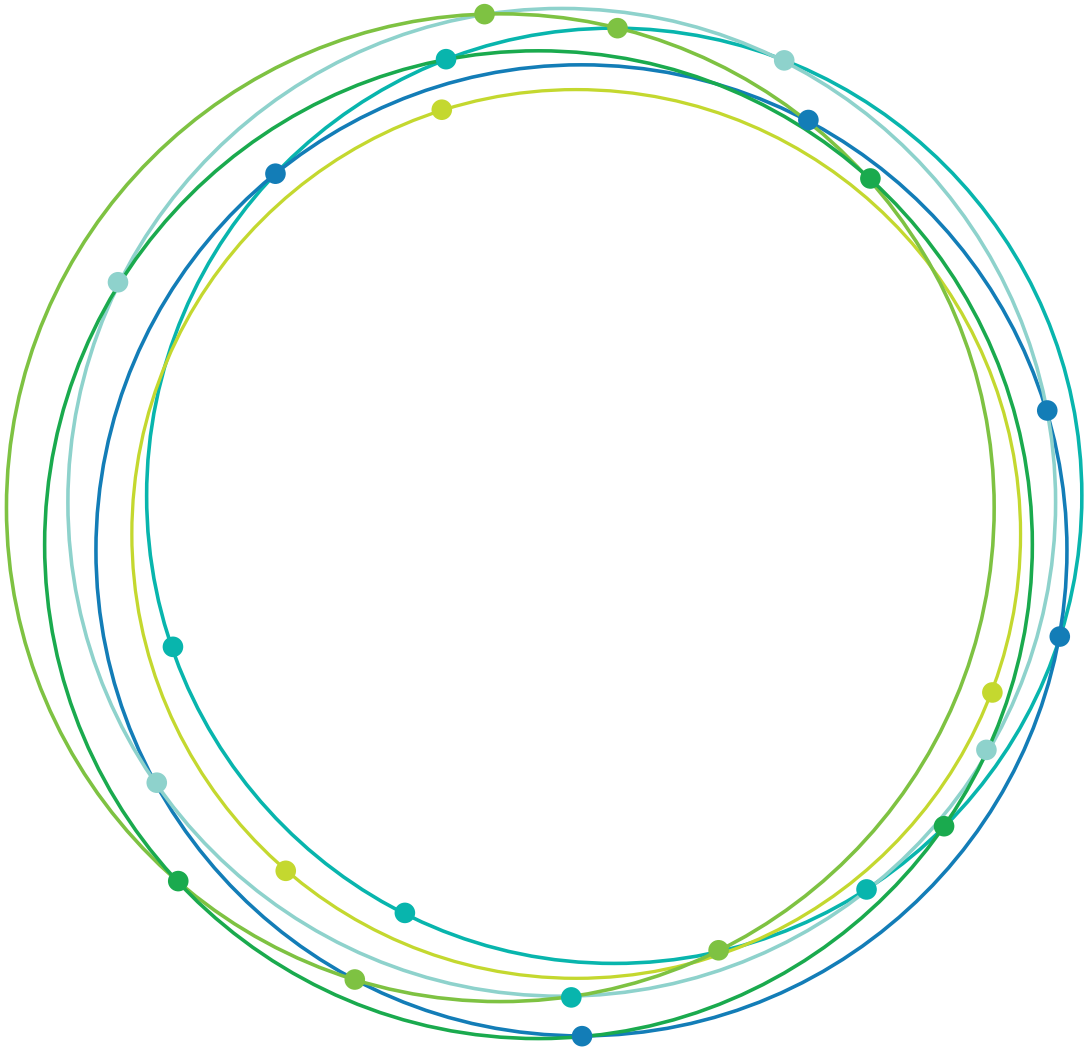
Deloitte.



Shaping the Future

Consumer Data Right

Deloitte Submission on the Consumer Data Right Rules Framework

12 October 2018

Introduction

On 11 September 2018, the Australian Competition and Consumer Commission (ACCC) released the Consumer Data Right (CDR) Rules Framework. This framework supports the implementation of the Consumer Data Right Bill, which is intended to encourage greater competition in the Australian economy. The ACCC has noted that it has adopted a phased approach to implementation under which CDR rules will be developed progressively. As a result, the Rules Framework focusses on the "matters that are essential for the commencement of Open Banking on 1 July 2019."[1]

The ACCC has invited comments on the Rules Framework. Deloitte is pleased to provide our observations in this submission.

