FINANCIAL SERVICES COUNCIL

Privacy Act Review Report

FSC Submission

31 March 2023

Contents

1. About the Financial Services Council

The FSC is a peak body which sets mandatory Standards and develops policy for more than 100 member companies in one of Australia's largest industry sectors, financial services.

Our Full Members represent Australia's retail and wholesale funds management businesses, superannuation funds, life insurers and financial advice licensees. Our Supporting Members represent the professional services firms such as ICT, consulting, accounting, legal, recruitment, actuarial and research houses.

The financial services industry is responsible for investing more than $3 trillion on behalf of over 15.6 million Australians. The pool of funds under management is larger than Australia's GDP and the capitalisation of the Australian Securities Exchange, and is one of the largest pools of managed funds in the world.

2. Introduction and Executive Summary

2.1. Introduction

The FSC welcomes the opportunity to provide feedback to the Government on the Privacy Act Review Report released on 16 February 2023 (the **Report**) and the 116 proposals (**Proposals**) set out in the Report.

The FSC is supportive of protecting the privacy of Australians and protecting consumers, while fostering a transparent, open and competitive economy. However, it is important that any changes to the Privacy Act do not create unintended consequences that result in detrimental impacts for consumers or unduly burdensome and impractical obligations for industry.

We have limited our specific comments in Sections 3 – 5 to Proposals in respect of which our members have raised concerns. We have also made some general comments in Section 2.2 below which reflect concerns of our members and have broader application to the issues discussed in the Report as well as other government policies.

2.2. General comments and executive summary

1. ***A roadmap is essential***. Given the broad scope and scale of the Proposals, and the inter dependent nature of many of the envisaged changes, as well as the considerable number of other government initiatives that have a bearing on the Proposals, it is important to have a roadmap from government that sets out the intended stages and accompanying time frames for the various contemplated changes. This roadmap should seek to identify as much as possible what consequences will arise for businesses as a result of any given Proposal. This is essential to assist stakeholders to effectively prepare for the future. We note that some businesses would require longer timeframes than others and some Proposals will need to work sequentially to ensure sufficient time for development and implementation. The roadmap can be refined over time and can be revised at suitable stages, but it would be advisable to publish an initial roadmap as soon as practicable. This could group the different Proposals into a number of stages and should allow for possible significant delays. It should also build in sufficient time for consultation with all relevant stakeholders. Without a roadmap it will be very difficult for stakeholders to be ready to meet the challenges of the new reforms as they are brought into law.

The FSC **recommends** that government provide a roadmap that sets out the intended stages and accompanying time frames for the various contemplated changes.

2. ***Appropriate transition periods are needed***. Transition periods will be required that reflect the scope and challenges of the Proposals and afford businesses with sufficient time to adapt and prepare. Consideration should be given to ensure that the transition periods should at least be comparable to the periods allowed in other international jurisdictions and take into account the significance of changes required of particular sectors. In addition, these periods should be reasonable in relation to each regulatory change as well as all such changes collectively; especially for Proposal 6.1 as the removal of the small business exemption would mean such businesses will be starting from scratch.

The FSC **recommends** that transition periods are provided that reflect the scope and challenges of the Proposals and afford businesses with sufficient time to adapt and prepare.

3. ***Coordination across government should be prioritised***. The considerable work undertaken by the Attorney-General's Department regarding the Privacy Act intersects and requires coordination with a number of other policy areas led by other government departments, notably Treasury and Home Affairs. For example, the Consumer Data Right (Treasury), the Australian Cyber Security Strategy (Home Affairs), Australian Cyber Security Centre, as well as work on regulating artificial intelligence and automated decision making (Industry, Science and Resources). To avoid inconsistency of messaging and policy direction, these and other relevant departments should establish interdepartmental committees or other review mechanisms[1]. Where businesses are required to comply with multiple reporting frameworks, further work should be done to harmonise security obligations across the various legislative frameworks.

The FSC **recommends** prioritising coordination across government.

