CONSUMER
DATA
STANDARDS

Consumer Experience Standards

Document management

Approval

Version	Date	Approved by
1.4.0	17.07.2020	Data Standards Chair
1.3.0	17.04.2020	Data Standards Chair
1.2.0	31.01.2020	Data Standards Chair
1.0.0	30.09.2019	Data Standards Chair

Change log

For older versions and a detailed list of changes see the change log

Version	Date	Author(s)	Description of changes
1.4.0		MP, EC	**Standards:** Displaying of unavailable accounts **Guidelines:** Updating links, references, and minor points of clarification
1.3.0	17.04.2020	MP, EC	**Principles added** **Standards:** OTP clarification; displaying unavailable accounts; profile selection step, transaction details optional language defect corrected **Guidelines**: Replacement of existing consent amended; CDR logo and accreditation number in authorisation flow removed; minor corrections, clarifications, and updated references
1.2.0	31.01.2020	MP, EC, NG	Data cluster language defect amended; CDR branding and accreditation check guideline added; Other minor clarifications and amendments. Guidelines added for concurrent consent; rule 4.23; rules 7.4 and 7.9;
1.0.1	12.11.2019	MP, EC	'Account balance' permission added to basic scope; minor copy and design edits
1.0.0	30.09.2019	MP, EC, BC, NG	Update to incorporate: proposed CDR Rules; CX Standards; manage and withdrawal.

Key decisions

The below table contains a list of key decisions reflected in the standards and guidelines.

#	Area	Decision
1	CX Standards	The CDR Rules require a number of data standards to be made. These include CX Standards outlined in the CX Standards section, which form part of the overall data standards.
2	Consent	These guidelines allow for the provision of consent at the level of data clusters and meet the requirements of the CDR rules. Consultation and research have indicated that fine-grained control will be needed within the regime. Further consultation on how fine-grained control will be accommodated into the CDR regime will be undertaken. This will include further rounds of consumer experience research.
3	Authentication	The DSB has determined that a single, consistent, authentication flow will be adopted by the CDR regime. The redirect with one-time password model is incorporated into the standards as the proposed authentication flow.
4	Right to Delete	The CX Standards and Guidelines reflect Subdivision 4.3.4 in the CDR Rules on a consumer's right to deletion. These rules state that a CDR consumer may elect that their collected data, and any data derived from it, be deleted when it becomes redundant.
5	Amending Consent	The CX Standards and Guidelines do not not cover various amending consent scenarios, including re-authorisation. This position reflects current CDR Rules. Further CX work on amending consent is underway to test how consent can be amended and how flows might be simplified without compromising the quality of consent.
6	Concurrent Consent	The technical standards will support concurrent consents to allow more than one consent to be established, at the same time, between an ADR and a DH. The ability to establish concurrent consents supports ADRs to provide multiple use cases while being specific as to each consent's purpose. CDR participants should refer to the technical standards for details on when concurrent consent scenarios should be implemented.
7	Joint Accounts	Since v1.3.0, the CX Standards and Guidelines have supported the mandatory joint account requirements for November 2020 as outlined in the CDR Rules, based on the following: (1) the joint account management service (JAMS) is entirely in the DH space; (2) after a joint account is elected via the JAMS it appears in the authorisation flow in the same way as an individual account; and (3) 1 to authorise is mandatory, 2 to authorise is optional, and as such 2 to authorise is not covered in the standards/guidelines for November 2020 implementation.

Overview

Overview

In August 2019, the Australian government introduced a Consumer Data Right to provide individuals and businesses with a right to access specified data in relation to them held by businesses.

The Consumer Data Right will be designated sector by sector, beginning in the banking sector, followed by energy and telecommunications, with a view to have it apply economy-wide.

The Australian Competition and Consumer Commission (ACCC), supported by the Office of the Australian Information Commissioner (OAIC), is the lead regulator of the Consumer Data Right. The rules developed by the ACCC set out details of how the Consumer Data right works.

Breaches of the CDR Rules and certain privacy safeguards can attract civil penalties up to an amount specified in the Rules, capped at, for individuals, $500,000, or for corporations, the greater of $10,000,000; three times the total value of benefits that have been obtained; or 10% of the annual turnover of the entity committing the breach. Refer to the *Treasury Laws Amendment (Consumer Data Right) Act 2019* and the CDR Rules for more details, including which privacy safeguards breaches may attract civil penalties.