The Rules Framework sets out the basis for an initial implementation of CDR for Authorised Deposit-taking Institutions (ADIs), and focusses on implementing what it has termed a 'minimum viable product' (MVP) for the commencement of open banking on 1 July 2019, with additional rules to be considered in further phases. In the consultation sessions, the ACCC has said that a MVP approach has been needed to meet the timelines set out by the Government for implementation of open banking.

We endorse this pragmatic approach to building out the rules, and understand the need to develop the rules progressively.

While there is merit in the ACCC's MVP approach to meet an implementation deadline, this approach also comes with costs and risks associated with uncertainty of scope. A lack of understanding of future requirements may result in additional technology and process costs for organisations as solutions are modified to accommodate subsequent changes to the rules or additional data sharing obligations.

Further context on key design considerations for future iterations of the rules, including the estimated timeframes for these changes, would enable market participants to adopt a strategic response to open banking and enable them to accommodate ongoing changes to their data architecture and API designs. This would reduce the risk of tactical solutions and minimise rework for CDR participants.

The key design principles should also cover areas of risk. An example of this would be ensuring that the CDR rules for data privacy are, at a minimum, at least as restrictive, if not more so, than what is set out in the Australian Privacy Principles (APP).

[1] Australian Competition and Consumer Commission, Consumer Data Right Rules Framework, 2018, page 10

In the Rules Framework consultation paper, the ACCC sets out the aim of the Rules Framework and its approach to rules development. The ACCC has invited comments on the content of the proposed rules, with stakeholder comments requested on a number of specific matters noted in the Rules Framework.

We have not commented on all of the matters noted by the ACCC. Our response to the Rules Framework includes comments on:

- CDR consumers (Section 3) – consideration should be given to the costs, potential benefits and likely usage arising from the extension of the CDR to former customers and offline customers.
- Data sets (Section 5) – The treatment of derived data is an important consideration. We support the exclusion from derived data of data resulting from "material enhancement". We also note that including a principle of reciprocity in the rules would help to address the uncertainty on what this concept includes or could include.
- Accreditation and data recipients (Section 6) – tiering of accreditation could be based on the attributes and the sensitivity of the CDR data being shared. Tiered accreditation of data recipients results in additional complexity for the implementation of the accreditation framework and may adversely impact the ability to implement open banking within the specified timeframes. The adoption of accreditation criteria in the banking sector presents an opportunity to leverage and build upon APRA's guidance for Data Risk Management (CPG 235) and the information security standard ISO27001.
- Consent (Section 8) – We agree with the concept that consents for sharing data from a joint account should reflect the authorisations for transfers of money from that account. The proposal to make rules that will prohibit the on-selling of CDR data and the use of CDR data for direct marketing would appear to conflict with the proposal to make rules that allow an accredited data recipient to use consumer's CDR data for a specific use for which the accredited data recipient has obtained express consent.
- Authorisation and authentication (Section 9) – The rules for the authentication process should prohibit the use and storage of sensitive personal identifiers. The introduction of intuitive capabilities to filter the data being shared could mitigate the risk of customers inadvertently 'oversharing' data through a lack of transparency on what is being shared.
- Privacy safeguards (Section 13) – The rules for unsolicited CDR data should reflect those set out in the GDPR with a period of 30 days for organisations to destroy or de-identify (so that it cannot be re-identified) CDR data. Whether the data is destroyed or de-identified (so that it cannot be re-identified), transparency of the outcome should be provided to the consumer. In addition we propose that the rules provide consumers with the right to specifically request that their data be destroyed (rather than de-identified).
- Reporting and record-keeping (Section 14) – the rules should provide clarity on the extent, if any, to which personal data should be retained for the purpose of keeping and maintaining records in relation to disclosures of CDR data directly to consumers, including response times.

The comments on the Rules Framework in our submission are intended to clarify aspects of the implementation, to be further detailed in the rules themselves, standards and the designation instrument for banking.

CDR Consumers (section 3)

Former customers and offline customers (sections 3.1 and 3.2)

The ACCC proposes that the first version of the rules extend the CDR to consumers who are:

1. current customers of that bank; and
2. have access to and use online banking.

