FSC FINANCIAL SERVICES COUNCIL

Privacy Act Review – Issues Paper

Financial Services Council Submission
2 December 2020

Contents

1. **About the Financial Services Council** 3
2. **Introduction** 3
3. **Executive summary** 3
4. **Background** 4
5. **Specific responses to questions in the Issues Paper** 5

1. About the Financial Services Council

The FSC is a leading 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, financial advisory networks and licensed trustee companies. 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 $3 trillion on behalf of more than 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 the fourth largest pool of managed funds in the world.

2. Introduction

The FSC welcomes the opportunity to provide a submission on the 68 questions raised in the Issues Paper published by the Attorney General's Department on 30 October 2020. This document is structured as follows:

- Executive summary;
- Background;
- Specific Responses on the 68 questions raised in the Issues Paper that are relevant to the financial services industry; and
- An invitation to engage with the Attorney General's Department and the Office of the Australian Information Commission (**OAIC**) during the reform process of Australian privacy laws.

3. Executive summary

The FSC is submitting on the following key points and our responses to the 68 questions in the Issues Paper are set out below:

- Supporting changes to update the current definition of 'personal information';
- Commenting on the proposed review of the current small business exemption;
- Supporting the removal of the employee records exemption;
- Commenting on the proposals regarding the method and frequency of obtaining consent for collection of information, noting that financial services providers generally obtain information from customers as part of a contractual and/or policy arrangement where they have a legitimate right to do so in connection with the primary purpose of providing their products and services;
- Commenting on the proposed introduction of a 'right to erasure' noting the current record retention obligations of financial services organisations;
- Commenting on the proposed new methods for customers to seek redress for breaches of their privacy and the current and forecast needs for OAIC resources to carry out their enforcement activities.
- Simplification of the Act by merging Australian Privacy Principle (**APP**) 10 and APP 13; and
- Recommending the fair and lawful provisions in APP 3 be repeated in the relevant provisions of APP 6.

4. Background

The FSC notes the inherent 'right to protection from unlawful or arbitrary interference with privacy' in Article 17 of the International Covenant on Civil and Political Rights. The principles articulated in this submission are based on that inherent right and the expectations of individuals and the wider community when entrusting information, including health, lifestyle and financial information to entities that are expected to respect that inherent right by implementing reasonable operational controls and risk mitigation strategies.

The FSC and its members support measures that strengthen privacy protections for individuals in Australia, and broadly supports consistency with similar principles in international privacy and data laws. The nature of financial services products and services is such that customers are often required to provide their personal and sensitive information, including health, lifestyle and financial information, in order to obtain those products and services. We are aware of the expectations of our customers and the wider community, regarding the way in which we collect, use, disclose and secure that information. The way in which we conduct business has changed significantly since the commencement of the Act in 1988, over 30 years ago, and many financial services organisations transact with their customers online, via mobile applications and using other technological advancements.

There are benefits and challenges regarding the use of modern technology and digitalisation to communicate and engage with our customers and these can provide efficiency, convenience and simplicity to customers, as opposed to traditional face to face interactions between financial services organisations and their customers. We acknowledge that customers expect that their data is appropriately handled, irrespective of the method of transmission or storage of data. Many financial services organisations also transact with related body corporates and other businesses based overseas and are bound by international privacy and data protection laws and regulations, in addition to those applicable in Australia. The main countries in which FSC members transact include, but are not limited to, the European Union (EU), New Zealand, Canada, Japan, Singapore, the Philippines, Hong Kong and the USA. It is noted that the new Privacy Act 2020 came into force in New Zealand (**NZ**) on 1 December 2020 to incorporate recent technological advancements.

We acknowledge that privacy laws in Australia were updated twice in the last five years with the adoption of the 13 Australian Privacy Principles, to replace the 10 National Privacy Principles, in March 2014 and the commencement of the Notifiable Data Breaches Scheme (NDB) in February 2018. We note that many other privacy law reforms have been implemented in other jurisdictions, but not Australia, including, but not limited to the General Data Protection Regulation (**GDPR**) in the EU. We note that privacy and data law reforms in other jurisdictions in which financial services organisations regularly transact, have considered the contemporary technological advances, data risks and community expectations and have amended the relevant legislation accordingly.

We are cognisant of the fact that some provisions of the Privacy Act, including some definitions, have not been updated in more than 30 years. During that 30-year period technological and communication advances have been significant. In 1988 we would expect that the vast majority of individuals did not have devices that could:

- track their online presence and shopping or product preferences to allow profiling and targeted marketing,

- track their online communications with friends and family, including messages, photos and videos;
- monitor their physical location and their health and fitness, such as watches and other devices that are worn on the body; or
- verbally request online internet searches and information and store that information.

In addition, in 1988 we would propose that there was little knowledge or understanding of the terminology or risks of issues such as hacking, phishing, IoT, profiling, data analytics, cryptography and cybercrime.

We acknowledge that technological advances are likely to continue at a similar or even greater pace in the coming decades and the way in which financial services are communicated with and deliver its products and services to customers in the future may be substantially different from the way they are provided now. It is important therefore, that any proposed changes to privacy and data security laws are principles based and "future proofed" so that additional changes are not required in response to technological and digitalisation advances going forward. Examples of technological advances that can impact how organisations collate, analyse and disseminate customer data, include, but are not limited to: Artificial Intelligence (AI) Big Data profiling, data harvesting, data mining, data analytics, cryptography disruptive innovation and the Internet of Things.