The Consumer Data Right requires common standards to be made to help consumers easily and safely share data held about them by businesses via application programming interfaces (APIs) with trusted, accredited third parties.

CSIRO's Data61 has been appointed as the Data Standards Body, designing the first iteration of open standards to support consumer-driven data sharing. The work is progressing through a technical working group and a consumer experience (CX) working group.

The CX Workstream exists to help organisations provide CDR consumers with simple, informed, and trustworthy data sharing experiences. CX Standards have been created to help achieve this along with the CX Guidelines, which are an example of how to put key data standards and CDR Rules into effect. CDR participants should refer to the CDR Rules for a complete list of requirements.

Following advice in the the Open Banking review, the CX Workstream has looked to the UK implementation of Open Banking and their accompanying CX Guidelines for reference.

The CX Guidelines cover:

- the process that a consumer may step through when consenting to share, manage, and withdraw access to their data;
- what (and also how) information should be presented to consumers to support informed consent; and
- particular language that should be used to ensure a consistent experience for consumers across the CDR ecosystem.

The outputs of CX research and consultation that led to the creation of these guidelines and standards can be found in these reports, and in public updates on this website. Formal consultation drafts and public submissions can be found on GitHub and the Consumer Data Standards website.

You can access major updates from the Data Standards Body in the standards section of our website, and by signing up to the Consumer Experience or Technical Working Group mailing lists.

Developing the CX Standards and Guidelines

The CX Guidelines and CX Standards have been developed for the Australian context through extensive consumer research, industry consultation, and in collaboration with key government agencies.

Over 250 research sessions have been conducted with over 240 unique participants across Australia. This research has influenced the content and form of the guidelines and standards.

In addition to these engagements the guidelines have been shaped by extensive collaboration across the Data Standards Body Workstreams (aligning with the API Standards and Information Security Profile) and across government with ACCC, OAIC, and Treasury.

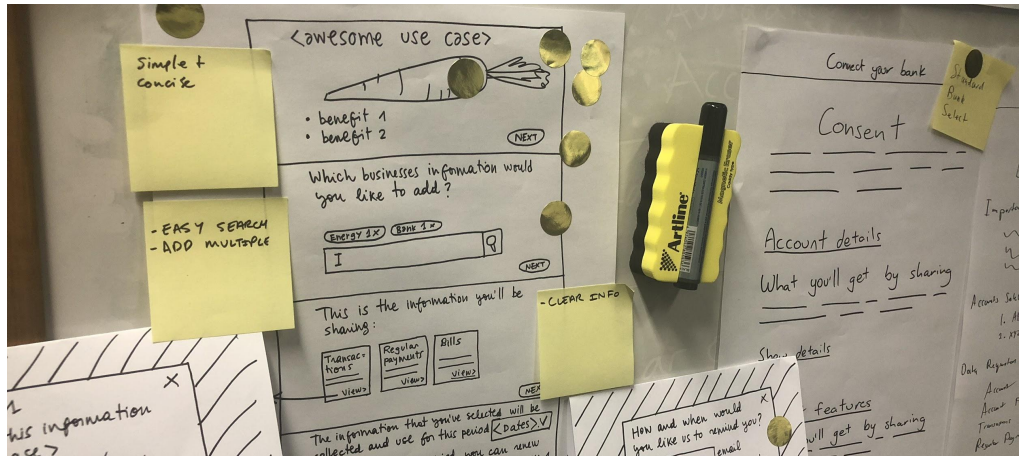
Feedback and guidance has also been provided by an Advisory Committee, spanning representatives from the financial sector, FinTechs, consumer groups, energy sector, and software vendors.

This document focuses on banking as the first designated sector and will be built on with further CX research and design activities.

The outputs of CX research and consultation can be found in these reports, and in public updates on this website.

They include:

- Phase 1 CX Research;
- Phase 2 CX Research:
  - Stream 1: consent flow, accessibility, joint accounts, cross sector data sharing
  - Stream 2: dashboards and withdrawal
  - Stream 3: consent flow, authentication models, reauthorisation, and notifications
- Phase 3 CX Reports;
- 5x industry workshops involving data holders, data recipients, ecosystem participants, consumer advocates, and government representatives.
- Formal consultation is conducted on the GitHub Standards and Maintenance pages as well as the Consumer Data Standards website.



CONSUMER DATA STANDARDS

Data Standards Principles

When the existing principles were defined the importance of consumer experience to the standards development process was underestimated. As a result, the existing principles are heavily focused on technical considerations and only a single outcome principle addresses CX.

