. Proposal 20.6 Prohibit targeting to a child, with an exception for targeting that is in the child's best interests. Proposal 20.7 Prohibit trading in the personal information of children. Proposal 20.8 Amend the Act to introduce the following requirements: (a) Targeting individuals should be fair and reasonable in the circumstances. (b) Targeting individuals based on sensitive information (which should not extend to targeting based on political opinions, membership of a political	• AFIA supports the limitation in Proposal 20.2 that information can still be collected for 'direct marketing', so long as the individual has the right to 'opt out'.[129] • AFIA members have sought clarification of how these rules on direct marketing and targeted advertising would apply in the context of providing information which is education, rather than pure marketing material, such as advising a customer they may be eligible for financial hardship assistance, or information on interest rates which is provided to brokers but not customers directly as advertising. • On Proposal 20.4, we seeks further information on the definition of 'trading in personal information' and specifically how it may interact with Proposal 20.1(c).[130] We seek specific examples of how these proposals may apply in a financial services context. • AFIA members have suggested Proposal 20.4 is arguably out-of-step with comparable jurisdictions and could have unintended consequences. There are many instances where businesses exchange data relating to mutual customers for beneficial efficiency reasons. Some of this 'trading' will be a core part of the service provided to customers, particularly where the service is a joint offering – Apple Pay, Co-Brand partners, Insurance Benefits on Cards. • AFIA members have specifically suggested the definition of 'trading in personal information' under Proposal 20.4 should specifically exclude activity that may be inadvertently captured currently, such as that related to restructuring or mergers and acquisitions.

[129] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 258.
[130] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 261.

association or membership of a trade union), should be prohibited, with an exception for socially beneficial content. Proposal 20.9 Require entities to provide information about targeting, including clear information about the use of algorithms and profiling to recommend content to individuals. Consideration should be given to how this proposal could be streamlined alongside the consultation being undertaken by the Department of Industry, Science and Resources.	• The main example provided in the Review related to Proposal 20.4 is selling customer lists and contact details, which is an outlier case. The example provided of exchanging a customer list, would be caught under direct marketing and targeting, without the need for Proposal 20.4 – given direct marketing and targeting is the ultimate purpose of the activity. • Therefore, the Government should consider if Proposal 20.4 may duplicate other aspects of the review covered in Chapter 20 and avoid duplication where possible. • AFIA members have further suggested Proposal 20.4 is somewhat at odds with CDR, and Digital Economy objectives which support the flow of data between organizations. • While operationally, direct marketing and targeting can be managed through channels and cookies – it is unclear how to implement a restriction on trading and to operationalize an opt-out. Further consultation on this point is required. • On Proposal 20.8's suggestion that 'targeted' marketing should be 'fair and reasonable in the circumstances', we recommend that if this is adopted the standard should be an objective, not a subjective one, to promote consistency with Proposal 12.1's suggested general requirement under the Act to 'collect use and disclose' information in a way which is 'fair and reasonable in the circumstances'.[131] • Proposal 20.9's suggestion that internal methods of targeted marketing and algorithm's should be disclosed may be complex. Further consultation is required on this topic to ensure that it does not compel provision of information which may be proprietary or commercial in confidence.[132] If Proposal 20.9 is adopted, AFIA member

[131] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 143-4 and 268.
[132] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 267-8.

	request detailed and specific guidance on what information should be provided. • AFIA members have noted customers increasingly expect personalisation for their service providers. They want content tailored to their needs, preferences and interests. This can be done through channels which are safe and secure. • To the extent personalisation is a part of the core value proposition provided to customers, through things like curated offers and promotions, operationalising the principle of opting out becomes complex. **The Relationship Between Direct Marketing, Targeting & Trading** • AFIA members suggest the below on the relationship between direct marketing, targeting and trading. • There is significant crossover between the concepts of direct marketing, targeting and trading. • Further, there are practical challenges when it comes to operationalizing such opt-outs given this cross-over. For example - if a customer opts-out of targeting but not marketing, could they still be sent a personalised email ad? • It's unclear how companies are expected to operationalize these requirements and subtle distinctions. A cookie opt-out covers part – but not all of targeting. There is nothing in the consultation that speaks to what technology capabilities or solutions are available to operationalize these opt-outs, or their costs. • The definition of targeting is quite broad. Online advertising that uses large segments to arbitrate between offers, does not pose any material risk to consumers. • Consideration should be given to a threshold requirement, for example where there is a risk of serious harm or material privacy risk.