Ultimately, there is a delicate balance between individuals' legitimate rights to privacy and their increasing desire to access financial products services and benefits conveniently, quickly and on demand. Many financial services organisations, and their business partners, operate businesses that pool and manage societal risks and we submit that these services an important public interest. For example, insurance risk in the case of insurers, longevity risk in the case of superannuation trustees and credit risks in the case of credit providers. We consider that our customers benefit when financial services organisations can properly assess these societal risks when designing and implementing their products and services for the benefit of their customers in an efficient manner, taking into regard the relevant legislative and regulatory obligations. Being able to collect data about societal risks and community expectations is key to providing benefits to customers of financial services organisations, such as developing product features in response to customer feedback and surveys. We note that regulators of financial services organisations regularly and increasingly collect aggregate information about financial services products and services, together with and the experience and feedback provided by customers.

5. Specific responses to questions in the Issues Paper

Objectives of the Privacy Act

Question 1: Should the objects outlined in section 2A of the Act be changed? If so, what changes should be made and why?

Response to Question 1:

We submit that the objects outlined in section 2A of the Act should be changed to align with the stated objects of privacy legislation in jurisdictions in which financial services organisations operate, including, but not limited to the EU, United Kingdom, New Zealand (**NZ**), Canada and United States. Our members regularly transact globally in relation to their

provision of products and services and in connection with their processes to transmit and store data entrusted to them by their customers.

We consider that section 2A could be simplifed and made consistent with other laws such as Article 1 of the EU GDPR and s3 of the NZ Privacy Act 2020. We submit that this step would help to 'future proof' the Act.

With regards to simplification of the Act, although these specific questions were not raised in the Issues Paper, we consider that any review of the Act should:

A. Question whether the requirement for collection by "fair and lawful means" in APP 3 could also be applied to the APP 6 requirements for use and disclosure of information. We consider that this is particularly important for organisations in the business of data collection and analysis, digital platforms such as social media organisations and businesses that regularly transact with children, the elderly and the vulnerable in our community; and

B. Question whether the similar principles and requirements of APP 10 and 13 regarding the quality and correction of information respectivley, are similar and potentially duplicated, and as such, that the two principles could be combined.

We note that if the Government was minded to consider implementation of a statutory tort, or other methods to remediate and redress interferences with privacy are implemented, it may be prudent to update section 2A to expand the current wording about individuals having the right to complain, so that it reflects the new obligations and any new expectations of the OAIC regarding their enforcement powers.

Definition of personal information

Question 2: What approaches should be considered to ensure the Act protects an appropriate range of technical information?

Question 3: Should the definition of personal information be updated to expressly include inferred personal information?

Question 4: Should there be additional protections in relation to de-identified, anonymised and pseudonymised information? If so, what should these be?

Question 5: Are there any other changes required to the Act to provide greater clarity around what information is 'personal information'?

Response to Questions 2 to 5:

In Australia, the definition of "personal information" in the Privacy Act states:

"*information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable*."

The current definition does not specify whether items such as ISP and mobile phone numbers can be interpreted as falling within that category and acknowledges guidance materials

published by the OAIC on that topic. However, it is our position that it would assist commercial businesses, including the financial services industry, if there was greater clarity about the categories of information that fall within the "personal information" definition. It may be useful to consider the definitions of "personal information" used in other jurisdictions, such as New Zealand and the EU. We consider that the current definition of personal information may not be as readily understood as the specific listing of what constitutes "sensitive" information. There is a level of ambiguity on behalf of organisations and individuals and we submit that a Plain English definition would be preferable to assist individuals in their understanding of the types of information that is considered personal information and their redress for such breach. For organisations, it will ensure compliance with the provisions of the Act regarding their collection, use, security and disclosure of that information.

We have considered individual and societal expectations pertaining to the privacy of personal information in the modern digital era. Deliberate or negligent misuse of data by organisations may not only contravene the relevant legislation in the jurisdictions in which they operate, but may also contravene the basic human right of privacy which is enshrined in many international laws and treaties and within the constitutions of nation states in which financial services organisations regularly transact.

We endorse the recommendation to update the definition of "personal information" to provide clarity to both consumers and businesses. Whilst guidance materials from the OAIC are useful, they are not binding on organisations which can result in ambiguity regarding whether one or more data sets meets the definition of "personal information." For consumer protection and business efficacy, we support aligning Australia's definition of "personal information" with international definitions including, but not limited to, technical data such as IP addresses, device identifiers, location data and any other online identifiers that may be used, individually or collectively, to identify one or more individuals. The Attorney General's Department may wish to consider the definitions of personal information in privacy regimes such as the UK, EU, Canada, US and New Zealand, including, but not limited to Article 4 of the GDPR. Many financial services organisations operate globally and the difference between the Australian and international definitions of personal information can lead to confusion for entities that need to comply with obligations under other jurisdictions.