Over the past year the Data Standards Body has used a range of principles and heuristics to guide the consumer experience work to date. These principles are now included in the standards alongside the outcome and technical principles.

OUTCOME PRINCIPLE 3

Data sharing provides a positive consumer experience

The standards will ensure that CDR consumers have simple, informed, and trustworthy data sharing experiences that provide them with positive outcomes over the short and long term.

CX Principle 1

The CDR is Consumer-centric

The CDR consumer experience is intuitive and is centred on consumer attitudes, needs, behaviours, and expectations – noting that these may change over time.

CX Principle 2

The CDR is Accessible and Inclusive

A diverse range of people are able to access, use, and comprehend the CDR ecosystem regardless of their background, situation, experience, or personal characteristics.

CX Principle 3

The CDR consumer experience is Comprehensible

When interacting with the CDR, consumers are able to understand the following:

- who their data is shared with;
- what information is shared;
- when sharing begins and ceases;
- where data is shared to and from;
- why their data is being requested; and
- how they can manage and control the sharing and use of their data

CX Principle 4

The CDR consumer experience is Simple and Empowering

Consumer interactions with the CDR are as simple as possible, but not at the expense of informed consent, consumer control, transparency, privacy, or comprehension. Consumers should be encouraged to be privacy conscious without experiencing cognitive loads that lead to disengagement. Consumers should also be empowered by the CDR without interactive burdens being placed on them.

CX Principle 5

Consumer Consent is Current

Consent is granted at a point in time and is only as current as the consumer's original intent. Consumer attitudes and behaviours may change over time and be impacted by external events such as the expansion of the CDR or consumer awareness. Consent terms should always align to current consumer preferences.

Consumer Experience Standards

Consumer Experience Standards

Version	Date	Approved by
1.4.0	17.07.2020	Data Standards Chair
1.3.0	17.04.2020	Data Standards Chair
1.2.0	31.01.2020	Data Standards Chair
1.0.0	30.09.2019	Data Standards Chair

The Data Standards Body (DSB) recognises that consumer adoption is critical to success for the CDR regime. To facilitate this goal the DSB has developed Consumer Experience (CX) Standards that identify a number of key elements to be aligned to across the regime.

The CDR Rules (8.11) require data standards to be made for:

- obtaining authorisations and consents, and withdrawal of authorisations and consents;
- the collection and use of CDR data, including requirements to be met by CDR participants in relation to seeking consent from CDR consumers;
- authentication of CDR consumers
- the types of CDR data and descriptions of those types to be used by CDR participants in making and responding to requests

As stated in the CDR Rules Explanatory Statement, accredited persons 'may be guided by the language and processes of [CX] guidelines and by consumer experience testing regarding consumers' comprehension of the consent process.' The DSB emphasises that aligning to the non-mandatory items in the CX Guidelines will help achieve consistency, familiarity and, in turn, facilitate consumer trust and adoption.

The obligations on CDR participants to apply the published standards commence on the commencement of the Consumer Data Right rules:

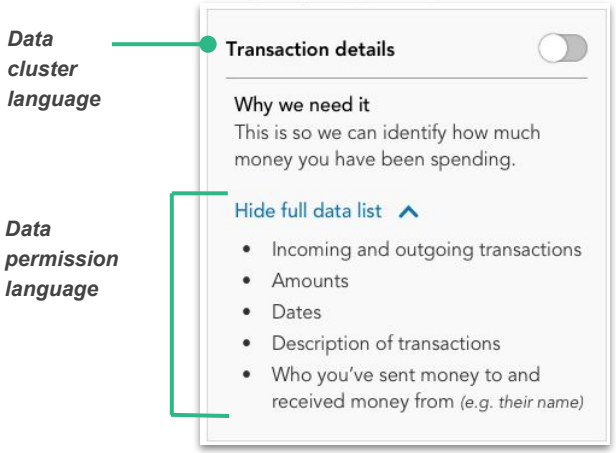
- where the rules require compliance with the standards, non-compliance with the standards may constitute a breach of the rules.
- where the standards are specified as binding standards as required by the Consumer Data Right rules for the purposes of s56FA of the legislation, they apply as under contract between a data holder and an accredited data recipient. The legal effect of binding standards as between data holders and accredited data recipients is fully set out in s56FD and s56FE of the legislation.