4. ***Coordination between regulators is increasingly important***. The privacy landscape involves the input of a number of regulators in addition to the Office of the Australian Information Commissioner (OAIC), including ASIC, APRA, the ACCC and the ATO. This is particularly the case in the area of cyber security[2]. There is a risk that these regulators may not act in a coordinated and consistent manner where their activities have an impact on privacy reform. This could result in inconsistent regulation and guidance. A framework should be established to enable them to coordinate and work together in an efficient manner. We note also that many businesses operating in Australia are part of international operations that also need to comply with overseas regulatory regimes.

The FSC **recommends** the establishment of a framework to coordinate the work of regulators and enable them to work together in an efficient manner.

5. ***Avoid unintended negative consequences for consumers***. The Report contemplates considerable changes and new requirements which will increase the regulatory burden for business. While enhancing transparency and consumer protections is important, the Proposals need to be considered individually and cumulatively with regard to potential negative impacts that they may in turn have on consumers. For example, substantial amounts of additional information to be provided to consumers in privacy policies and collection notices or requiring consumers to make more decisions concerning consent and other issues, need to be balanced to avoid information overload, disengagement

[1] We note a similar sentiment has been expressed by other government agencies and regulators, see for example ACCC Chair Gina Cass-Gottlieb speech at the Opportunities and Challenges in the Digital Revolution Conference at Monash University on Friday, 17 March 2023 " We are also aware of the broader context in which we are making these recommendation…the wide range of other digital platform issues that the Government is currently considering including in relation to cybersecurity, privacy, and misinformation and disinformation. It is important that all relevant government departments and agencies are involved ….": Opportunities and Challenges in the Digital Revolution | ACCC

[2] See for example APRA Prudential Standard CPS 234 Information Security; the Privacy Safeguard Guidelines relating to Part IVD of the Competition and Consumer Act 2010 (Competition and Consumer Act), which establishes the Consumer Data Right; and ASIC guidance including at Cyber resilience | ASIC

and consumer fatigue or impacting the ability of a business to competitively deliver the goods or services that the consumer has paid for.

The FSC **recommends** avoiding providing too much information to consumers which risks adverse unintended consequences.

6. ***Facilitate crime prevention***. The Privacy Act does not have a general principle which clearly permits a business to act on the information it holds to protect consumers from fraud or other crime. Given that businesses holding information about their consumers can be in a position to prevent crime, there should be clear legislative protections for consumers (and businesses) in the Privacy Act to deal with scenarios where it would be appropriate for a business to take action in the face of imminent or actual criminal activity. For example, this could include permitting businesses within a particular sector to share certain data sets with other entities in the same sector (e.g. banks), such as information about known scam websites, scam phone numbers, illicit bank account details and IP addresses. This would potentially help to reduce the risk of their customers falling victim to financial crime. On a broader level, government should work to improve the Australian privacy framework to enhance the ability of regulators to share data with each other and with APP entities to improve their collective ability to detect and prevent financial crime. For example, where a particular scam is reported to AUSTRAC, government could examine ways to enable AUSTRAC to share relevant information more efficiently with ASIC or at risk consumers. The Privacy Act could include a general principle that permits businesses to assist with this regulatory action within appropriate boundaries.

The FSC **recommends** that further consideration is given to enabling businesses and regulators to use information to combat crime.

7. ***Avoid overregulating financial services businesses***. To the extent the Privacy Act is materially amended and imposes material additional or changed requirements on financial services businesses, this will add to the growing cumulative regulatory burden they face. Financial services businesses are already highly regulated with respect to many of the issues raised in the Report. This is particularly the case with regards to requirements concerning record keeping and protection of information. Overly prescriptive requirements that overlap or, worse, conflict with other laws and regulations that are relevant to financial services businesses will be counterproductive. It is important that changes to the Privacy Act do not conflict with other existing legal or regulatory requirements or result in overlapping or unnecessarily burdensome regulation. And where there are unintended conflicts between the requirements of the Privacy regime and other legislation, there will need to be clear methods to resolve these conflicts. In this regards the proposed review of existing laws should be substantially completed before relevant changes to the Privacy Act are brought into effect[3].

[3] See 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. The FSC also suggests that legislative instruments and guidance published by ASIC, APRA and other regulators is also of relevance.

The FSC **recommends** that the Proposals are reviewed against existing legislation and guidance to prevent inconsistency and conflicts of laws.