Accordingly, we endorse, in principle, the proposal to update the current definition of personal information in the Act to include the following items: IP addresses, device identifiers, location data, URL's with social media profiles and other online identifiers such as files embedded on devices such as pixel tags and cookies and device fingerprints.

The value, amount and extent of the data and the number of data sets may increase the likelihood of identifying one or more individuals e.g. a date of birth on its own would be unlikely to identify an individual. By contrast, a date of birth combined with contact details, financial details, policy or account number details etc. would generally increase the ability of organisations to identify an individual and transact with them on a commercial basis.

We consider that de-identified and pseudonymised data should still be protected where it is reasonably likely that a person, or entity that can access that data can re-identify it. Where there is no reasonable risk of re-identiifcation, data should be excluded from the definition of personal information to allow financial services organisations to better understand their customers, their makets, the societal risks they pool and develop more effective products and services for the benefit of their customers.

We acknowledge that cybercriminals looking to commit fraud, identity theft and other offences may aim to obtain a number of different data sets about individuals to build a profile of an individual for the purposes of being able to bypass operational controls implemented by businesses such as identification checks before the disclosure of information.

As stated in our Executive Summary, we consider that any definition of personal information should be sufficiently wide to allow for any technological changes and new methods of being identified and transmitting and storing data that may occur in the future.

Small business exemption

Question 7: Does the small business exemption in its current form strike the right balance between protecting the privacy rights of individuals and avoid imposing unnecessary compliance costs on businesses?

Question 8: Is the current threshold appropriately pitched or should the definition of small business be amended?

a. **If so, should it be amended by changing the annual turnover threshold from $3 million to another amount, replacing the threshold with another factor such as the number of employees or the value of assets or should the definition be amended in another way?**

Question 9: Are there businesses or acts and practices that should or should not be covered by the small business exemption?

Question 10: Would it be appropriate for small businesses to be required to comply with some but not all of the APPs?

a. **If so, what obligations should be placed on small businesses?**
b. **What would be the financial implications for small businesses?**

Question 11: Would there be benefits to small businesses if they were required to comply with some of the APPs?

Question 12: Should small businesses that trade in personal information continue to be exempt from the Act if they have the consent of individuals to collect or disclose their information?

Response to Questions 7 to 12:

Currently, entities out of scope of the Act include small businesses with an annual turnover of AUD $3 million or less. This does not include assets held, capital gains or proceeds of capital sales. Regardless of turnover, the Act covers businesses that are:

(a) health services providers;
(b) businesses trading in personal information;
(c) credit reporting agencies;
(d) reporting entities for the purposes of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth); and
(e) related to a business the Act covers.

Based on 2019 data from the Australian Bureau of Statistics, small businesses make up 98.45% of all Australian businesses and have a turnover of less than $200,000. This means there is a lot of personal information being processed by these businesses that is currently not protected under the Act (except in cases where businesses comply with a privacy code such as market research).

Financial services providers utilise the services of many third-party service providers to assist them to deliver their products and services to customers. These include, but are not limited to service providers that assist our businesses with communications to and from customers such as mail houses, IT infrastructure and support, projects, product development, research and marketing etc. For example, within the life insurance sector, third party providers are also used to assist in efficiently implementing activities related to underwriting assessments and claims assessments etc. This necessitates our organisations placing reliance on those third-party providers to treat the personal and sensitive information of our customers in accordance with applicable privacy and data security laws and regulations. However, the current scope of the Act does not extend to a number of organisations with an average annual turnover of AUD $3 million or less, unless they meet specific criteria such as being healthcare providers. Further detail on this point is set out below in response to the specific recommendations. Financial services organisations will take a number of risk mitigation steps when using these third-party providers in order to protect the information and restrict its usage and disclosure under the arrangement. However, when using the services of third-party services providers that are not subject to the provisions of the Act, this can increase the risks of harm to customer information, depending on the extent and value of information disclosed.

Generally, when financial services providers conduct due diligence, a contract is put in place and vendor management is carried out. However, for small businesses out of scope for privacy legislation the residual risks can still be significant, particularly if the outsourced service provider is handling medical and/or financial information. In the event of a breach of the provisions of the Act or a notifiable data breach, our customers would be likely (and rightly) hold the financial services organisation accountable if the act or omission was actually the fault of the third-party service provider. This would be likely to result in brand and reputation damage to the financial services provider rather than the outsourced service provider, apart from any customer detriment. Depending on the size and sophistication of the outsourced service provider they may not have either the financial or IT resources to implement a robust privacy management framework or controls. They may simply become insolvent and renege on the contract as a result of a data breach, particularly for start-up organisations, fintechs etc. It is our position that it would be more equitable if **all commercial businesses handling personal and/or sensitive information** should be bound by the provisions of the Act. This is likely to result in greater protection of information about Australians and more consistency between commercial businesses regarding their information handling practices, including, but not limited to, the security of Personally Identifiable Information ("**PII**").

If the turnover threshold is simply amended, an arbitrary turnover amount may result in businesses being financially structured to have an annual turnover of less than the limit imposed which could lead to businesses existing or being established primarily for data analytics purposes for commercial gain. We acknowledge that financial services providers are regulated by a number of Government departments and agencies in addition to the OAIC, such as ASIC, APRA, AUSTRAC, ATO etc. and are bound by substantial legislative and regulatory obligations, industry codes, standards and similar. By contrast, under the current Act a small business, fintech, start-up business or data analytics organisation may not be bound by any relevant privacy or data legislation and may not have any regulators monitoring its business practices, acts or omissions with regards to PII data.

