

Data Standards Body

Technical Working Group

Decision Proposal 089 - Direct Consumer Access

Contact: James Bligh

Publish Date: 2nd November 2019

Feedback Conclusion Date: 17th January 2020

Context

Part 3 of the CDR rules ([found here](#)) outlines a requirement for CDR data holders to implement a **direct request service** through which an eligible CDR consumer is able to make a **consumer data request** to obtain some or all of their CDR data.

It is understood from this part of the rules that the **direct request service** has the following characteristics:

- The request can only be made by a consumer to obtain their own data
- The service does not need additional consent or authorisation. Once the identity of a consumer is confirmed they are implicitly authorised to access all available CDR data
- The rules require that the data be disclosed in human readable form
- The rules require that the data be disclosed but not that it be disclosed in a structured or exportable form (i.e. a visual, interactive representation is sufficient)
- Refusal to disclose in cases where harm may be caused is acceptable, but notification of this fact should occur
- Other specifics of the service are to be defined in the CDR standards (hence the requirement for this decision proposal)

This decision proposal articulates an option for inclusion in the CDR standards that will provide specifics for data holders to be compliant with Part 3 of the rules.

This decision proposal has been written to obtain community feedback prior to a recommendation for a final proposal being made to the Data Standards Chair.

Decision To Be Made

Determine the requirements for data holders under the standards to comply with the CDR rules pertaining to direct consumer access to CDR data.

Identified Options

As described above the CDR rules largely define the requirements for the **direct request service** under the CDR regime. As this service is consumer facing, however, the question remains as to how specific consumer experience requirements for this service should be.

For some parts of the CDR regime, where customer understanding and ease of use are critical, the DSB has defined explicit standards as well as additional guidelines outlining best practices for participants to take into account during implementation.

For the **direct request service**, this approach could again be taken. Alternatively, the standards could define the technical requirements for implementation but leave the consumer experience to data holders to determine.

The DSB is currently recommending that only technical standards for the **direct request service** be defined and that the consumer experience is left to the competitive space for the data holders to determine.

Current Recommendation

In light of the context and options discussions outlined above the following recommendation for the **direct request service** standards are as follows:

General requirements for the Direct Request Service

- Data Holders **MUST** provide a mechanism in their existing digital channels for a consumer to access CDR data that is associated with them.
 - Existing digital implementations that show CDR data are not considered sufficient to meet this requirement. The mechanism to meet the requirements of the **direct request service** **MUST** be dedicated for that purpose and this should be indicated as such to the consumer.
 - An entirely separate channel specifically for the **direct request service** **MUST NOT** be created unless the Data Holder does not currently offer a digital channel.
 - Data holders are not required to make this available through all of their digital channels (i.e. access via both web and mobile is not required) but all eligible CDR consumers **MUST** be able to access this service.
- Data Holders **MUST** authenticate consumers using existing mechanism utilised for their existing digital channels.
- In addition to normal authentication mechanisms Data Holders **MUST** perform an additional “proof of human” check to ensure that the access is not being automated. This check should be sufficient for the purpose but the specific type of check is left to the Data Holder to determine.

Data disclosure requirements

- When requested, CDR data MUST be disclosed visually in simple tabular form according to the structure of the payloads for the CDR end points
- Structural fields within CDR payloads (such as enumerations differentiation different data structures) do not need to be displayed. All designated CDR data MUST, however, be displayed.
- Data MUST be presented in raw form. Where this data would be confusing for a consumer explanatory information SHOULD be made available.
- Data labels for each field MUST be provided using language that will be reasonably understandable to the consumer.
- Data MUST be accessed interactively beginning with a high-level representation of the available data. Consumers MUST then be able to obtain more detail by clicking through into more detailed entities and structures in a way that is aligned with the defined CDR end points.
 - Wherever an ID is presented in the CDR end point payloads the ability for a customer to click through to the detail and data sets available using that ID MUST be available. The ID value itself is not required to be displayed.
- Data MUST be presented according to the categorisations and using the data cluster language defined in the CX standards. This provides an interested consumer with a clear understanding of the specific data being shared when they later authorise CDR data sharing.
- Data Holders SHOULD use the same underlying technical implementations that service data requests for Data Recipients to service the ***direct request service***.