8. ***Provide more detail in a timely manner*.** Many of the Proposals in the Report require further consultation with industry and work with other branches of government, while in respect of other Proposals the specific wording of draft legislation and accompanying OAIC guidance will be critical. The FSC cautions against endorsing a particular Proposal until the full details have been properly considered and been discussed during meaningful public consultation processes, as well as having had the benefit of considered input from other relevant branches of government. It is important to ensure the changes to the Privacy Act are made in a coordinated manner with other relevant policy changes both with respects to content and timing. Where OAIC guidance or other regulatory guidance is integral to a Proposal, this guidance should be finalised well before the related Privacy Act amendment takes effect to avoid the undesirable scenario of a legislative change taking effect before the relevant guidance is available.

The FSC **recommends** that draft legislation and guidance is provided to stakeholders as early as possible to enable meaningful consultation.

9. ***Maximum periods to comply with obligations to be reasonable.*** Care needs to be taken to ensure that periods set for businesses to comply with their privacy related statutory duties are reasonable and do not impose an undue or unreasonable burden for businesses. For example, the reporting period of 72 hours to report for notifiable data breaches appears to be too short to be reasonable for many industry participants, particularly small businesses (see page 18 comments on Proposal 5.4). This would appear to be a situation where a "one size fits all" approach may not be appropriate and consideration should be given to other more granular measures, for example different time frames and/or different levels of detail that reflect the size of the reporting entity as well as the magnitude and seriousness of the particular breach.

The FSC **recommends** that proposed compliance timeframes do not impose an undue burden on businesses.

3. Part 1: Scope and application of the Privacy Act

3.1. Personal information, de-identification and sensitive 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.*

The concept of a connection not being too tenuous or remote can be explained and clarified through explanatory materials and OAIC guidance (and in due course potentially through case law), but only up to a point, and there will inevitably be a level of some uncertainty. Including a definition of "relates to" in OAIC guidance rather than the Privacy Act will have the benefit of greater flexibility and may help avoid unintended consequences for consumers and businesses.

Expanding the definition of personal information will require businesses to review all of the data they retain about consumers, which for many will be a material impost on time and resources. It is important that OAIC guidance is provided in a timely manner before any proposed changes are implemented.

Proposal 4.6 *Extend the following protections of the Privacy 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:

(b) from misuse, interference and loss; and

(c) from unauthorised re-identification, access, modification or disclosure.

(d) 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.

There is considerable uncertainty as to the expectations on an APP entity to prevent an overseas business from breaching the APPs in relation to de-identified information, as well as a practical concern as to how this would work in practice. It is doubtful to what extent an APP entity will be able to carry out an effective due diligence of a potential contract counterparty prior to entering into a commercial arrangement. And once a contract has been negotiated and entered into, an APP entity is unlikely to be able to effectively test or carry out ongoing monitoring as to what an overseas recipient does with any information it is provided. On the other hand, an overseas recipient is unlikely to be willing to agree to abide by Australian law which it knows little or nothing about and may be commercially unwilling to investigate or assume any associated legal risks in respect thereof. The question of "what is

reasonable in the circumstances" will be difficult to answer and in the FSC's view the test of "ensuring" compliance is unduly onerous.

In addition, it is not clear how the broader test of Proposal 12.1 (requiring that the collection, use and disclosure of personal information must be fair and reasonable in the circumstances) would sit alongside the test proposed in Proposal 4.6 in relation to APP 8 and is likely to create further confusion. For example. Proposal 12.1 states that the fair and reasonable test is to be an objective test to be assessed from the perspective of a reasonable person, but there is no such similar statement in Proposal 4.6, which gives rise to the question as to whether the distinction is merely an omission or intentional (and if it is intentional, what is the underlying rationale for it?).

3.2. Small business exemption

Proposal 6.1 *Remove the small business exemption, but only after:*

(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.

There will be considerable challenges associated with the removal of the small business exemption. When it comes to impact analysis and consultation, it is important that this be carried out in a tailored fashion with representatives from specific industry sectors so that specific industry concerns can be properly identified. For example, with regards to the financial services industry, authorised representatives (**ARs**) of Australian financial services licensees (**AFSLs**) currently rely on their AFSL to comply with certain aspects of the Privacy Act including in relation to requirements concerning privacy policies. Any changes to these requirements will need to consider the impacts on the AFSL and its ARs.