We acknowledge that there are organisations established or adapted to specifically specialise in the business and value of data for profiling and marketing purposes and we submit that businesses set up to obtain multiple data sets about individuals for financial gain should be bound by the provisions of the Act.

We submit that it would be an unfair and unreasonable imposition on true small businesses such as local shops, hairsalons etc. to require them to comply with all obligations within the Act. However, we acknowledge that some businesses under the current $3m turnover would be collecting, handling and disclosing significant amounts of personal and sensitve information, such as businesses involved in data analytics, Big Data, IoT and AI. We note the current provisions in section 6D(4)(c) and (d) of the Act relating to these types of businesses and consider that there would be a number of businesses collecting, using and disclosing personal and sensitive information about individuals that did not fit within the current definiton of “benefit, service or advantage for disclosure or collection of personal information.” As such the review of the small business exemption in the Act may wish to expand this definition to capture the range of businesses involved in data analytics, profiling, marketing and so forth.

We propose that in 2020, as opposed to 1988, small businesses should be able to access and implement basic IT security and cyber security operational controls to protect the information that they hold. APP 11 stipulates that the range of security measures that an entity is expected to implement will depend on its size and the nature and extent of the information that it holds.

Whilst it would generally be inequitable to require small businesses to comply with the full extent of the obligations in the Act, we consider that any organisation handling personal and sensitive information about a large number of individuals should be able to implement some basic IT security and cyber security controls to protect that information from unauthorised access, misuse, loss, unauthorised disclosure and interference (including hacking and phishing attacks). We consider that small businesses that are registered charities or provide community services should be exempt from the provisions of the Act, as should small businesses that only collect and use a limited amount of personal information such as contact details to make appointments with their customers. By contrast, those small businesses that collect, hold, secure and disclose a significant amount of personal and sensitive information should implement reasonable controls such as those set out in APP 1, 3, 4, 5, 6, 8, 10, 11, 12 and 13. We think consumers would expect this.

We submit that societal and community expectations are such that individuals providing personal and sensitive information that could result in a real risk of harm would expect an organisation to be bound by the provisions of the Act e.g. a small accounting business holding information such as a TFN, salary amount, assets and liabilities, expenses, bank and credit card details.

We suggest that small businesses can take advantage of technological advances since 1988 to secure and protect their customer information and their business information. Since the late 1980’s there is a great deal more awareness about basic IT security and cyber security hygiene such as the importance of access controls, software updates and anti-virus protections. Compared to the late 1980’s it is much easier to implement these operational controls with “smart” devices regularly updating security patches in response to known threats without much effort from the user of those devices.

We submit that any small business entrusted with either a great deal of personal information, or any sensitive information, should adhere to at least basic privacy law provisions about collection, use, security, disclosure, accuracy, access, consent etc. via one of three ways:

1) Employing an IT/Cyber person with the knowledge and skills to implement and maintain appropriate systems, controls, policies, training, testing etc.

2) Hire an IT/Cyber consultant as an outsourced service provider, to establish and maintain appropriate systems, controls, policies, training, testing; and/or

3) Look online to find out what minimum controls should be implemented e.g. the Australian Cyber Security Centre, OAIC and ASIC Scamwatch websites have this information. Once the small business is aware of the minimum controls that should be implemented they can take action to protect their customer information and review the operational controls periodically e.g. a "light" version of the operational controls known as the "Essential 8" and set out in APP 11, such as the items outlined below:

- Operational controls to back up, retain and be able to retrieve information, including the use of cloud software;
- Physical and electronic controls to access systems and applications on a "needs only" basis, such as unique login and strong passwords with the use of dual or multifactor authentication;
- Regular penetration testing against hacking and phishing attacks;
- Anti-virus controls including regular patches and upgrades;
- Regular reviews of installed software, including the implementation of software patches and updates;
- Ensuring there is accountability for IT and cyber security controls within the organisation, or by utilising reputable external resources; and
- Regular training and scenario testing for staff to identify, report and remediate IT and cyber security incidents and breaches.

We propose that small businesses should be clear on their website and communications whether or not they comply with the Act. For example, some small businesses which are in the business of marketing, A1, Big Data, data analytics etc. currently have a document on their website that appears to be an APP Privacy Policy, when they are actually exempt from the provisions of the Act as they are under the $3m turnover threshold and do not provide services such as health services. This can create a false sense of security for individuals and other businesses transacting with that small business.

We submit that it would not be an overtly costly or administrative burden for small businesses to keep information about their customers up to date, implement security controls and inform customers about their information handling practices such as disclosures of information to other organisations.

We consider that contemporary community expectations are such that customers would expect small businesses to collect, use and disclose information about individuals for legitimate business purposes in connection with the products and services that they provide to their customers.

