31st March 2023

Privacy Act Review Team
Attorney-General's Department
3-5 National Circuit
Barton
ACT 2600

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

Dear Privacy Act Team,

Privacy Act Review Report response

The Australian Financial Markets Association (AFMA) is responding to the Attorney-General's Department Privacy Act Review Report consultation. AFMA is the leading industry association promoting efficiency, integrity and professionalism in Australia's financial markets, including the capital, credit, derivatives, foreign exchange, energy, carbon, and other specialist markets. Our membership base is comprised of over 125 of Australia's leading financial market participants, including Australian and foreign banks, securities companies, state government treasury corporations, fund managers, energy firms, as well as other specialised markets and industry service providers. Financial services firms are centred on the protection and accurate processing of private data, so these updates are particularly pertinent to this sector.

Consequently, AFMA welcomes the opporunity to provide feedback to this consultation, following our previous submission in January 2022, which can be found here. AFMA was pleased to note that a number of our previous concerns have been alleviated and we welcome these revisions. However the proposals surrounding the following sections, remain largely unaltered: *4, 7, 12, 15, 19, 23* and *25*, in regard to which we also expressed concerns. Accordingly, our previous comments still stand in regard to these matters.

This submission is limited to addressing elements of the report and its proposals which were deemed relevant to the AFMA membership, please see the attachment for comments in detail and as they relate to each proposal. AFMA supports greater public rights and security over individual privacy. In this context after review of the privacy report we consider that certain proposals require greater consultation, alteration, clarity, and elaboration.

Overarchingly, we would also request that clarity be sought from the OAIC regarding timelines for the remainder of this consultation. Namely, when does the OAIC foresee these changes to the Privacy Act being implemented and will organisations have a grace period for implementation?

Broadly, AFMA also seek that consideration be made to the extensive pre-existing banking and financial services regulations and legislation, many of which already include requirements surrounding privacy and data, such as the *Corporations Act 2001*, also currently under review. We would therefore request that no overlap with such frameworks be made with the amendments to the Privacy Act.

With regard to proposals for small businesses, clarity as to whether this will encapsulate Foreign Authorised-Deposit Taking Institutions (Foreign ADIs) is required. Should Foreign ADIs be contained

Australian Financial Markets Association
ABN 69 793 968 987
Level 25, Angel Place, 123 Pitt Street GPO Box 3655 Sydney NSW 2001 Tel: +612 9776 7900 Facsimile: +612 9776 4488
Email: info@afma.com.au Web: www.afma.com.au

within the proposed coverage of small businesses in future, AFMA asserts that clear timeframes and compliance requirements be provided to those affected to allow Foreign ADIs to liaise with the offshore home office, upskill where necessary, ensure technological capabilities and safeguard compliance with their own internal privacy and data standards and pre-existing regulatory requirements. AFMA would be glad to contribute to the proposed impact analysis should Foreign ADIs be ringfenced for inclusion under small businesses.

Whilst not an Attorney-General's Department consultation, AFMA similarly recommended in our feedback on data releases regarding identity theft matters and in our submission to the Strategic Plan for the Payments System — for data breaches of a certain scale, data releases should be made available to all relevant essential service providers (banks, telecommunication firms, insurers, health care providers, etc.). Financial service firms want to play their part but the current inability to swiftly share information in light of a breach to protect customers, remains a key barrier.

AFMA would welcome the opportunity to discuss our comments further with the Attorney-General's Department, you can contact me via myoung@afma.com.au or 02 9776 7917.

Yours sincerely,

Monica Young
Policy Manager

ATTACHEMENT

Proposals

15. Organisational Accountability

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.

Further clarity on the role and responsibilities of the senior employee responsible for privacy are requested, including whether the employee needs to be based in Australia as opposed to offshore and to what extent oversight activities can be carried out offshore.

23. Overseas data flows

Proposal 23.1. Consult on an additional requirement in subsection 5B(3) to demonstrate an 'Australian link' that is focused on personal information being connected with Australia.