The FSC would caution against prematurely requiring small businesses to comply with the full extent of the Privacy Act. Some small businesses would process and use a relatively large amount of personal information while others would have almost none and appropriate risk assessments should be done in this regard. It would be appropriate to consider a staged process that involves a gradualist approach to making different parts of the Privacy Act applicable to different sectors of the economy only once they are ready and able to comply.

Comprehensive roadmaps and related reasonable transition periods (*see Paragraphs 1 & 2 of Section 2.2 above)* will be particularly important for small businesses to plan and implement necessary changes to become fully compliant having in mind that the majority of them will have to set up entirely new internal systems, practice and procedures. Also, it is

recommended that consideration be given to ensure that they are given as much flexibility and support as possible, such as having the capacity to outsource.

3.3. Employee records exemption

Proposal 7.1 *Enhanced privacy protections should be extended to private sector employees…*

The FSC supports further consultation on extending appropriate privacy protections to private sector employees, in particular the interaction of privacy and workplace relations laws. We agree with the statement in Proposal 7.1(b) that the aim should be to include "*ensuring that employers have adequate flexibility to collect, use and disclose employees' information that is reasonably necessary to administer the employment relationship, including addressing the appropriate scope of any individual rights and the issue of whether consent should be required to collect employees' sensitive information*". In this regard administering the employment relationship would need to take into account issues such as performance management, employer-employee disputes and whistle-blower investigations. We note that in some cases it may be appropriate to seek consent from the current or former employee and in others, the employer may appropriately refuse to provide detailed or sensitive information about a current or former employee if requested by another organisation such as a new employer. Appropriate exemptions need to be fully explored, including a right to quarantine information rather than erase it (see comments on Proposal 18.3, below) and those set out in Proposal 18.6 that would apply to rights of the individual[4].

[4] Proposal 18.6 contemplates "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".

4. Part 2: Protections

4.1. Privacy policies and collection notices

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.

The FSC considers that there is a risk of information overload in providing more detailed collection notices to individuals. The reality is that the vast majority of individuals will not read these collection notices. The content of collection notices that is provided to individuals automatically should be reconsidered with a view to reducing the quantity of information provided. Some of the information could be moved to a privacy policy, and/or only provided upon request. The longer a collection notice is, the less likely many consumers are to read them.

The related Proposal 10.3 to develop standardized templates and layouts for collection notices also poses a risk of excessive use of "boilerplate" terms that are simply not read by the recipients, and a "tick the box" approach where businesses feel that to protect themselves they need to include as much information as possible in the collection notice. To do so would of course make them even less readable and accessible.

4.2. Consent and online privacy settings

Proposal 11.1 *Amend the definition of consent to provide that it must be voluntary, informed, current, specific, and unambiguous.*

The FSC agrees that further OAIC guidance should be published to clarify the parameters of the proposal. In this regard, the Report states that "*Whether a particular consent is current would depend on the context. Consent can be considered as current where the purpose for which the personal information is handled has not materially changed. Periodic renewal of consent should not generally be required*. "[5] With regards to periodic renewal, this is likely to

[5] Page 105

be impractical and a disproportionate burden for many businesses with no consumer benefit and the added negative impact on consumers of considerable consent fatigue. We would suggest that the OAIC guidance makes it clear that periodic renewal should only be required in exceptional, specified circumstances and again subject to appropriate exceptions (such as contemplated in Proposal 18.6).

4.3. 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.*

The FSC notes that there are already other existing and proposed prescribed requirements to provide detailed written information in privacy policies[6] and collection notices that go to the collection, use and disclosure of personal information, and the preparation of privacy impact statements, as well as an overarching proposal that this must be fair and reasonable in the circumstances.[7] All of these requirements will effectively require businesses to prepare a number of written records in any event and accordingly it would appear duplicative and confusing to add a separate new requirement as set out in Proposal 15.1. Depending on the requirements, businesses may need to expend material time and resources to comply. The administrative burden and cost to industry could be considerable, and it is not clear what the benefits would be.