We consider that setting an annual turnover amount such as $10m would exempt a number of small businesses from the provisions of the Act that were quite capable and resourced for implementing appropriate operational controls to protect the information entrusted to them by their customers and business partners. Setting an annual turnover amount may also involve the risk of a business being financially structured so as to deliberately be below the limit and exempt from the provisions of the Act, even if that business collected, used and disclosed significant amounts of personal and sensitive information that would be likely to result in a real risk of reasonable harm to customers if it was lost, misused or subject to unauthorised access and/or disclosure.

Rather than an annual turnover amount, we consider that the type and extent of information should form the primary criteria for being subject to the provisions of the Act. Should more of the 98.45% of small businesses in Australia be bound by the obligations in the Act, we consider that big businesses would be more likely to appoint those smaller businesses as third party providers and entrust their customer information to them.

Should the small business exemption be amended or removed from the Act, we consider that it would be helpful for businesses if the OAIC were to provide guidance materials regarding the steps that organisations would be expected to take to comply with the new obligations.

Employee records exemption

Question 13: Is the personal information of employees adequately protected by the current scope of employee records exemption?

Question 14: If enhanced protections are required, how should concerns about employees' ability to freely consent to employers' collection of their personal information be addressed?

Question 15: Should some but not all of the APPs apply to employee records, or certain types of employee records?

Response to Questions 13 to 15:

During 2020 employers have gained greater insights into the activities, health, travel movements and homes of their employees than ever before. As a result of the COVID-19 pandemic, employers have been required to collect personal and sensitive information about their employees in order to comply with Federal and State Health Orders and Directives. Prior to the pandemic employees entrusted the following types of information to their employers and we consider that they had reasonable expectations that there would be appropriate operational controls to protect the security of that information:

- Salary and bonus information;
- Tax file number and other Government identifiers such as passport and driver licences to complete employee due diligence checks;
- Information about the employee performance and any disciplinary proceedings;
- Information such as the results of Australia Federal Police criminal history checks and bankruptcy checks to complete employee screening processes;

- Information about the employees' health, lifestyle and wellbeing, such as medical reports to support sick leave and workers compensation claims.

As such, we support the removal of the employee records exemption from the Act. We consider that this would align Australia with other jurisdictions such as the EU and NZ. In the employee/employer relationship there is a natural power inbalance so this means its is even more important that individuals as employees have their privacy protected by law, as they usually don't have a choice about the processing of their personal information.

We submit that the removal of the employee records exemption from the Act will not cause a significant imposition on businesses as it is common practice to segregate functions such as payroll and human resources to ensure that information about employees is on a "need to know" basis and only assessible to approved staff. In addition, many businesses implement physical and electronic access controls to employee records, including specific IT systems designed to protect the privacy of employees.

We submit that employees would reasonably expect their employers to implement reasonable operational controls to protect the privacy of information about employees, outlined above. Employers have access to information about their employees that they didn't have in 1988. Issues regarding employee physical and mental health, working from home arrangements and any work health and safety concerns were not as prevalent in 1988. Therefore, we consider a timely review of this exemption is needed, especially in this current enviroment and the information requried to be disclosed as a result of the pandemic.

We consider that employers should only use, handle and disclose employee records for a legitimate business purpose. For example, to help the organisation to comply with the law or protect its legitimate interests, for the purposes of an internal or external investigation or law enforcement process, such as fraud or immigration and visa issues. Another example, would be if the organisation was defending a complaint or dispute in regard to payment or disciplinary procedings and the information was needed to provide the factual evidence. 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 about a current or former employee if requested by another organisation such as a new employer.

Should the employment records exemption be removed from the Act, we consider that it would be helpful for businesses if the OAIC were to provide guidance materials regarding the steps they would be expected to take to comply with the obligations to protect the privacy of current and former employees.

Notice of Collection of Personal Information - Approving awareness of relevant matters.

Question 20: Does notice help people to understand and manage their personal information?

Question 21: What matters should be considered to balance providing adequate information to individuals and minimising any regulatory burden?

Question 22: What sort of requirements should be put in place to ensure that notification is accessible, can be easily understood; and informs an individual of all relevant uses and disclosures?

Question 23: Where an entity collects an individual's personal information and is unable to notify the individual of the collection, should additional requirements or limitations be placed on the use or disclosure of that information?

Response to Questions 20 to 23:

Financial services organisations generally collect information about their customers and other individuals as a result of a contractual obligation to provide products and services. For example, a customer may have completed an application for an investment or loan product after confirming that they had read the Product Disclosure Policy and declared that they had read the privacy statement and APP Privacy Policy of the organisation.

Simillarly, a customer may have applied for a life insurance policy and consented to the collection of reasonable and relevant information to complete the underwriting assessment. The life insurer would generally ensure that the customer had confirmed that they had received the relevant product disclosure document, understood their duty of disclosure and informed the customer about their information handling practices by referencing a short form privacy statement and a long form APP Privacy Policy.

By contrast to the robust steps that financial services organisations take to inform customers about their information handling practices, including the collection, use, security and disclosure of information, we note that less regulated organisations may "bury" or attempt to disguise notices at the end of lengthy terms and conditions that individuals may not read, for example, when downloading applications for social media accounts.