21. Security, retention and destruction **Proposal 21.1** Amend APP 11.1 to state that 'reasonable steps' include technical and organisational measures. **Proposal 21.2** Include a set of baseline privacy outcomes under APP 11 and consult further with industry and government to determine these outcomes, informed by the development of the Government's 2023-2030 Australian Cyber Security Strategy. **Proposal 21.3** Enhance the OAIC guidance in relation to APP 11 on what reasonable steps are to secure personal information. The guidance that relates to cyber security could draw on technical advice from the Australian Cyber Security Centre. **Proposal 21.4** Amend APP 11.1 so that APP entities must also take reasonable steps to protect de-identified information. **Proposal 21.5** The OAIC guidance in relation to APP 11.2 should be enhanced to provide detailed guidance that more clearly articulates what reasonable steps may be undertaken to destroy or de-identify personal information. **Proposal 21.6** The Commonwealth should undertake a review of all legal provisions that require retention of personal information to determine if the provisions appropriately balance their intended policy objectives with the privacy and cyber security risks of entities holding significant volumes of personal information. This further work could also be considered by the proposed Commonwealth, state and territory working group at Proposal 29.3 as a key issue of concern where alignment would be beneficial.	• AFIA members seek further clarification on the definition of the term 'reasonable steps' in the context of the review's proposals related to the security, retention and destruction of personal information, particularly insofar as they relate to proposals 21.1, 21.3 and 21.4.[133] Clarification on the definition of 'reasonable steps' will likely be provided by the OAIC guidance and Commonwealth legal review in proposals 21.5 and 21.6.[134] • AFIA asks that processes to provide feedback to that OAIC guidance and Commonwealth legal review be publicly announced well ahead of time, to allow for stakeholder feedback. • AFIA support Proposal 21.6 and consider that this review should focus on the legal obligations regarding the retention of personal information in the financial services industry, where obligations are complex and overlapping, noting the large volumes of information which are currently required to be held.[135] • AFIA has concerns regarding proposals which related record retention, such as proposals 21.7 and 21.8, which relate to APP entities establishing and specifying their own 'maximum and minimum periods of retention in relation to personal information.'[136] • AFIA members seek further guidance as to what, if any, mandatory regulatory requirements will flow from these proposals, given they seem to focus on APP entity level policies. • If APP 1.4 and APP 11 are amended, per proposals 21.7 and 21.8, the Department should provide draft amendments

[133] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 20, 268-72.
[134] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 273.
[135] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 21.
[136] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 21 and 276.

However, this review should not duplicate the recent independent review of the mandatory data retention regime under the Telecommunications (Interception and Access) Act 1979 and the independent reviews and holistic reform of electronic surveillance legislative powers. Proposal 21.7 Amend APP 11 to require APP entities to establish their own maximum and minimum retention periods in relation to the personal information they hold which take into account the type, sensitivity and purpose of that information, as well as the entity's organisational needs and any obligations they may have under other legal frameworks. APP 11 should specify that retention periods should be periodically reviewed. Entities would still need to destroy or de-identify information that they no longer need. Proposal 21.8 Amend APP 1.4 to stipulate than an APP entity's privacy policy must specify its personal information retention periods.	for industry and stakeholder feedback.[137] AFIA members seek detailed guidance if this proposal is adopted. • On Proposal 21.8's suggestions an APP entity's privacy policy must 'specify its personal information retention periods', We seek clarification as to whether this would require specification of generic retention periods or maximum retention periods.[138] • AFIA requests guidance on what the treatment should be if these periods change.