This proposal also raises the practical question of what the "record" would constitute. Further guidance will need to be provided to provide more clarity. To the extent that this proposal requires the preparation and maintenance of some sort of register, we suggest that consultation with appropriate stakeholders is held well ahead of any proposed implementation date.

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.*

This proposal should be modified so that the senior employee can be sourced from another entity that is a member of the same corporate group. To restrict the appointment to an employee employed by the same legal entity is likely to prove impractical and of no consumer benefit in many situations, notably in the context of international businesses. The proposal could also be expanded to allow this role to be outsourced to a third party provider, subject to appropriate guardrails. Enabling the outsourcing of this role is likely to be of particular benefit to smaller businesses (*see also Proposal 3.2 on small business above).*

---

[6] See Proposal 10 and Proposal 11.
[7] See Proposal 12.1, 12.2 and 12.3

The FSC would caution against introducing a requirement on financial services businesses which is duplicative of provisions contained in other legislation – for example, we note that the Financial Accountability Regime (**FAR**) Bill 2023 has been re-introduced in the House of Representatives by the government recently, and if passed would require APRA-regulated entities to appoint a senior executive to take responsible for a number of business areas including privacy.

4.4. Rights of the individual

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.

The FSC has concerns about the burden on industry of a right to erasure. Implementing it will involve considerable effort to identify all the areas of a business where personal data could be kept, including computer back-ups, emails, databases and the like.

Given this, the exceptions to the right of erasure require careful consideration. In this regard the proposal in 18.3 to allow the quarantining of certain limited information needs further detail. Stakeholders should be provided with more specifics about what that limited information would be. In addition, the quarantining of information rather than erasure should be permitted not only for the purposes of law enforcement, but also where it is of clear benefit to a customer or necessary for the business to carry out the services that it has contracted with the customer to provide. Further, the relevant exceptions set out in Proposal 18.6 should cover not only situations where the right is inconsistent with another law or contract, but also where it is inconsistent with regulatory requirements, guidance or industry codes (noting that often regulatory guidance goes beyond the law or at times is arguably inconsistent with the letter of the law).

The FSC also notes that the financial services industry is required to keep records and data in a number of situations. Financial services organisations are generally regulated by ASIC, APRA, AUSTRAC among others and are required to retain, securely store and be able to access information about customers and business activities to respond to regulatory enquiries and communications. In addition to this obligation to retain information, other key record retention obligations include, but are not limited to:

- Corporations Act 2001 (Cth) - obligations regarding business records;
- Anti-money laundering and counter-terrorism financing Act 2006 (Cth);

- Insurance Contract Act (s21) 1984 (Cth) - for life insurers; and
- The Superannuation Industry (Supervision) Act 1993 (Cth).

If passed, the FAR would add to his list of statutes. Other laws of general application also apply, such as the Spam Act 2003 (Cth) and the Australian Consumer Law. In addition, such organisations need to retain and access information to provide to law enforcement agencies, courts and tribunals, including, but not limited to the Australian Federal Police and AFCA.

The nature of the financial services industry is such that customers expect their information to be held securely and available for the organisation to produce or review in the provision of its products and services. Therefore, a right to erasure needs to strike the appropriate balance and particular care should be taken to avoid inconsistent requirements.

The right of erasure is based to an extent on the provisions of the EU's General Data Protection Regulation (**GDPR**). However, the FSC suggests that it does not go beyond the parameters of the GDPR by conveying rights on individuals which are broader than under the GDPR. Instead, consistency with the GDPR should be the aim. Better alignment with other international regimes will assist industry compete internationally and provide a more navigable framework for consumers when comparing products or services provided by businesses in different jurisdictions. Where the Proposal seeks to expand beyond the rights contained in the GDPR we suggest this be amended. For example, while Proposal 18.3(b) is similar to Article 17 and 19 of the GDPR, Article 19 appears to only require the controller to notify other controllers to whom the controller has disclosed the individual's personal data. The proposed Section 18.3(b) is significantly broader, requiring notification to APP entities from which the APP entity has collected the information. We suggest that the obligation to notify other APP entities of the erasure request be limited only to other APP entities to whom the APP entity has disclosed the information.

