Australian Finance Industry Association Limited
ABN 13 000 493 907
L11 130 Pitt Street Sydney NSW 2000
02 9231 5877 www.afia.asn.au

The Manager

Regulation and Strategy

Office of the Australian Information Commissioner

GPO Box 5218

Sydney NSW 2001

19 November 2019

By email: consultation@oaic.gov.au

Dear Sir / Madam,

CONSULTATION – OAIC Privacy Safeguard Guidelines

The Australian Finance Industry Association [**AFIA**] welcomes the opportunity to comment on the OAIC's Draft Privacy Safeguard Guidelines for the Consumer Data Right Regime (the **Consultation Paper**_.

AFIA KEY POSITIONS SUMMARY

AFIA members recognise that customers' personal information is a valuable asset both for themselves and also the organisation(s) that handle it. As a critical and significant business asset, AFIA members afford customers' personal information the highest protection. AFIA is keen to work with the OAIC (as well as other relevant regulators or policy-reformers – including Treasury) to ensure data is used appropriately in the broader market, noting that data has a multitude of users.

At a macro level, AFIA supports the methodology underpinning the Consultation Paper and the potential it has to empower the OAIC to influence behaviour, through ensuring privacy safeguards are appropriately provided for so that individuals are not unnecessarily exposed to risks of harm when the Consumer Data Right (**CDR**) Regime comes into force next year.

AFIA encourages the OAIC to take a holistic and coordinated approach in this space – especially given the amount of change underway – for example, the Digital Platforms inquiry final report, various statutes being amended, multiple ASIC Regulatory Guidance reports being released at the end of 2019/early 2020. Such coordination will help drive a more consistent approach, improve the level of understanding amongst customers and businesses and reduce compliance uncertainty.

AFIA strongly believes that when data is used appropriately and in line with consumer consent or expectations, it has the potential to build, enhance and deepen customer relationships add more value which facilitates the development of better products and services to meet ongoing customer needs.

Further detail on AFIA and our position follows.

AFIA BACKGROUND

By way of background, AFIA is the voice of a diverse Australian finance industry. AFIA supports our Members to ensure a fair, equitable and competitive market for customers through representation, insights and connectivity. AFIA is uniquely placed to respond given our broad and diverse Membership of over 100 financiers operating in the consumer and commercial markets (including small-medium business and agri-finance).

AFIA members:

- include banks (major, regional and mutual/community-owned) and non-banks;
- range from ASX-listed public companies through to small businesses providing finance;
- operate via a range of distribution channels including bricks and mortar premises, intermediaries (finance brokers, dealerships, suppliers) through to online / digital access
- collectively operate across all states and territories in Australia in capital cities through to regional and remote areas: the majority operating across at least one border;
- have customers from all demographics, all age groups (legally able to borrow) in support of Australia's diverse and multi-cultural community with:
    - consumers ranging from high to low-income earners (including some whose main income source may be government welfare); many with substantial assets, others with few; single borrowers through to blended families; covering the whole range of employment scenarios, full-time, part-time, seasonal or casual employment.
    - commercial entities ranging from sole traders and partnerships through to the more complex corporates (e.g. trusts, corporate group) and government-entities, some with no employees through to others with hundreds (if not thousands) of employees.
- provide a broad range of products:
    - consumer: from personal unsecured loans, revolving products (including credit cards and interest free products coupled with lines of credit), loans secured by land or personal property; consumer leases of assets (including household/electrical/IT or cars) and buy-now, pay later solutions;
    - commercial: asset or equipment finance (finance/operating lease, secured loan or hire-purchase agreement or novated leases); working capital solutions (online unsecured loans;

debtor and invoice finance; insurance premium funding; trade finance; overdrafts; commercial credit cards) together with more sophisticated and complex finance solutions.

AFIA'S INSIGHTS - PROCESS

To examine this issue. AFIA has engaged with our Members. Our submission focuses on sections in the Consultation Paper where Members had some commentary or were seeking greater clarification.

A large number of members have contributed to our feedback. We note, however, that while Members have contributed to inform this response, from an organisational view, the positions being put by AFIA may not reflect every Member's specific position on all the issues. Their individual member viewpoint will get captured through the relevant member's organisationally-targeted submission.

AFIA KEY POSITIONS – DETAILED COMMENTARY

To explore our Key Positions in further detail AFIA provides the following insights shaped by operational input from our Members:

Recommendation 1 – Clarification on Privacy Safeguard 2

AFIA notes that in the Consultation Paper, when the OAIC refers to the application of Privacy Safeguard 2, it describes how organisations in the banking sector will be unable to deal with consumers on an anonymous basis. Members are concerned that, as currently drafted, this is not extended to the wider finance sector.

AFIA recommends:

*In the statement included after Section 2.13 on anonymity and pseudonymity in the banking sector, we recommend that this be extended to the financial services sector more broadly, to more clearly capture Accredited Data Recipients (**ADR's**) that are not ADIs.*

Recommendation 2 – Clarification on Privacy Safeguard 4

AFIA and its members note that it is unclear when reading the Consultation Paper as to whether Accredited non-ADI's are Data Holders or data recipients.

Further to this, members would like clarification on the obligations of a Data Holder that is not an ADI.

AFIA recommends:

AFIA recommends that the OAIC clarify whether Accredited non-ADI's are Data Holders and ensure that this is reflected across the whole Consultation Paper.