The ACCC has requested comments on what would be a reasonable timeframe for extending the CDR to former customers and offline consumers.[2]

A core principle of regulation is that broadly defined benefits should be weighed against broadly defined costs. Consideration should be given to the practical ability for data holders to be able to provide data on former and offline customers and the mechanism(s) by which CDR data for former and offline customers is shared with these customers or accredited data recipients.

Customer records for former customers may be in a different format or recorded in different systems from those used for current customers. In addition, the authentication and consent mechanisms used for active, online customers may not be practicable for former customers.

The online consent process, axiomatically, will not apply to offline customers who request that their data be shared with third parties. As a result, the extension of the CDR to offline banking customers will require a manual process for both identity verification and consent.

Before extending the CDR to former customers or offline banking customers, consideration should be given to the costs associated with these additional processes compared with the potential benefits and likely usage. In addition, consideration should be given to whether existing data transfer mechanisms may adequately address this requirement. This regulatory impact assessment should be undertaken before deciding whether, and if so when, to extend the CDR to offline customers. This is particularly the case for offline former customers.

Additionally, the scope boundary for former and off-line customers requires clarification to accommodate scenarios where an active customer has a mix of active and inactive accounts and online and offline accounts. A potential approach could to be include all customer accounts that were active and on-line from a designated date (e.g. 1 July 2019), regardless of whether they are subsequently closed.

Data Sets (section 5)

Data Sets (section 5)

The ACCC has requested submissions on what metadata could be within scope, what benefits to consumers it could deliver if it was in scope, and what risks would arise and need to be managed.[3]

Meta data relating to transaction data could include:

- Transaction time
- Transaction currency
- Transaction exchange rate
- Transaction category (food & dining, fitness/leisure, utilities etc.)
- Transacting party (e.g. where multiple cardholders exist)
- Transaction channel (branch, ATM, direct debit, card payment, phone banking, BPAY, internet banking, mobile banking)

[2] Rules Framework (2018), Section 3, page 14

[3] Rules Framework (2018), Section 5, page 17

- Transaction location (for transactions via merchant, branch, ATM etc.)
- Counterparty name
- Counterparty details (e.g. industry classification)

This metadata enables potential users to develop and exploit a deeper and richer insight into a consumer's behaviour and identify opportunities to provide greater value for the consumer. This is potentially amplified as CDR is extended to other industry sectors.

- Additional counterparty/transaction details may enable identification of spend habits that could be assessed for competitive alternatives (e.g. utilities)
- Details on fees and charges such as exchange rates could enable identification of more beneficial foreign transaction options
- Transaction channel and location details could enable behaviour patterns (i.e. manual bill payments and associated extra fees and charges) that could be optimised via targeted recommendations.

However, we appreciate that additional data carries both additional burden and risk.

Many of the metadata fields proposed are already provided on customers' transaction statements. However, some may be embedded within transaction description fields but not actively maintained or co-located by data holders. This could potentially result in costly and time-consuming processes to extract and share this information to customers and accredited data recipients.

In addition, the inclusion in CDR data of information about the location and time of a transaction creates a higher risk profile from a data privacy perspective. The inclusion of this information would need to be permitted or constrained by the customer at the time they provide consent.

Furthermore, enriched counterparty details risk inadvertently exposing information about counterparty behaviours without their authorisation, particularly if aggregated over multiple (potentially de-identified) consumers.

Finally, richer data would potentially require data recipients to invest more time and effort to extract meaning from this data, particularly if pre-defined standards are not agreed to and implemented.

As such, we support the exclusion of metadata from the initial phase, to allow for consistency across this data to be addressed as well as addressing other potential barriers to sharing, and meaningful usage of, this data.

Derived data (section 5.2)

We endorse the need to distinguish between types of 'transformed' or 'value-added' data for the purpose of CDR data scope, and support the exclusion from derived data of data resulting from "material enhancement".

This protects the IP and assets built by data holders to apply transformation and analytics to enhance value from data.

Customer data (section 5.3.1)

The proposed rules for customer data note that "any unique identifiers associated with the listed items" will be within scope.[4]

The rules should specifically state that TFNs should not be requested or collected unless required under taxation, superannuation, or personal assistance laws as delineated in Privacy (Tax File Number) Rule 2015.

[4] Rules Framework (2018), Section 5.3.1, page 19

One of the use cases for Open Banking is price comparison. We note that the Rules Framework does not include in customer data, account data that defines how the product has been configured for a customer's account (including activated features and tailoring of fees). Without rules requiring disclosure of account configuration data, data recipients would need to rely on generic product information or estimate the account configuration from the associated transaction data.