[137] Attorney-General's Department, *Privacy Act Review Report* (December 2022), on APP 1.4, see 21 and 277. On APP 11, see 21 and 275-6.
[138] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 277.

22. Controllers and processors of personal information **Proposal 22.1** Introduce the concepts of APP entity controllers and APP entity processors into the Act. Pending removal of the small business exemption, a non-APP entity that processes information on behalf of an APP entity controller would be brought into the scope of the Act in relation to its handling of personal information for the APP entity controller. This would be subject to further consultation with small business and an impact analysis to understand the impact on small business processors.	• On Proposal 22.1, we seek further clarification on the differences between the proposed obligations that would apply to the defined terms 'APP entity controllers' and 'APP entity processors'.[139] • AFIA suggests this recommendation adds significant complexity to the Act. We further notes many of the objectives of Proposal 22.1 are already largely accomplished via Proposal 6.1, the removal of the small business exemption. Therefore, pursuing both changes may be unnecessary.[140] • AFIA notes the Review indicates Proposal 22.1 is intended to align with the *Californian Consumer Privacy Act* ('CCPA'), where a **controller** is any for profit legal entity which 'determines the purposes and means of processing the personal information', whereas as **processors** is a 'service provider' which receives personal information **from a controller** and 'processes' the personal information under a 'service contract'.[141] • AFIA notes that the variant obligations which apply to **processors and controllers** are outlined on pages 281-282 of the review. • However, as we have indicated with respect to Proposals in Chapter 18 and Proposal 26, the financial services sector is exempted from the Californian legislation on which Proposal 22.1 is modelled, as it is covered by separate bespoke legislation, formulated to recognise the unique characteristics of the financial services sector.[142] • AFIA recommends a similar bespoke approach should be considered in the Australian context.

[139] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 280-2.
[140] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 12, 72-8.
[141] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 281.
[142] Clarip, 'GLBA Exemption in California Consumer Privacy Act (CCPA)' (accessed on 21 March 2023). This partial exemption is connected to the *Gramm-Leach-Bliley Act 1999* (US) (GLBA).

	• If Proposal 22.1 is adopted, we seek guidance on how this would align with approaches to this issue under the GDPR, given companies operate across multiple jurisdictions.
23. Overseas data flows **Proposal 23.1** Consult on an additional requirement in subsection 5B(3) to demonstrate an 'Australian link' that is focused on personal information being connected with Australia. **Proposal 23.2** Introduce a mechanism to prescribe countries and certification schemes as providing substantially similar protection under APP 8.2(a). **Proposal 23.3** Standard contractual clauses for use when transferring personal information overseas should be made available to APP entities. **Proposal 23.4** Strengthen the informed consent exception to APP 8.1 by requiring entities to consider the risks of an overseas disclosure and to inform individuals that privacy protections may not apply to their information if they consent to the disclosure. **Proposal 23.5** Strengthen APP 5 in relation to overseas disclosures by requiring APP entities, when specifying the countries in which recipients are likely to be located if practicable, to also specify the types of personal information that may be disclosed to recipients located overseas. **Proposal 23.6** Introduce a definition of 'disclosure' that is consistent with the current definition in APP Guidelines. Further consideration should be given to whether online publications of personal information should be excluded from the requirements of APP 8 where it is in the public interest.	• On Proposal 23.1, it is unclear what constitutes an 'Australian link', further guidance and examples would be useful, especially as applied to financial services.[143] • On Proposal 23.2, AFIA members seek clarity on who would be authorised to provide such certifications and who could rely on them for what purposes.[144] OAIC or the Attorney-General's Department may be best placed to provide guidance and certification. • On Proposal 23.3, AFIA members support provision of standardised contractual clauses to facilitate overseas data flows.[145] These should be non-mandatory, given the need for flexibility in individual business scenarios. • AFIA members seek greater clarity on how Proposal 23.4's suggested 'strengthened informed consent' exception under APP 8.1 will be affected by Proposal 11.1's amended definition of consent to meet to the GDPR standard.[146] • AFIA Members suggest Australia should recognize the concept of Binding Corporate Rules (BCRs). To the extent BCRs have been approved by a relevant data authority in Europe – and where Europe is deemed to be a jurisdiction with 'substantially similar protections' – transferring data between companies that are signatories to those BCRs should be acceptable. Currently, it is unclear if BCRs would be deemed a certification scheme or not.[147]