We note that many people do not read or comprehend privacy notices and consider that it is the responsibility of individuals to manage the security of their information and understand basic steps they can take to protect it. For example, the OAIC, Australian Cyber Security Centre and ASIC's Scamwatch all provide simple to follow information about basic security controls individuals can implement. As mentioned, many financial services organisations also play a role by having educational materials on their websites for their customers about how they can protect their information.

We generally support the recommendation to strengthen notification requirements, particularly for organisations that are currently exempt from the Privacy Act and not currently subject to robust regulatory scrutiny. We consider that there is merit in strengthening notification requirements for organisations transacting with children and teenagers. This is due to the fact that younger people may currently be transacting with businesses and not receiving any notification about what information is held about them and the information sharing processes of those businesses both within Australia and overseas.

We acknowledge that providers of financial services generally have robust notification processes to meet the requirements of APP 5 when they commence a business relationship with their customers and when they subsequently collect additional personal information. Examples of this include, but are not limited to, when a product disclosure statement is provided, when an account is opened, when a life insurance policy is obtained or when assessing a financial hardship application. We consider that individuals transacting with a financial services organisation generally would take time to consider their business relationship and view notification communications. Customers that have a business relationship with a bank, life insurer, or credit provider may be likely to expect that relationship to last many years. This longevity of business relationship contrasts to the time individuals would be likely to consider notification communications from businesses with which they have

a transient or brief relationship with such as when they are purchasing goods and services online or downloading a mobile phone application.

Currently, organisations that are not bound by the Act are not required to meet the APP 5 notification requirements which can result in customers not having the contact details or complaints process of those organisations if they have questions or concerns about the information handling practices of those organisations. We consider that if individuals are informed that businesses hold information about them via a notification process, this assists individuals understanding of the extent and cumulative nature of data gathering and sharing

We submit that financial service providers should not be subject to any additional requirements or limitations on using personal information, if the personal information is collected by a third party. Financial service providers are required to notify customers that their information is collected by third parties under APP 5 and so we consider sufficient and reasonable notice is provided to customers by financial service providers within a privacy policy and/or statement.

Consent to collection and use and disclosure of personal information

Question 26: Is consent an effective way for people to manage their information?

Question 27: What approaches could be considered to ensure that consent to the collection, use and disclosure of information is freely given and informed?

Question 28: Should individuals be required to separately consent to each purpose for which an entity collects, uses and discloses information? What would be the benefits or disadvantages of requiring individual consent for each primary purpose?

Question 29: Are the existing provisions effective to stop the unnecessary collection of personal information?

a. **If an individual refuses to consent to their personal information being collected, used or disclosed for a purpose that is not necessary for providing the relevant product or service, should that be grounds to deny them access to that product or service?**

Question 30: What requirements should be considered to manage 'consent fatigue' of individuals?

Response to Questions 26 to 30:

To be a valid consent, the consent must be:
- Voluntary,
- Informed,
- Specific ,
- Current, and
- Given by a person with capacity.

We consider that the 'current' elements of consent (set out above) should be reviewed to ensure that it makes it clear that consent lasts and is considered current until it is withdrawn or revoked, unless the consent is provided for a specific timeframe.

Where an individual claims under an insurance policy (which are long term contracts) we consider it sufficient if the insurer obtains the consent once and then uses the consent in line with legislative, regulatory and industry code obligations, which requires an insurer to assess an insurance application or claim using only relevant information.

Individual consents for each primary purpose would be unworkable for businesses providing multiple products and services for customers and would not be a good customer outcome for customers with long term business arrangements with financial services organisations. For example, an individual may obtain a superannuation or other investment product at age 18 and retain that product until age 65. It would not be appropriate to ask for a renewal of that consent each year or every few years. We consider that it would be unreasonable to present customers with multiple and/or excessive requests for consent during their business relationship with a financial services organisation such as during the entirety of the period that they hold a superannuation product, or during the assessment of a claim and throughout the period during which benefits are being paid on a claim.

Similarly, an individual transacting with a life insurance company may apply for an income protection product at age 25 and all relevant consents are obtained during the application and underwriting processes. The claimed condition may occur at age 30 with the individual receiving income protection benefit payments until age 65. Once again, the individual would not be expected to refresh their consent every year or every few years.

Financial services organisations are bound by numerous laws, regulations and industry codes that require us to collect, use and disclose personal and sensitive information and that if an individual refuses to provide a consent, or withdraws an existing consent, we may not be able to provide our products and services to them, or pay their benefits e.g. superannuation, banking and insurance products.

For organisations who are not insurers and not collecting sensitive data, consent would often not be an appropriate basis for collecting and using personal information where it is required for purposes such as under current laws relating to financial crime, including anti-money laundering and counter-terrorism financing, credit reporting, contractual reasons and so forth.

In addition, consent should only be required in circumstances such as the collection of sensitive information or if the collection will be for purposes unrelated to the primary purpose of collection.

Access, quality and correction
Question 45: Should amendments be made to the Act to enhance:

a. **transparency to individuals about what personal information is being collected and used by entities?**
b. **the ability for personal information to be kept up to date or corrected?**

Response to Question 45:

We consider that the Act currently provides sufficient transparency to individuals about what information is being collected and used by entities and the ability for personal information to be kept up to date or corrected.