This could lead to potential gaps in the information and limit the usefulness of data where customers have current discounts or special features in place.

However, we support the exclusion of account configuration data from the initial phase and consideration of its inclusion in a subsequent phase of open banking.

Transaction data (section 5.3.2) and Interaction with data standards (5.3.4)

The ACCC has noted that a "principle underlying the specification of transaction data is that data relating to transactions made by the CDR consumer in relation to the relevant products will be within scope. … A further principle is that transaction data should include, at a minimum, data that is available on a consumer's bank statement."[5]

We support these principles. However, the ACCC briefing noted that these data sets are not standardised across financial institutions.

In order to assist in managing quality, consistency and effective use of CDR data, we recommend that standardised reference data and supporting hierarchies for key data elements be specified for both data holders and data recipients. The standards will need to address data set standardisation, and data holders will need to address how they map their data sets to this standardised reference data as part of their data sharing mechanism.

Reciprocity (Section 5.4)

The introduction of data sharing is intended to encourage greater competition. This competition could come from new entrants from outside a designated sector, including from organisations operating in the technology sector.

The Explanatory Memorandum to the draft CDR Bill defined the principle of reciprocity:

> *"When in possession of a consumer's CDR data, an accredited entity can also be directed by a consumer to provide that data to other CDR participants."*[6]

The definition of reciprocity in the Explanatory Memorandum only refers to an entity sharing data they have received. It does not refer to providing 'equivalent data'.

The Farrell Report noted, in the context of banking, that:

> *"it would seem unfair if banks were required to provide their customers' data to data recipients such as FinTechs or non-bank credit providers, but those data recipients were not required to reciprocate in any way, merely because they were not banks and therefore did not hold 'banking' data."*[7]

It went on to recommend that:

> *"Entities participating in Open Banking as data recipients should be obliged to comply with a customer's direction to share any data provided to them under Open Banking, plus any data held by them that is transaction data or that is the equivalent of transaction data."*[8]

---

[5] Rules Framework (2018), Section 5.3.2, page 20
[6] Exposure Draft Explanatory Materials, paragraph 1.46, page 12
[7] The Australian Government, the Treasury, Open Banking: Customers choice convenience confidence, December 2017 (Farrell Report), page 43
[8] Farrell Report (2017), op. cit., Recommendation 3.9 page 44

While acknowledging the potential for sector creep, the Farrell Report recommended that:

> *"as part of the accreditation process for data recipients that do not primarily operate in the banking sector, such as data recipients from the technology sector, the competition regulator should determine what constitutes equivalent data for the purposes of participating in Open Banking."*[9]

The Rules Framework notes that:

> *"In the ACCC's view the concept of reciprocity raises complex issues requiring further consideration. The ACCC therefore does not propose to make any rules regarding reciprocity in the first version of the rules."*[10]

There appears to be a range of views on what the concept of reciprocity involves which differ based on when it applies, and what data it applies to.

	Concept of reciprocity	**Comments**
1	An organisation receiving CDR data is obliged, at the request of a consumer, and ***at the time that the obligations of a data holder apply*** to that organisation, to provide to an accredited third-party data recipient, the CDR data it received and any other CDR data it holds.	This concept of reciprocity would be the simplest to apply within the timeframes set out for the implementation of open banking. For the first 12 months this would result in the four major banks being the only data holders required to share CDR data. Other accredited data recipients (non-major ADIs and non-ADIs) would be able to receive data but would not be required to share CDR data.
2	An organisation receiving CDR data is obliged, at the request of a consumer, and ***at the time that the obligations of a data holder apply*** to that organisation, to provide to an accredited third-party data recipient, the CDR data it received and any other CDR data it holds ***and any data that is the equivalent of CDR data***.[11]	This concept of reciprocity requires that 'equivalent data' be defined in the rules. For non-ADIs consideration should be given both to what constitutes equivalent 'customer-provided' data and to what constitutes equivalent 'transaction' data.
3	An organisation receiving CDR data is obliged, at the request of a consumer, and ***at the time it receives CDR data***, to provide to an accredited third-party data recipient, the CDR data it received and any other CDR data it holds.	This concept of reciprocity requires that any organisation can only participate in CDR as an accredited data recipient if it also is willing to provide data. For the first 12 months there is a risk that this approach to reciprocity would result in only a limited number of CDR participants, perhaps only the four major banks. This is NOT consistent with the principle of encouraging greater competition.
4	An organisation receiving CDR data is obliged, at the request of a consumer, and ***at the time it receives CDR data***, to provide to an accredited third-party data recipient, the CDR data it received, any other CDR data it holds ***and any data that is the equivalent of CDR data***.[12]	As for (3). In addition this concept of reciprocity requires that 'equivalent data' be defined in the rules. For non-ADIs consideration should be given both to what constitutes equivalent 'customer-provided' data and to what constitutes equivalent 'transaction' data.
5	An organisation holding CDR data is entitled to request or obtain data from an accredited data recipient before sharing data it has been directed to share by a CDR consumer.[13]	The Rules Framework has stated that this is NOT what is meant by the principle of reciprocity.