[143] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 286.
[144] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 288.
[145] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 289.
[146] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 14, 127-130.
[147] European Commission, '*What are Binding Corporate Rules*' (25 May 2018).

24. CBPR and domestic certification Nil proposals.	• AFIA has no comments on CBPR and domestic certification, given no proposals have been made.[148]
25. Enforcement **Proposal 25.1** Create tiers of civil penalty provisions to allow for better targeted regulatory responses: (a) Introduce a new mid-tier civil penalty provision to cover interferences with privacy without a 'serious' element, excluding the new low-level civil penalty provision. (b) Introduce a new low-level civil penalty provision for specific administrative breaches of the Act and APPs with attached infringement notice powers for the Information Commissioner with set penalties. **Proposal 25.2** Amend section 13G of the Act to remove the word 'repeated' and clarify that a 'serious' interference with privacy may include: (a) those involving 'sensitive information' or other information of a sensitive nature (b) those adversely affecting large groups of individuals (c) those impacting people experiencing vulnerability (d) repeated breaches (e) wilful misconduct, and (f) serious failures to take proper steps to protect personal data. The OAIC should provide specific further guidance on the factors that they take into account when determining whether to take action under section 13G.	• AFIA supports Proposal 25.1's suggested 'tiered' approach to civil penalties, to ensure that enforcement is proportionate to the type of conduct in question.[149] However, we note a tiered approach is inconsistent with the uncapped damages in Proposal 26's suggested 'direct right of action'.[150] We note others have suggested penalties should take into account the size of the business committing the contravention.[151] • AFIA has reservations about Proposal 25.2(b)'s suggestion that 'serious' interference with privacy could include an interference which 'adversely impacts' a 'large group'.[152] It is unclear what minimum harm threshold must be met to constitute an 'adverse impact' or what number of people is sufficient to constitute a 'large group'. Any amendment to section 13G of the Act should be subject to further consultation with industry on draft legislation.[153] • AFIA notes Proposal 25.4's suggested power for the Information Commission to undertake public inquiries and reviews on specified matters related to enforcement. This may be raise concerns of prejudicing future legal proceedings in the court system.[154] • AFIA notes Proposal 25.5's suggestion amendments to ss 52(1)(b)(ii) and 52(1A)(c) so they would include **not only** actions to 'mitigate' or 'redress' any **'actual' loss or**

[148] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 298-300.
[149] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 22-3 and 304-305.
[150] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 330.
[151] Anna Johnston and Alex Kotova, *Submission to the Attorney-General Department's Consultation on the Review of the Privacy Act: Final Report* (31 March 2023), 11.
[152] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 22, 308.
[153] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 22, 308.
[154] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 22, 311-12.