We note the provisions of APP 10 and 13 regarding the quality of information and updating information and note that it is incumbent upon individuals to provide their updated contact information such as their phone, email and postal address to the businesses that they transact

with so that ongoing communications can be sent quickly and efficiently. As set out in our Executive Summary, we would recommend that any review of the Act, should challenge whether any simplification and consistency of provisions is logistically possible, such as combining APP 10 and 13 and making the "fair and lawful" provisions within APP 3 having wider implications, such as adding it to the APP 6 obligations.

We note the obligations on financial services providers to regularly communicate with customers to fulfil their legal and regulatory requirements such as sending statements and items such as lapse and cancellation notifications. Organisations rely upon their customers quickly notifying them about changes to previous contact details, for example, as the result of a marriage, divorce, moving house etc. We are also aware that customers may wish to change contact details if they consider that they have been compromised, such as a phone number or email address.

Increasingly financial services providers use secure portals for customers to log on using a password that they are asked to keep secure and generally, it is quick and easy for customers to change passwords if they have been compromised.

We note in the OAIC's NDB reports that a number of breaches result from organisations sending correspondence to an out of date email address or contacting a customer on a phone number that is out of use. As such, it may be prudent for both financial services organisations and the OAIC to publish reminders on websites about the importance of keeping contact details up to date to avoid sending personal and sensitive information to an unintended and unauthorised recipient.

Right to erasure

Question 46: Should a 'right to erasure' be introduced into the Act? If so, what should be the key features of such a right? What would be the financial impact on entities?

Question 47: What considerations are necessary to achieve greater consumer control through a "right to erasure' without negatively impacting other public interests?

Response to Questions 46 to 47:

We acknowledge that the current Act sets out the circumstances in which organisations can hold and retain information such as where there is a lawful authority to do so. The nature of the financial services industry is such that customers expect their information to be held securely and available for the organisation to review to provide ongoing products and services to their customers. An example of the benefits of retention of information, includes being able to leverage off information already known by a financial services organisation or group of companies to provide additional products and services to customers.

We submit that customers would expect this process to occur in a seamless manner without asking the customer to complete additional paper or online forms. If the financial services organisation already has the relevant PII they can simply request the customer to confirm it is correct e.g. obtaining details of a savings account with the same organisation that a cheque account is held for by the same customer.

Financial services organisations are generally regulated by ASIC, APRA, AUSTRAC and other regulators such as the Life Code Compliance Committee (**LCCC**) and as such we are required to retain, securely store and be able to access information about our customers and our

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).

In addition, 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.

Generally, individuals have a right to access information held by organisations about them and as such, financial services organisations are required to retain information to meet APP 12 access requests and to respond to complaints and litigation.

Due to the obligations set out above, we submit that any 'right of erasure' should not apply to information held by financial services organisations. This is supported by our statutory record retention obligations set out above, and that in most cases, financial services organisations will be able to demonstrate that the information is needed for the purpose it collected it (APP 11.3). In addition, section 21(2)(c) of the Insurance Contracts Act 1984 is particularly relevant for life insurers in respect to when certain disclosures are required to be made by customers when applying for insurance so that the insurer may underwrite the insurer's risk of providing cover. Any disclosures which the insurer ought to have known in the ordinary course of business are not required to be disclosed by the customer. This can be problematic for life insurers where a customer has completed an application for cover and disclosed a pre-existing condition or high risk lifestyle matter (i.e. smoking) which caused the application for insurance to be declined, if that customer re-applies for cover and does not (for whatever reason, which may not be intentional) disclose this information in the second application. If the information provided in the first application is erased then the insurer may not be able to rely on a non-disclosure remedy as the insured may argue that the insurer ought to have known that information and the insurer is unable to verify the non-disclosure.

Retention of information is also important regarding disclosures made during the application process for life insurance products. The life insurer may need to refer to those disclosures to consider whether the policy responds to the claim, or during the underwriting assessment for applications regarding additional cover. For example, if the customer had disclosed in an insurance application that they had suffered a recent knee replacement, and the insurer proceeded to issue cover, excluding knee conditions, the insurer needs to not erase this information so that it can pay valid claims (if the customer claims).

We acknowledge that there are obligations under APP 4 when information is unsolicited which may necessitate the information being destroyed, anonymised or de-identified.

It may be appropriate for the Attorney General's Department and OAIC to review the erasure of information provisions within the GDPR when reviewing similar provisions in the Act.

Question 48: What are the benefits and disadvantages of the current accountability approach to cross-border disclosures of personal information?

a) Are APP 8 and section 16C still appropriately framed?

Question 49: Is the exception to extraterritorial application of the Act in relation to acts or practices required by an applicable foreign law still appropriate?

Question 50: What (if any) are the challenges of implementing the CBPR system in Australia?

Question 51: What would be the benefits of developing a domestic privacy certification scheme in addition to implementing the CBPR system?

Question 52: What would be the benefits or disadvantages of Australia seeking adequacy under the GDPR?