It is important that in looking to international jurisdictions for suitable comparators, the entirety of any given comparator jurisdiction's privacy regime is examined as a whole, otherwise there is a risk that false comparisons and conclusions will be drawn.

4.5. Direct marketing, targeting and trading

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.*

We note that the Report explains the reference to "unqualified" by stating:

"The opt out of personal information being used or disclosed for direct marketing purposes would be unqualified, meaning that an entity would have to stop using or disclosing personal information for direct marketing where a person exercised their right to opt out. Importantly,

exercising the opt out should not be a barrier to service for individuals who elect to make this choice."[8]

This explanation should be further developed. It does not provide clarity on the parameters or conditions around exercising the right to opt out and is somewhat circular.

Where an individual does elect to opt-out, there may be some situations where it is reasonable for an entity not to provide a particular service. Further consideration should be given to this issue.

In addition, it would be useful to know to what extent the right to opt out would impact other entities within a corporate group.

Industry should be consulted before any proposed definition or guidance around the nature of this unqualified right is defined.

Proposal 20.3 *Provide individuals with an unqualified right to opt-out of receiving targeted advertising.*

The FSC suggests that this be amended to limit the opt out of targeted advertising to "personal information", so that an organisation is not expected to opt out an individual from targeted advertising which uses deidentified or unidentified information and modelling based on groupings and other non-individualised information. This is because such information would likely be too remote or tenuous to the individual for an organisation to operationally comply with such an obligation, especially within a large group. This limitation should still provide control for an individual, as the new definition of personal information will be expanded.

Proposal 20.4 *Introduce a requirement that an individual's consent must be obtained to trade their personal information.*

While the FSC agrees that 'trading' in personal information should be appropriately regulated, in our view the proposed definition of 'trading' is too broad and the requirement for consent in order to 'trade' an individual's personal information needs to be balanced with appropriate exemptions after consultation with stakeholders.

At Section 20.4.1 of the Report, it is noted that "The GDPR does not include specific obligations for trading in personal data. Trading in personal data constitutes processing under the GDPR, for which organisations need to identify a lawful basis. In the data brokering context, the lawful bases that are generally referred to are consent and legitimate interests."[9]

We propose that the EU approach be adopted. Namely, 'trading' should not be defined and/or or consent should not be the only basis for 'trading' personal data, with particular

[8] Page 257
[9] Page 207/208

consideration given to the legitimate interests grounds for trading. We propose leaving it to the APP entities to identify the appropriate legal basis, and provide the appropriate transparency notifications to individuals when processing their personal data.

4.6. Security, destruction and retention of 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.*

The FSC welcomes this review. The more businesses are required by law to retain data, the greater the risk of loss or attack. Financial services businesses are particularly subject to numerous data retention requirements (See Proposal 18.3 above). There are a number of government policy initiatives that may require them to acquire even more data, including the Consumer Data Right (CDR), Australian Government Digital Identity System[10], and the Australian Cyber Security Strategy. The costs of insurance also need to be factored in, particularly in the context of the growing number of successful cyber-attacks. The FSC encourages government to undertake this review and ensure meaningful consultation with stakeholders is a part of the process.

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.*

The FSC notes that other Australian laws have record retention requirements that should be reviewed for consistency and overlap prior to any implementation of this Proposal in the Privacy Act – see our comments on Proposal 18.3 above.

Proposal 21.8 *Amend APP 1.4 to stipulate than an APP entity's privacy policy must specify its personal information retention periods.*

The requirement to specify in a privacy policy what could be a large number of different personal information retention periods would appear to be contradictory to the requirement for a clear, up-to-date, concise and understandable information collection notice (as per Proposal 10.1). While we accept that the privacy policy and the collection notice are two different documents, it would seem sensible that a privacy policy should also be clear, concise and understandable to the extent reasonably possible. The more detailed information is required to be included in a privacy policy, the more difficult it will be to read and understand, thus undermining its purpose. And we also note that in Proposal 16.3 the

[10] See Home | Digital Identity and Digital Identity system – Parliament of Australia (aph.gov.au)

Report states that both collection notices and privacy policies should be clear and understandable, particularly for information addressed specifically to a child.