Proposal 25.3 Amend the Act to apply the powers in Part 3 of the Regulatory Powers (Standard Provisions) Act 2014 to investigations of civil penalty provisions in addition to the Information Commissioner's current investigation powers. Proposal 25.4 Amend the Act to provide the Information Commissioner with the power to undertake public inquiries and reviews into specified matters on the approval or direction of the Attorney-General. Proposal 25.5 Amend subparagraph 52(1)(b)(ii) and paragraph 52(1A)(c) to require an APP entity to identify, mitigate and redress actual or reasonably foreseeable loss. The current provision could be amended to insert the underlined: a declaration that the respondent must perform any reasonable act or course of conduct to identify, mitigate and redress any actual or reasonably foreseeable loss or damage suffered by the complainant/those individuals. OAIC should publish guidance on how entities could achieve this. Proposal 25.6 Give the Federal Court and the Federal Circuit and Family Court of Australia the power to make any order it sees fit after a civil penalty provision relating to an interference with privacy has been established. Proposal 25.7 Further work should be done to investigate the effectiveness of an industry funding model for the OAIC.	**damage** suffered by individuals due to a breach of those sections (the current test). The Review proposes also allowing compensation for any 'reasonably foreseeable' loss or damage flowing from a breach.[155] This change may significantly increase potential liabilities for APP entities. • Proposal 25.6's suggests the courts mentioned therein should have the capacity to make 'any order [they] see fit' after a civil penalty provision has been breached.[156] This unlimited penalty provision goes against the principle of tiering expressed in Proposal 25.1 and may create uncertainty for businesses seeking to comply in good faith with the provisions.[157] • On Proposals 25.7 and 25.8 related to establishing industry and contingency funding models for OAIC to enforce the above, we would refer the Department to our work on industry funding models in the ASIC context.[158] • If such models are pursued, it is crucial to ensure that subsectors regulated by such a model only bear the relative costs of the amount of enforcement for which they are directly responsible.[159] It is also important that, as much as possible, such a scheme not disproportionately see good actors subsiding enforcement activities against those who are not meeting their obligations.[160]

[155] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 22, 314-15.
[156] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 316.
[157] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 22-3 and 304-305.
[158] AFIA Submission, '*ASIC Industry Funding Model*' (28 October 2022).
[159] AFIA Submission, '*ASIC Industry Funding Model*' (28 October 2022), 4-5.
[160] AFIA Submission, '*ASIC Industry Funding Model*' (28 October 2022), 4-5.

Proposal 25.8 Further consideration should be given to establishing a contingency litigation fund to fund any costs orders against the OAIC, and an enforcement special account to fund high cost litigation. Proposal 25.9 Amend the annual reporting requirements in OAIC Act to increase transparency about the outcome of all complaints lodged including numbers dismissed under each ground of section 41. Proposal 25.10 The OAIC should conduct a strategic internal organisational review with the objective of ensuring the OAIC is structured to have a greater enforcement focus. Proposal 25.11 Amend subsection 41(dc) of the Act so that the Information Commissioner has the discretion not to investigate complaints where a complaint has already been adequately dealt with by an EDR scheme.	

26. A direct right of action **Proposal 26.1** Amend the Act to allow for a direct right of action in order to permit individuals to apply to the courts for relief in relation to an interference with privacy. The model should incorporate the appropriate design elements discussed in the review.[161]	• AFIA notes complexities with the direct right of action in Proposal 26.[162] • It allows a claim to be brought by any individual or representative class who have suffered an 'interference with their privacy', this could incentivise third-party litigation funders to seek to profit from such claims.[163] • AFIA notes the proposed direct right of action does not have a minimum harm threshold.[164] According to the Review it is open to any person or group who suffers 'any loss or damage' due to an 'interference with their privacy'.[165] This includes 'any loss or damage' to 'the person's feelings or humiliation'.[166] • AFIA members suggest, if adopted, this right should be actionable only in cases of 'serious harm', covering conventional recognised existing legal categories of harm like -- demonstrated financial loss, or reasonable damages for distress or inconvenience. • There is no limitation on the damages or remedies under Proposal 26. The Federal Court may could award any order the court sees fit, including 'any amount of damages'.[167] • By comparison, the maximum award ever made by the New Zealand Human Rights Review Tribunal, under the *Privacy Act 2020* (NZ), was $168,000. Normal awards for less serious cases have been under $10,000.[168] • AFIA notes, under the proposed model, the right would be enforceable in the Federal Court of Australia, **only after** a