We agree with the proposal to add a requirement to confine the Act's extraterritorial application to offshore businesses 'carrying on business' in Australia but only in respect of their processing of information that is connected with Australia. It is critical that the language of this additional requirement makes it clear that an offshore entity subject to the Privacy Act is not regulated with respect to its processing of personal information that is not related to it carrying on of business in Australia, e.g., relating to personal information of its employees in its offshore office or its domestic offshore clients. To achieve this, the language of the additional requirement in section 5B(3) needs to link back to the carrying on of business in Australia, e.g., to use the wording set out on page 236 of the Attorney-General's Department's Report ("**AGD Report**"):

1. "the organisation or operator carries on business in Australia or an external Territory, and
2. **in doing so, processes personal information of individuals in** ~~that is *connected to* Australia~~ as a result of offering them goods or services or monitoring their behaviour in Australia.

Without this link back to the carrying on of business in Australia, the language proposed on page 236 could still operate so that an offshore organisation carrying on business in Australia is subject to the Act with respect to its processing of the personal information of an Australian citizen employed in its offshore office who has no involvement in the organisation's business in Australia. This would mean that a different standard of protection would attach to different nationalities within the same business, which would not be operationally feasible to implement. The benefit of using the EU GDPR language of "offering goods and services / monitoring behaviour" is that it is already widely understood and has been followed in several other countries, so this would provide organisations with certainty as to its interpretation.

We agree with the AGD that the Australian link requirement must also be expressed as an additional requirement to the 'carrying on business' test and not a standalone trigger for extraterritorial application. This will ensure that organisations which do not carry on business in Australia and are not established in Australia are not caught by the Act's extraterritorial application simply virtue of incidentally (i.e. not in a targeted way) processing personal information of individuals located in Australia or Australian citizens. In summary, it is not sufficient to simply require the personal information be "connected" with Australia as this is very broad and difficult to monitor. The Australian

link should be that the personal information is of individuals that reside in Australia, where the offshore entity has actively solicited that individual for the business it is carrying on in Australia. This would exclude, for instance, Australians who through reverse enquiry reach out to a US based entity for its products.

Proposal 23.2. Introduce a mechanism to prescribe countries and certification schemes as providing substantially similar protection to the APPs under APP 8.2(a).

Care should be taken so that organisations are not limited to relying on a single transfer mechanism such as prescribed countries in order to be able to transfer personal data offshore. There should be additional or alternative transfer mechanisms in place such as binding corporate rules, standard contractual clauses, consent, contractual necessity, and public interests. There should be a mechanism to recognise the regulations that offshore entities are bound by, such that these entities are not required to follow Australian privacy laws. This would avoid any potential conflicts of law issues and make it easier for the offshore entities to administer their compliance frameworks.

23.3 Standard contractual clauses for use when transferring personal information overseas should be made available to APP entities.

It is not entirely clear from the commentary in the discussion paper as to whether the proposed Standard Contractual Clauses **(SCCs)** are voluntary or mandatory. We support the introduction of voluntary SCCs as one of a selection of mechanisms for compliant international transfers, along with a flexible, 'substance over form' approach to SCCs, so that entities may choose either to implement the template Australian SCCs word for word, or for organisations that already have in place the SCCs developed by other jurisdictions (e.g., EU, UK etc., which will particularly apply for entities subject to the Act's extraterritorial application) they may rely on those foreign SCCs to the extent that they provide all the key protections offered by the Australian SCCs, and simply supplement those foreign SCCs to the extent there are any gaps.

28. Notifiable data breaches scheme

Proposal 28.2 (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.

Notification should be based on whether such a breach is likely to result in a high risk to the rights and freedom of the individuals. It should not be an automatic notification upon awareness of a data breach. If an organization is able to implement subsequent measures which ensure that the high risk to the rights and freedom of individuals are no longer likely to materialise, then the requirement to notify individuals can be dispensed with.