:86 400

Australian Competition and Consumer Commission
Via ACCC Consultation Hub

ACCC-CDR@accc.gov.au

8 May 2019

Submission by 86 400 Ltd in response to Competition and Consumer (Consumer Data) Rules 2019 – Exposure Draft

86 400 Ltd (**86 400**) welcomes the opportunity to provide feedback on the Exposure Draft of the Competition and Consumer (Consumer Data) Rules 2019 (**Rules**).

86 400 was founded in 2017 by Cuscal Limited (**Cuscal**) and is currently 100% owned by Cuscal. Cuscal in turn is largely owned by Australian challenger banks and customer-owned banks.

After conferment of a licence to operate as an authorised deposit-taking institution, 86 400 intends to offer a range of deposit and credit products. 86 400 will be a digital bank which intends to stay at the forefront of technology enabled banking services. 86 400 will be both a data holder and in due course will be an accredited ADI data recipient.

We appreciate the effort in producing a draft set of rules to cover the complex set of processes required to facilitate the Consumer Data Right. In this submission we have set out some areas where we feel the Rules may be improved or augmented.

1. **Process for the data holder to validate the status of an accredited data recipient.**

We would expect that this would be technically achieved by the register exposing an API to data holders. It may be the intention for this to be included in the Data Standard on "the processes for making product data requests and consumer data requests" but we think it would be useful to include a section within Division 5.3 of the Rules outlining the Registrar's responsibility in this regard.

2. **Mechanism for data holders to ensure continued accreditation status of accredited persons.**

The draft Rules provide detailed processes for the suspension and revocation of accreditation but they do not provide a process for communication of register updates to data holders. This is significant where a consumer has provided consent for a period of time. We would expect that the Registrar would need to make available an API or a regular file to data holders (at least daily) against which the data holder could wash its consents, to ensure that it does not continue to provide data to recipients who are no longer accredited. We suggest that the Rules include a communication process for updates to the register.

86400 Ltd
ABN 13 621 804 813

Level 1, 89 York Street
Sydney NSW 2000

3. Multi Party Disputes

We can envisage scenarios where consumers believe that a data breach of some kind has occurred but it is unclear whether the party responsible is the data holder or the accredited recipient (or its outsourced provider). In those circumstances there does not appear to be a mechanism to assist with dispute resolution. We would suggest that there be some obligation on participants to assist each other with dispute resolution and perhaps some instruction for consumers on their initial avenue of complaint.

4. Interactions between Parties

We note that proposed S56D of the *Competition and Consumer Act 2010* binds all participants to the Data Standards as if they were part of a multilateral contract. We think it appropriate therefore that the Standard provide certain details for the interaction between those parties. In particular:

(i) **Service Levels**: We note there are references to the Data Standards in respect of responses to customer data requests. We would expect that service levels be established for these responses within the Standards. We think that the Rules should cover the rights of a consumer for a failure to meet those service levels.

(ii) **Support for enhancement to API's:** We would expect the Data Standards to cover API enhancements and the requirements for data holders to support current and recent API versions.

(iii) **Mechanism for data recipient to gain access to data from the Data Provider:** Technically each data recipient will need to be allocated authorisation credentials by each data holder from which they seek access. The Rules do not currently provide for this and the proposed classes of Standards within Clause 8.1 do not appear to cover this mechanism.

(iv) **Establishment of different API end points to support CDR:** Data holders will need to establish different end points for API's depending on whether the data is product data or consumer data. We would expect the Standards to provide details of these. Product data may not require any credentials to be passed, while consumer data will.

5. Consent Expiry and Renewal (Rule 4.12)

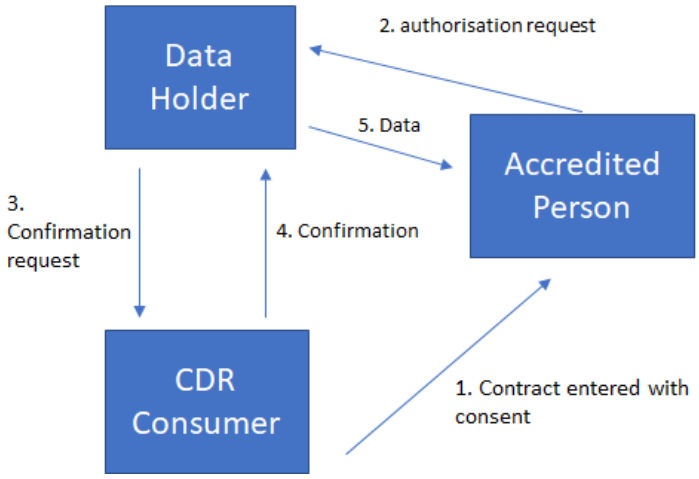
Under Rule 4.12 consumer consents expire after a maximum of 12 months. There is no mechanism in the Rules for the renewal of consents, so that a renewal would need to follow the original consent process. We do not think that is an efficient or desirable outcome for consumers in the context of a continuing service which the consumer has requested (e.g. the display of aggregated banking transaction details).