While the extension of the principle of reciprocity to non-ADIs does potentially raise complex questions in relation to the identification of equivalent transaction data, it is possible for the rules to outline a principle of reciprocity that would apply to CDR participants and CDR data.

[9] Farrell Report (2017), op. cit., page 44
[10] Rules Framework (2018), Section 5.4, page 22
[11] Farrell Report (2017), op. cit., page 44
[12] ibid
[13] Rules Framework (2018), Section 5.4, page 21

Consideration could be given subsequently to extending the definition of data to be shared to equivalent 'customer-provided' data held by non-ADIs. It would also be possible subsequently to including sharing of relevant equivalent 'transaction' data, to the extent to which this exists and can be defined.

Including a principle of reciprocity in the rules would help to address the uncertainty on what this concept includes or could include.

Accreditation and data recipients (section 6)

Accreditation (section 6)

The Rules Framework notes that rules will be developed related to granting, suspending and revoking accreditation.[14]

Rules may also be required to ensure ongoing performance against accreditation criteria. This may take the form of ongoing periodic review by the Data Recipient Accreditor and / or attestation by the data recipient.

Proposed Rules for accreditation (section 6.2)

The ACCC has requested views about the types of tiers that it would be useful and practical to implement for accreditation of data recipients, having regard to existing business models and likely use cases for CDR data. In addition, the ACCC has requested views about the basis on which lower tiers could be restricted and the way in which these limitations would reduce risks relating to the collection, storage or use of CDR data and therefore provide a basis for reduced accreditation requirements.[15]

The Farrell Report recommended the implementation of a tiered accreditation model, under which "parties would be accredited to receive and hold data, based on the potential harm that the relevant data set and that party pose to customers, and to the Open Banking system."[16]

The Farrell Report noted, "Tiered accreditation would allow for a more flexible application of the burden of accreditation."[17]

If tiered accreditation were adopted, potential options to consider for definition of lower tiers include:

- Tiering based on the ***attributes*** of the CDR data being shared, e.g. basic customer information (including account credit limits and opening/closing account balances) could be an example of a limited data set available to a lower tier accredited CDR participant. This could be supported by the definition of standard subsets of data attributes to be made available to lower tier participants. A subset of data may exclude higher risk data attributes, resulting in a lower risk profile for the provision of the limited data set.
- Tiering based on the ***sensitivity*** of the CDR data being shared. This would allow for higher accreditation requirements for data recipients receiving data sets that have data that are more sensitive or that include sensitive data attributes such as data from minors or, at a future point, health data.
- Tiering based on ***standardised*** and/or ***approved uses*** of CDR data e.g. lower tier participants may be eligible to receive CDR data for purposes such as proof of income / expenditure or to summarise monthly expenditure by merchant type. The tiered accreditation could be

[14] Rules Framework (2018), Section 6, page 22
[15] Rules Framework (2018), Section 6, page 22 and Section 6.2 page 25
[16] Farrell Report (2017), op. cit., page 24-25
[17] Farrell Report (2017), op. cit., page 25

restricted to a set of use cases that might be considered lower risk for consumers, e.g. aggregation of data. However, we note that the Farrell Review did not recommend accreditation based on the proposed use for the data, noting, "customers must be able to choose the purpose of that transfer, without interference from regulators or data holders."[18]

However, as noted above, a core principle of regulation is that broadly defined benefits should be weighed against broadly defined costs. Tiered accreditation of data recipients results in additional complexity for the implementation of the accreditation framework and may adversely impact the ability to implement open banking within the specified timeframes.