[161] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 324-328.
[162] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 324.
[163] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 326.
[164] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 330.
[165] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 330.
[166] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 330.
[167] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 333.
[168] Privacy Commission (NZ), 'What are the consequences if I breach the Privacy Act?' (accessed on 21 March 2023).

	complaint had been made to OAIC or the Federal Privacy Commission **and** that complaint assessed for conciliation or a recognised industry External Dispute Resolution (EDR) scheme.[169] • AFIA notes that under Proposal 26.1(d), conciliation by the Australian Financial Complaints Authority (AFCA), could be used instead of conciliation with OAIC, as a condition precedent to exercising the direct right of action in the Federal Court of Australia. • AFIA members have noted the broad powers of AFCA, both in relation to Proposal 26 and generally, to make orders with respect to **all provisions and obligations of the *Privacy Act***.[170] • AFIA members have noted that under Proposal 26.1(d), and the *Privacy Act* generally as it may be amended following the Review, AFCA can award compensation of up to $500,000 without the need for an additional court hearing.[171] • Furthermore, AFIA members note that even in cases where the complainant is unsuccessful, meaning the credit provider is vindicated, credit providers can still be forced to pay over $8,000 in fees.[172] • If Proposal 26 is adopted, for the reasons outlined above, AFIA members would support conciliation by OAIC rather than AFCA as a condition precedent to the bringing of an action in the Federal Court of Australia.[173] • However, we note financial services are partially exempted from a similar right of action in jurisdictions in the USA, such as the *California Consumer Privacy Act*

[169] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 324.
[170] AFCA Approved Rules (13 January 2021), 26 at B.2(i).
[171] AFCA Approved Rules (13 January 2021), 40.
[172] AFCA, *Fee Structure: FY 24 Fee Schedule* (March 2023).
[173] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 328.

	(CCPA) *and the California Privacy Rights Act* (CPRA).[174] A similar exemption should be applied to financial services in Australia, given the unique considerations involved with the sector.
27. Statutory Tort Proposal 27.1 Introduce a statutory tort for serious invasions of privacy in the form recommended by the ALRC in Report 123. Consult with the states and territories on implementation to ensure a consistent national approach.	• AFIA notes the model suggested in Proposal 27 is outlined on pages 338 to 339 of the review. • AFIA notes Proposal 27 has similar complexities to Proposal 26. • For example, the Review states Proposal 27 would not be limited to conduct which is related to 'personal information', unlike other suggested protections proposed by the Review.[175] • The Review also notes that under Proposal 27 'the invasion [of privacy] need not cause actual damage, and damages for emotional distress may be awarded'.[176] • If such a tort is adopted, as with our suggestions in respect to Proposal 26, consideration should be given to excluding the financial services sector and providing bespoke legislation which accounts for our unique characteristics.[177] • AFIA supports the Review's recommendation that further consultation being undertaken before any statutory tort is adopted. We suggests further specific consultations undertaken with the financial services sector.

[174] Clarip, 'GLBA Exemption in California Consumer Privacy Act (CCPA)' (accessed on 21 March 2023). This partial exemption is connected to the *Gramm-Leach-Bliley Act 1999* (US) (GLBA).
[175] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 342.
[176] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 338.
[177] Clarip, 'GLBA Exemption in California Consumer Privacy Act (CCPA)' (accessed on 21 March 2023). This partial exemption is connected to the *Gramm-Leach-Bliley Act 1999* (US) (GLBA).