The expansion of the definition of personal information under Proposals 4.1 and 4.2, together with Proposal 21 will require APP entities to consider what information will fall under the new definition, whether the steps taken to secure personal information and de-identify information are “reasonable” according to enhanced guidance and assess whether changes are needed to meet any baseline security outcomes. Additionally, APP entities will likely need to review existing service provider contracts to determine if data handled under the contracts is considered personal information under the new definition and/or whether the handling (including security, retention and destruction) of personal information is consistent with the new requirements.

The FSC also notes that the work required by industry to gather and categorise the relevant data for the purposes of this requirement would be significant and the regulatory burden considerable. Businesses will have a number of retention periods and many will have to comply with the requirements of several regulators making these retention data sets detailed and complex. In addition, the requirement to take into account inferred and general information is likely to constitute a significant additional amount of work for industry and may not always be practicable or technically feasible. Guidance will need to be provided as to the practicalities of how the relevant information can be embedded in a privacy policy.

Given these complexities, it would be important to provide for a meaningful transition period to allow businesses to make the required preparations.

5. Part 3: Regulation and enforcement

5.1. 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.

The introduction of any new civil penalty provisions should be treated with caution where there is the possibility that they end up capturing minor or technical breaches. The financial services industry is already grappling with a relatively new breach reporting/reportable situations regime that has had the effect of requiring large amounts of minor or technical breaches to be reported to ASIC. In our view, this has had little if any discernable consumer benefit, but with the negative impact of materially burdening financial services businesses and inundating ASIC staff with information that serves as an unwelcome distraction from more serious breaches. In this context, the FSC is concerned that the introduction of low-level civil penalty provisions will compound this problem. We also have concerns that the attached infringement notice powers end up being overused, particularly where there are complex issues that require evaluative judgments.

5.2. 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 this chapter.*

The FSC supports the design element set out in the Report that the claimant would first need to make a complaint to the OAIC to have their complaint assessed for conciliation by the OAIC. However, we would request further clarity on what a permissible assessment by "another recognized EDR scheme" would entail.[11] It would seem that the OAIC is best placed to assess complaints regarding privacy, given its expertise and oversight of the relevant issues. It is not clear what other body (for example, AFCA) would be appropriate. If the wrong type of EDR scheme is used the gateway model could be undermined.

The FSC notes that even if a direct right of action is introduced, it will likely be expensive and time consuming for individuals or groups to pursue this right by commencing litigation, particularly in circumstances where the act or omission of the business being sued could

[11] Page 279

have been identified and addressed by the relevant regulatory body. We submit that in this context it is important that the OAIC and other relevant regulatory bodies are adequately resourced to pursue and address privacy concerns raised by individuals in a timely manner and pursue appropriate investigations.

5.3. A statutory tort for serious invasions of privacy

Proposal 27.1 *Introduce a statutory tort for serious invasions of privacy in the form recommended by the ALRC in Report 123.*

It will be important to understand what constitutes a "serious" invasion, whether this is contained in a legislated materiality threshold, legislated factors, in explanatory memorandum or further guidance.

5.4. Notifiable data breaches scheme

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 28.2 (a) includes an obligation to notify the OAIC within 72 hours of becoming aware of a potential data breach. The Report indicates that the NDB Scheme enhancement is intended to assist with the objective of ensuring quick action is taken to minimize harm to affected individuals when a data breach occurs.

However, this proposed obligation appears to be at odds with section 26WF of the Privacy Act which provides, broadly, that where an entity takes remedial action to objectively eliminate the risk of serious harm to the affected individuals, then it is no longer a reportable breach under the scheme. It would appear that a similar exception to the requirement to make a report to the OAIC should be included in the design element of Proposal 28.2(a). It would be of limited utility to send details of a minor breach to OAIC which has been effectively remediated.

If the objective is to minimize harm, then APP entities ought to be required to notify affected individuals as soon as reasonably practicable where there is a suspected data breach (as set out in proposal 28.2(b)). However, early notification to the OAIC will not minimize harm to

the affected individuals and will potentially clog the OAIC's inbox with unnecessary over-reporting.