Criteria for general level of accreditation (section 6.2.1)

The Rules Framework notes that the "ACCC considers that the criteria for accreditation should be objective, to the extent possible, related to the security and integrity of the CDR regime and primarily directed towards ensuring that applicants demonstrate their capacity to manage CDR data in accordance with the privacy safeguards."[19]

Specifically, the ACCC proposes to make rules that specify the steps an accredited data recipient must take to protect CDR data from misuse, interference, loss or unauthorised access, modification and disclosure.[20]

The ACCC has requested views on certification against industry standards that may be appropriate to recognise in the rules as evidence of this criterion in the accreditation process. [21]

The adoption of accreditation criteria in the banking sector presents an opportunity to leverage and build upon APRA's guidance for Data Risk Management (CPG 235).

The inclusion of rules requiring certification to CPG235 would require ADIs and other accredited data recipients to demonstrate compliance with the following aspects of data risk management in relation to their CDR data:

1. The adoption of a systematic and formalised approach for governing and managing customer data
2. Elevation of staff awareness around obligations (i.e. training programs)
3. Designing for every stage of the data lifecycle including Capture, Processing, Retention, Publication, and Disposal
4. Consideration of auditability, de-sensitisation, end user computing (including robotic process automation), and outsourcing and offshoring of data.
5. Ensuring that data is fit-for-use
6. Establishment of monitoring and exception management capabilities
7. Establishment of an appropriate assurance and review regime.

The ACCC could also consider rules requiring appropriate organisational and technical measures to comply with the Privacy Safeguards, in addition to "procedures and processes".[22] This includes ongoing information privacy obligations to maintain an accreditation that is developed by the ACCC along the lines of the ISO27001 accreditation program.

[18] Farrell Report (2017), op. cit., page 24
[19] Rules Framework (2018), Section 6.2.1, page 25
[20] Rules Framework (2018), Section 6, page 22
[21] Rules Framework (2018), Section 6.2.1, page 26
[22] ibid

Accreditation and Outsourcing (section 6.8)

The Rules Framework states that when an accredited data recipient engages an outsourced service provider the accredited data recipient remains "responsible and liable for compliance"[23] with CDR obligations and "liable for all CDR obligations they owe to their consumers, including those aspects that may be undertaken by an outsourced service provider."[24]

Ownership and responsibility will be instrumental to the success of open banking. This means that all those holding CDR data, including third party processors, should be accountable.

The rules should include the following elements that form part of the GDPR requirements.[25]

- Liability of all, including detail on determining the extent of liability of each party; and
- Mandatory requirement that a written agreement with the outsourced service provider include specific clauses to comply with the CDR before a CDR participant can engage the outsourced service provider.

To further strengthen accountability of third-party processors, consideration could be given in a future phase to requiring third-party processors to also be accredited as data recipients.

Ongoing information security obligations (section 6.9)

The ACCC has requested views about information security standards (particularly sector specific standards), compliance with which would demonstrate that an entity has in place adequate policies and systems in relation to risk management and security in relation to management of CDR data.[26]

A list of common security and data standards that could be applied to CDR participants is provided below:

- Australian Security Directorate Information Security Manual Principles / Controls
- ASIC REP 429 Cyber Resilience
- APRA's CPG 234 (Management of Security Risk in Information and Information Technology)
- APRA's CPG 235 (Managing Data Risk)
- ISO 15489-1 (International Standard for Records Management in a digital age)
- ISO 27001 series
- NIST Cybersecurity Framework
- Global Data Protection Best Practices (e.g. GDPR)

The ACCC should make a determination as to what standards apply. We note that the most common standards in commercial enterprises are ISO27001 series and NIST.

The ACCC should also make a determination as to the scope of application of those standards in relation to CDR participants. For example, ISO27001 allows a limitation of scope of application. However, no such limitation should apply in relation to CDR data or the underlying processes and systems.

The ACCC's determination may also extend to stating that all industry specific standards should apply to CDR participants. For example if CDR data is received from a financial institution that was required to apply CPG 235, the rules could state that the accredited data recipient is also required to apply those standards.

In addition, the rules should state that the scope of the standards must apply across all aspects of the data including people, process, technology and third parties.