28. Notifiable data breaches scheme – impact and effectiveness **Proposal 28.1** Undertake further work to better facilitate the reporting processes for notifiable data breaches to assist both the OAIC and entities with multiple reporting obligations. **Proposal 28.2** (a) Amend paragraph 26WK(2)(b) to provide that if an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of the entity, the entity must give a copy of the statement to the Commissioner as soon as practicable and not later than 72 hours after the entity becomes so aware, with an allowance for further information to be provided to the OAIC if it is not available within the 72 hours. (b) Amend subsection 26WL(3) to provide that if an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach of an entity the entity must notify the individuals to whom the information relates as soon as practicable and where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases as soon as practicable. (c) Require entities to take reasonable steps to implement practices, procedures and systems to enable it to respond to a data breach. **Proposal 28.3** Amend subsections 26WK(3) and 26WR(4) to the effect that a statement about an eligible data breach must set out the steps the entity has taken or intends to take in response to the breach, including, where appropriate, steps to reduce any adverse impacts on the individuals to whom the relevant information relates.	• AFIA supports Proposal 28.1's streamlining of reporting processes for Notifiable Data Breaches (NDBs).[178] • AFIA seeks further information on what would constitute 'reasonable grounds' and the definition of the term 'eligible data breach' under Proposal 28.2(a).[179] • AFIA seeks further information on how the time period of 72 hours was chosen as the appropriate timeframe and whether there may be more appropriate timeframes applicable to financial services in certain cases.[180] • AFIA seeks consultation on Proposal 28.2(c)'s suggestion that entities should be required to 'take reasonable steps to implement practices, procedures and systems' to enable responses to data breaches.[181] We would welcome further guidance on what would be required to meet this threshold. • On Proposal 28.4, we would suggest that the circumstances under which the Attorney-General could permit information sharing with respect to personal information in the event of a NDB should be limited and clearly defined.[182]

[178] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 338.
[179] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 351-2.
[180] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 352.
[181] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 352.
[182] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 356.

However, this proposal would not require the entity to reveal personal information, or where the harm in providing this information would outweigh the benefit in providing this information. Consider further a requirement that entities should take reasonable steps to prevent or reduce the harm that is likely to arise for individuals as a result of a data breach. **Proposal 28.4** Introduce a provision in the Privacy Act to enable the Attorney-General to permit the sharing of information with appropriate entities to reduce the risk of harm in the event of an eligible data breach. The provision would contain safeguards to ensure that only limited information could be made available for designated purposes, and for a time limited duration.	
29. Interactions with other schemes **Proposal 29.1** The Attorney-General's Department develop a privacy law design guide to support Commonwealth agencies when developing new schemes with privacy-related obligations. **Proposal 29.2** Encourage regulators to continue to foster regulatory cooperation in enforcing matters involving mishandling of personal information. **Proposal 29.3** Establish a Commonwealth, state and territory working group to harmonise privacy laws, focusing on key issues.	• AFIA supports Proposals 29.1 to 29.3, including:[183] 1. The Department creating a 'privacy law design guide' for Commonwealth agencies; 2. Regulators continuing to foster co-operation in these matters 3. Creation of a unified Commonwealth, state and territory working group, tasked with harmonising privacy laws and focusing on key privacy issues. • AFIA strongly urges that the principles guiding Proposals 29.1 to 29.3 should accord with our other suggestions in this submission. • Any co-ordinated action must adopt approaches rendering the law simple and easy to understand, so regulated entities obligations are clear and compliance is facilitated.[184]

[183] Attorney-General's Department, *Privacy Act Review Report* (December 2022), 357-62.
[184] AFIA, 'Submission to Treasury's Consultation on Improving Corporations and Financial Services Law' (20 September 2022), citing the Explanatory Memorandum of the Treasury Laws Amendment (Measures for Consultation) Bill 2022 at 5[1.4].

30. Further review Proposal 30.1 Conduct a statutory review of any amendments to the Act which implement the proposals in this Report within three years of the date of commencement of those amendments.	• AFIA supports Proposal 30's suggested statutory review of any amendments to the Act which implement this review, to occur three years from the commencement of the amendments. We would urge any such review should remain cognisant of the principles and recommendations we have put forth in this submission.