Recommendation 3 – Outsourcing of data

AFIA and its members note that specific consideration should be given to the outsourcing of data to a cloud storage provider, whereby the cloud storage provider only stores data and does not process it. In the Consultation Paper, it appears that a cloud storage provider may be seen as providing a service by storing the data, even though they are not providing any service to a customer and are only holding the data for a Data Holder/ADR.

Further, members have expressed concerns about what an overseas disclosure to a cloud storage provider (for example, Amazon Web Services (**AWS**)) would look like.

AFIA recommends:

AFIA recommends that the OAIC clarify that cloud storage providers are not providing services when they are only storing data. Further, AFIA recommends that further clarification and examples are provided on what compliant disclosure to an overseas cloud storage provider would look like.

Recommendation 4 – Privacy Safeguard 12- Right to Erasure of Data

Many organisations, especially those in financial services, have legal obligations to hold personal information for specific periods of time – for example under Anti Money Laundering / Counter Terrorism Financing requirements, responsible lending and other laws. Organisations also need to hold data for audit, taxation and legal reasons.

Given these requirements, the proposed obligation, under Privacy Safeguard 12, to delete all user data (which exceeds existing obligations) will be very complex to apply in practice.

Modern systems, that are cross-linked across various databases and create numerous backups, make it nearly impossible to completely remove user data.

Additionally, if an accredited data recipient were required to depart from existing methods of deleting database records, this would require major technical work. This would be extremely onerous, particularly for smaller ADR's.

Given these practical considerations, which are amplified when dealing with de-identified individuals, Members seek clarity on what is an acceptable definition of deletion.

The consequences of erasing all data is exacerbated when dealing, for example, with customer complaints and disputes. Deletion means it is not possible to investigate and review a customer's financial history and position and potentially prevents a customer receiving the outcome they desire.

AFIA recommends:

AFIA recommends, for the reasons outlined above, notwithstanding a customer's request to delete 'all data', a provision be included that allows entities to retain information if it relates to legislative, audit and taxation purposes. In such circumstances, it is proposed that service providers outline in writing to a customer what date has been retained and the reasons behind it.

Further, our Members have indicated that clarification would be needed on the following aspects of this recommendation:

- *What is an acceptable definition of 'deletion'*
- *Will deidentified data sets stored with a unique identifier in two different places be allowed, even if there is a possibility that the data set could be reidentified again?*
- *Can de-identified data be used for analytical purposes (provided it is stored in accordance with Privacy Safeguard 12)?*
- *How far will 'required under law' extend and how does it relate to key processes within financial services such as dispute resolution and underwriting assessments*

Recommendation 5 – Data Fields

AFIA and its members note that there is some uncertainty in the Consultation Paper as to whether drivers' licence numbers would be an excluded field.

AFIA recommends:

AFIA recommends that all excluded data fields are listed in the Consultation Paper.

Recommendation 6 – Notification

AFIA and its members note that there is some uncertainty as to whether providing a notification on the consumer's dashboard would be an accepted form of notification under Privacy Safeguard 5.

AFIA recommends:

AFIA recommends that the OAIC clarify in the Consultation Paper that notifications on a consumer's dashboard would comply with Privacy Safeguard 5.

Further, AFIA recommends that the OAIC provide clear examples of the forms of communication and level of detail needed in a notification

Recommendation 7 – Corrections of Data

AFIA and its members note that when reading through Privacy Safeguard 13, in particular the example provided in 13.23, whereby the data was to be pushed back to the consumer to notify the Data Holder to correct the situation as opposed to the ADR. There is inconsistency in saying a customer shouldn't have to go back and forth between a data holder and an ADR, however there are other parts of the Consultation Paper that suggests members should be doing that.

AFIA recommends:

AFIA recommends that that the ADR should go directly to the Data Holder to inform them that the information is incorrect and that the Data Holder will need to correct it. The consumer should be made aware and provided the appropriate notice under CDR rule 7.15, however the consumer need not be part of the conversation that the ADR and Data Holder have to ensure that the information is correct and up to date.

Recommendation 8 – Liability of Accredited Data Recipients

AFIA and its members note that the scope of the liability of ADR's needs further clarification.

AFIA recommends:

We recommend that the Consultation Paper further clarify the scope of the liability of ADR's. In particular, further clarity on section 56EK(2) of the Treasury Laws Amendment (Consumer Data Right) Bill 2019 Act is needed to provide for:

1) its applicability to be only where paragraphs 1(c), (e) and (f) do not apply; and
2) the limits of liability for those acting "on behalf of" the overseas recipient.]

Recommendation 9 – Further examples and visual aids needed

Finally, while AFIA and its members believe the Consultation Paper, as a whole, is largely clear and relevant, it would benefit from further examples and clarification.

AFIA recommends

We recommend the following is included in the Consultation Paper:

- *An example on consent in regards to Responsible Lending, and whether the withdrawal of consent may only be made at a point in time, or whether the data collected in the Responsible Lending assessment will need to be destroyed at the end of the time period of consent (say for example after 60 days).*

- *Flowcharts for Privacy Safeguards 6,7,8 and 9 on use and disclosure, due to the complexity of the rules*
- *Further examples and visual aids to clarify the above-mentioned recommendations*
- *Further examples and visual aids to explain better the ACCC released guidelines on accreditation, in particular on information security.*

NEXT STEPS

Should you wish to discuss our feedback further, or require additional information, please contact me at [redacted] or Chalisa Parekowhai, Associate Director, Policy at [redacted] or both via [redacted].

Kind regards

[redacted]

Karl Turner
Chief Operating Officer
Executive Director, Policy & Risk Management