---

[23] Rules Framework (2018), Section 6.8, page 30
[24] Rules Framework (2018), Section 12.1.2, page 50
[25] General Data Protection Regulation, Chapter 4, Controller and Processor
[26] Rules Framework (2018), Section 6.9, page 31

Consent (section 8)

Consent - Joint accounts and complex authorisations (section 8.1.1)

The ACCC has requested stakeholder views on the complexities of the issue of consent in relation to complex accounts and any other relevant scenarios. Specifically the ACCC has requested comments on how the rules should address alternative scenarios; that is, whether specific rules are needed relating to bringing data from complex accounts within the CDR.[27]

Joint owners

We agree with the concept set out in the Rules Framework that authorisation for transfers of data relating to a joint account should reflect the authorisations for transfers of money from that account.[28]

The rules should require that data holders ensure joint owners of accounts are properly notified, prior to the request for data transfer, so that each party is capable of presenting any potential infringements to their own rights.

Treatment of minors

The Rules Framework notes that the ACCC "does not propose to make rules that will treat minors differently to any other consumer who may take advantage of the CDR."[29]

Given the imbalance of power in transacting with minors, it is important to ensure that appropriate safeguards are in place. The GDPR notes "Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data."[30]

The rules for accreditation of CDR data recipients could include specific requirements for the handling of sensitive data received by accredited data recipients from minors. (Refer also to comments on section 6.2).

Consent should be time limited (8.3.1)

De-identification and destruction of redundant data

Refer comments on Safeguard 11

Authorisation period

The ACCC proposes to make a rule that would limit the period of authorisation provided to data holders to 90 days, noting that this is consistent with EU requirements under PSD2.[31] This is also consistent with the recommendation in the Farrell Report.[32]

In principle we support the adoption of rules that are consistent with international frameworks. A limit of 90 days on the period of authorisation to data holders is likely to be relevant to many use cases for open banking, including applications for credit or savings accounts.

The Farrell Report noted that some use cases, such as a personal budgeting app, "would be impractical without persistent authorisation because they require data to be updated regularly."[33]

Another potential use case for open banking is the provision of account aggregation services to consumers. These services are recurring and by nature are likely to extend beyond a 90-day period.

---

[27] Rules Framework (2018), Section 8.1.1, page 33
[28] Rules Framework (2018), Section 8.1.1, page 33 citing Farrell Report (2017), op. cit., Recommendation 4.7
[29] Rules Framework (2018), Section 8.1.2, page 34
[30] GDPR Recital 38 dealing with the specific protection of personal data of children
[31] Rules Framework (2018), Section 8.3.1, page 37 and Section 9.5, page 43
[32] Farrell Report (2017), op. cit., page 88
[33] ibid

A requirement for regular re-authorisation, particularly if the consumer needs to provide this to multiple data holders, may adversely impact the consumer experience for these services.

Where the nature of the service is typically recurring, the matter of authorisation period should be dealt with as a preference option at the time of consent. However, we advocate the maximum period before re-consent should be 180 days.

Direct marketing and on-selling of CDR data (8.3.3)

The Rules Framework notes that:

> *"The Open Banking review provided for a general freedom of use for any lawful use. The Government supported this approach, proposing to leave consumers free to determine what their data is used for, allowing for self-selection by consumers of agreed uses. It did not propose that consumers would be prohibited from granting consent to any lawful use, but acknowledge that additional use restrictions or regulation can be imposed if this becomes necessary".* [34]

The Rules Framework then notes that:

> *"As provided for in the consent process, the ACCC proposes to make a rule requiring accredited data recipients to identify to a consumer the uses to which the consumer's CDR data can be put, and obtain express consent to specific uses according to the consumer's wishes."*[35]

Notwithstanding this, the Rules Framework also proposes to make rules that will prohibit the on-selling of CDR data and the use of CDR data for direct marketing.[36]

The proposal to make rules that will prohibit the on-selling of CDR data and the use of CDR data for direct marketing would appear to conflict with the proposal to make rules that allow an accredited data recipient to use consumer's CDR data where it has obtained express consent to a specific use.

The rules should allow direct marketing or on-selling of data to occur where a CDR consumer has provided explicit consent to this specific use. The rules should also provide CDR consumers with the option to opt-out of continuing to receive direct marketing at any time that direct marketing information is received. This approach would be consistent with the GDPR principles.

Other matters

The approach of a rigorous consent scheme places the risk on the consumer, rather than the organisation.