Figure 1 below illustrates the initial proposed consent process.

86400 Ltd
ABN 13 621 804 813

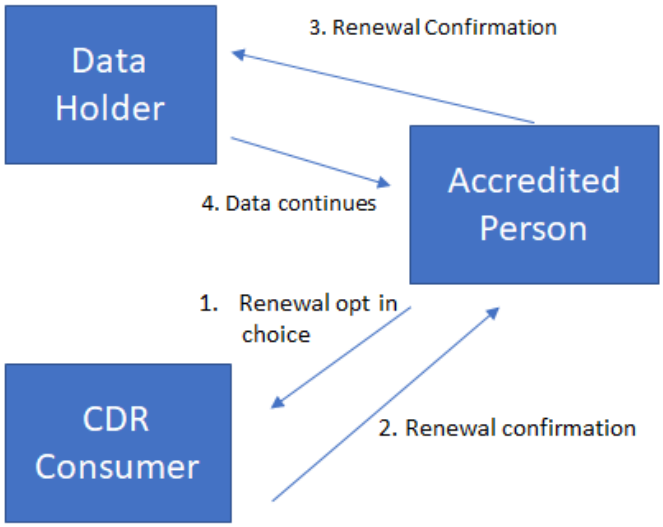
Level 1, 89 York Street
Sydney NSW 2000

Figure 1 . Initial consent process (per exposure draft)



While we accept the reasoning for consumers to update their consent, we believe that such updates are more efficiently transacted by the consumer directing their service provider (or accredited recipient) to confirm their consent with the data holder. This overcomes the need for another interchange between the consumer and the data holder. This proposed alternative is depicted in figure 2 below.

Figure 2 . Suggested consent renewal process



86400 Ltd
ABN 13 621 804 813

Level 1, 89 York Street
Sydney NSW 2000

The consumer will have provided their initial consent directly to the data holder, so when the data holder receives the renewal request it can still be satisfied that it is a legitimate renewal instruction from its previously identified customer.

Given that the accredited recipient is subject to stringent accreditation requirements, we think it reasonable that they be trusted to accurately pass on an individual's renewal of consent without the data holder having to re-obtain that consent.

We note that the consumer will be able to view their consents on both the accredited person and data holder dashboards and be able to withdraw consent any time.

6. Notification of current consent each 90 days (Rule 4.14)

We think that the Rules could specify what is meant by customer notification. For example, where a customer is a regular user of an account aggregation service, we believe it is intrusive for the service provider to have to remind the individual by email or SMS of their consent each 90 days. We think notification for an ongoing consent should be satisfied by:

(i) the accredited person displaying the user's consent status as "current" on a home page or access point for the service; and

(ii) Notifying the user by SMS or email if the user has not used the service for 90 days.

7. Joint Accounts (Part 3)

We think that the draft rules covering joint accounts are confusing and potentially conflicting and, if our interpretation of them is correct, will not provide a desirable outcome for consumers.

3.1 (1) of the draft Rules (page 89) gives each joint account holder the ability to make data requests and provide or revoke authorisations. Rule 3.2 allows the data holder to provide the functionality for joint account holders to perform those items together. We cannot see why a data holder would provide that functionality when it is always required to act on the instructions of a single joint account holder.

In our view the rules governing joint account holders should be consistent with the authority which the account holders have provided the data holder to operate their account (**Authority to Operate**). Typically, ADI's will designate accounts as "both to operate" if the Authority to Operate requires both parties to initiate or authorise a transaction or "either to operate" if either party can initiate or authorise a transaction.

We think that a "both to operate" instruction reflects the intention of the consumers to require both of them to be involved in important decisions involving their account. We submit this should extend to CDR requests and authorities. Either party should be permitted to revoke a jointly made consent or authorisation.

We recognise that this alternative could make implementation of a CDR consent management solution quite onerous and consideration may need to be given for "both to operate" joint accounts to be excluded from the definition of "required consumer data". That exclusion would affect a minority of joint accounts.

86400 Ltd
ABN 13 621 804 813

Level 1, 89 York Street
Sydney NSW 2000

We hope that these comments have been useful and would be happy to provide further explanation if that would assist the ACCC.

Yours Sincerely

Brian Parker
Chief Information Officer
[redacted]

Scott Jamieson
Head of Compliance
[redacted]

86400 Ltd
ABN 13 621 804 813

Level 1, 89 York Street
Sydney NSW 2000