Responses to Questions 48 to 52:

We consider that a review of the Act should take into account the cross-border requirements of privacy legislation in other jurisdictions, such as New Zealand and the EU, to take into account the global transactions of many contemorary businesses and the burden of needing to comply with different regulatory obligations, in those different jurisdictions. As a general rule, we consider that if an organisation is dealing with a jurisdiction that has comparable safeguards and data security principles to Australia, there should be no impediment to conducting business in that jurisdiction, as there is no significant increased risk to the privacy and data security of individuals and there iare methods to redress interferences of privacy in those relevant jurisdictions.

Enforcement powers under the Act and the role of the OAIC

Question 53: Is the current enforcement framework for interferences with privacy working effectively?

Question 54: Does the current enforcement approach achieve the right balance between conciliating complaints, investigating systemic issues, and taking punitive action for serious non-compliance?

Question 55: Are the remedies available to the Commissioner sufficient or do the enforcement mechanisms available to the Commissioner require expansion?

a) **If so, what should these enforcement mechanisms look like?**

Responses to Questions 54 to 55:

We consider that a review of the Act should take into account the enforcement powers, enforcement activities and reports published from time to time by privacy regulators in other jurisdictions, such as New Zealand and the EU, particularly in response to global challenges and identified threats to the privacy of individuals, such as the activities of cybercriminals and state actors.

Direct right of action

Question 56: How should any direct right of action under the Act be framed so as to give individuals greater control over their personal information and provide additional incentive for APP entities to comply with their obligations while balancing the need to appropriately direct court resources?

Statutory tort

Question 57: Is a statutory tort for invasions of privacy needed?

Question 58: Should serious invasions of privacy be addressed through the criminal law or through a statutory tort?

Question 59: What types of invasions of privacy should be covered by a statutory tort?

Question 60: Should a statutory tort of privacy apply only to intentional, reckless invasions of privacy or should it also apply to breaches of privacy as a result of negligence or gross negligence?

Question 61: How should a statutory tort for serious invasions of privacy be balanced with competing public interests?

Question 62: If a statutory tort for the invasion of privacy was not enacted, what other changes could be made to existing laws to provide redress for serious invasions of privacy?

Response to Questions 56 to 62:

We reiterate the inherent right to protection from unlawful or arbitrary interference with privacy contained within Article 17 of the International Covenant on Civil and Political Rights. As such, we consider that individuals should have a range of measures available to them to redress privacy breaches and to provide adequate remediation in response to any harm caused by such breaches.

It is acknowledged that this direct right of action is available to individuals in jurisdictions such as the UK, New Zealand, certain provinces of Canada and the EU. However, it can 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 have been identified and addressed by the relevant regulatory body.

We submit it is imperative that the relevant regulatory bodies are adequately resourced:

- to pursue and address privacy concerns raised by individuals in a timely manner: and
- to commence their own motion investigations if the regulatory body becomes aware or suspects that an organisation does not have an appropriate privacy and data framework based on its size and the type and extent of information that they handle.

Notifiable Data Breaches scheme – impact and effectiveness

Question 63: Have entities' practices, including data security practices, changed due to the commencement of the NDB scheme?

Question 64: Has the NDB Scheme raised awareness about the importance of effective data security?

Question 65: Have there been any challenges complying with the data breach notification requirements of other frameworks (including other domestic and international frameworks) in addition to the NDB scheme?

Response to Questions 63 to 65:

Since the commencement of the NDB scheme financial services organisations have implemented appropriate controls and processes in response to the NDB scheme requirements. These processes generally include, but are not limited to, the following:

- Updating and reviewing internal privacy policies and procedures to incorporate the provisions of the NDB scheme, based on the requirements of the NDB scheme and relevant publications from the OAIC;
- Implementing, reviewing and testing Data Breach Response Plans that are based on the requirements of the NDB scheme and relevant publications from the OAIC;
- Reviewing processes to identify, escalate, remediate and notify incidents and breaches, including the process to assess incidents and breaches against the eligibility criteria of the NDB scheme where there is a real risk of serious harm;
- Developing and reviewing notification communications to the OAIC and impacted individuals based on the requirements of the NDB scheme and relevant publications from the OAIC;
- Reviewing and rolling out training and reminders for staff to generate awareness of the NDB scheme and their responsibilities;
- Updating educational materials for customers on our websites to inform them of practical steps they can take to protect their information and steps they can take if they have concerns about their privacy, or wish to lodge a complaint; and
- Reviewing OAIC reports on the NDB scheme and subsequent updated OAIC guidance materials.

We consider that the NDB scheme has raised awareness regarding data security and that OAIC publications have assisted the general public to understand the types of breaches that occur and the root cause of those breaches such as cyber criminals deliberately hacking organisations in an attempt to obtain information for financial gain.

A number of financial services organisations operate globally and are subject to other data breach identification and notification schemes such as the GDPR which requires them to be fully aware of the obligations and eligibility criteria for each framework that applies to their business transactions.

An invitation for the Attorney General's Department and the OAIC to directly engage with the FSC on any proposed privacy law reforms following the consideration of this submission on the Issues Paper.

FSC members are interested in developments in Australian privacy laws and would be appreciative of the opportunity to directly engage with the relevant Government departments and agencies, including the Attorney General's Department and the OAIC on any proposed reforms. In the interim, if there are any points in this submission that require further explanation or detail, please contact me ( ) or, in my absence, – FSC Deputy CEO ( ).

Senior Legal Counsel