The rules should require data holders to perform a risk assessment for cross-border data transfers, rather than allowing data holders to rely only on a rigorous consumer consent regime.

[34] Consumer Data Right Booklet page 6 as quoted in the Rules Framework, Section 12, page 48
[35] Rules Framework (2018), Section 12, page 48
[36] Rules Framework (2018), Section 8.3.3, page 39

Authorisation and authentication process (section 9)

Authorisation and authentication (sections 9.4 and 9.6)

The ACCC should consider rules for the authentication process that prohibit the use and storage of sensitive personal identifiers (e.g. Tax File Numbers, credit card numbers).

The ACCC may consider the introduction of an "opt in" configuration of data sets to be shared noting that:

- One customer may hold many accounts
- Each account has limits, balances, and transactions
- Transactions are made up of different types of transactions including merchant transactions, direct debits and credits, bill payments, fees and charges and account transfers.

The introduction of intuitive capabilities to filter the data being shared could mitigate the risk of customers inadvertently 'oversharing' data through a lack of transparency on what is being shared.

A practical alternative to this could be the introduction of sub-standards and associated API calls for specific purposes, which could reduce the burden on customers to correctly configure authorisations.

Privacy Safeguards (section 13)

Privacy Safeguard 4 – Dealing with unsolicited data

We support the approach set out in privacy safeguard 4 requiring accredited data recipients who received unsolicited CDR data to destroy or de-identify (so that it cannot be re-identified) the CDR data as soon as practicable.

In line with GDPR recommendations, we suggest that the rules set the practical period as 30 days.

We would also recommend that the rules include similar considerations to GDPR in the event that a data holder cannot meet the 30-day period.

Similarly, GDPR provides guidance on dealing with destruction of data held by intermediaries. We recommend that the ACCC follow the principles outlined in GDPR with regard to data that is no longer held for the purpose of providing the service or for any other relevant purpose.

This extends to data that has been acquired but whose use is no longer required, such as the scenario of 'coarse grained' data that has been refined. Any data that is no longer required to provide a service and which has no legal basis for retention should be destroyed or de-identified (so that it cannot be re-identified) within a reasonable period set at 30 days.

Privacy Safeguard 10 – Quality of data

Data Recipients may be unknowingly provided with incomplete data through the application of granular authorisations and the absence of account level detail (such as discounts or additional features).

The ACCC should consider whether a rule is required to enable data recipients to highlight to the consumer any gaps in the data received. This would pre-empt data completeness issues which have the potential to adversely impact the ability of the data recipient to deliver an outcome to the consumer for the agreed use of the data.

The ACCC may also wish to consider the introduction of rules for customer-collected data – using the authorisation process as an opportunity for customers to validate that the information is up-to-date and correct before it is shared.

Privacy Safeguard 11 – Security of CDR data

De-identification and destruction of redundant data

The rules could outline that CDR participants should clearly communicate with consumers whether CDR data is destroyed or de-identified so that it cannot be re-identified.

Additionally the rules should provide consumers with the right to explicitly request that their data be destroyed (rather than de-identified) given the extent to which data techniques allow for the potential of re-identification when new data sets are added. This should be provided as an option as part of consent and be made available thereafter.

The approach of destruction also needs to consider a situation where the data recipient is required to hold the data as a business record associated with decisions on the provision of a product or service. This could become increasingly challenging when shared data sets are used as the basis for a quote or service offering.

Reporting and recordkeeping (section 14)

The Rules Framework notes that data holders will be required to keep and maintain "records of any disclosures of CDR data directly to consumers, including response times".[37]

The rules should provide clarity on the extent, if any, to which personal data should be retained for the purpose of keeping and maintaining these records given the proposed rules requiring that data is destroyed or de-identified so that it cannot be re-identified.

[37] Rules Framework (2018), Section 14.2, pages 57 and 58

Contact us

Paul Wiebusch
Partner, Financial Services
[redacted]

Simon Pelletier
Partner, Strategy
[redacted]

Melissa Ferrer
Partner, Data
[redacted]

John O'Mahoney
Partner, Deloitte Access Economics
[redacted]

Jonathan Benson
Principal, Data
[redacted]

Michael Thomas
Director, Deloitte Access Economics
[redacted]

Tommy Viljoen
Partner, Privacy
[redacted]

Ilana Singer
Manager, Privacy
[redacted]

Alex Lord
Director, Conduct
[redacted]

Deloitte.