For CX Standards the key words **MUST**, **MUST NOT**, **SHOULD**, **SHOULD NOT**, and **MAY** are to be interpreted as described in RFC2119.

Consumer Experience Standards

Data Language Standards

In accordance with *CDR Rule 8.11(1)(d)*, a data standard must be made to provide descriptions of the types of data to be used by CDR participants in making and responding to requests. Adherence to this language will help ensure there is a consistent interpretation and description of the consumer data that will be shared across different CDR implementations.



Example of data language standards presented in a consumer-facing interaction

#	Area	CX Standard

1	**Data Language Standards:** Language to be used	Data Recipients and Data Holders **MUST** use data language standards to describe data clusters and permissions in consumer-facing interactions as outlined in *Table 1*
		• Data language standards **MUST** be used when CDR data is being requested, reviewed, or access to such data is withdrawn.
		• Data Recipients and Data Holders **MUST** use the appropriate data standards language for business consumers as denoted with an '*' in *Table 1*
		• Data Recipients and Data Holders **SHOULD** expand on the proposed language where appropriate to communicate further details of what is being shared.
		  ○ Additional details **MAY** include additional information in context, such as in-line help or tool tips, and/or additional permissions where they may exist.
		  ○ Examples of permission details that **MAY** be used and provided as in-line help are denoted with an '†' in *Table 1*

2	**Data Language Standards:** Detailed scope requests	If a scenario requires it, Data Holders and Data Recipients **MUST** merge and amend *Basic* and *Detailed* data cluster and permission language to show that *Detailed* scopes include *Basic* data. · Data Holders and Data Recipients **MUST** use the alternative language denoted with an '‡' in *Table 1* (rows greyed out for clarity). **Example:** A Data Recipient presents the *Detailed* data cluster in a data request to a consumer, but does not present the *Basic* data cluster. The *Detailed* scope includes *Basic* data, but this is not apparent to the consumer based on the data cluster language and permissions used for the *Detailed* scope.

Consumer Experience Standards

Data Language Standards

Table 1.
Individual consumer

Data cluster language	Permission language	Authorisation scopes
Name and occupation	Name; Occupation;	common:customer.basic:read
Contact details	Phone; Email address; Mail address; Residential address;	common:customer.detail:read
Name, occupation, contact details ‡	Name; Occupation; Phone; Email address; Mail address; Residential address;	common:customer.detail:read

Consumer Experience Standards

Data Language Standards

Table 1.
Business consumer

Data cluster language	Permission language	Authorisation scopes
Organisation profile*	Agent name and role; Organisation name; Organisation numbers *(ABN or ACN);*† Charity status; Establishment date; Industry; Organisation type; Country of registration;	common:customer.basic:read
Organisation contact details*	Organisation address; Mail address; Phone number;	common:customer.detail:read
Organisation profile and contact details*‡	Agent name and role; Organisation name; Organisation numbers *(ABN or ACN);*† Charity status; Establishment date; Industry; Organisation type; Country of registration; Organisation address; Mail address; Phone number;	common:customer.detail:read

Consumer Experience Standards

Data Language Standards

Table 1.

Data cluster language	Permission language	Authorisation scopes
Account name, type and balance	Name of account; Type of account; Account balance;	bank:accounts.basic:read
Account numbers and features	Account number; Interest rates; Fees; Discounts; Account terms; Account mail address;	bank:accounts.detail:read
Account balance and details‡	Name of account; Type of account; Account balance; Account number; Interest rates; Fees; Discounts; Account terms; Account mail address;	bank:accounts.detail:read

Consumer Experience Standards

Data Language Standards

Table 1.

Data cluster language	Permission language	Authorisation scopes
Transaction details	Incoming and outgoing transactions; Amounts; Dates; Descriptions of transactions; Who you have sent money to and received money from; *(e.g. their name)†*	bank:transactions:read
Direct debits and scheduled payments	Direct debits; Scheduled payments;	bank:regular_payments:read
Saved payees	Names and details of accounts you have saved; *(e.g. their BSB and Account Number, BPay CRN and Biller code, or NPP PayID)†*	bank:payees:read

Consumer Experience Standards

Accessibility Standards

In 2015, almost one in five Australians reported living with disability (roughly 18.3% or 4.3 million people). Making the Consent Model accessible will make consent simpler and easier for everyone.

This section refers to the Web Content Accessibility Guidelines (WCAG), which cover a range of recommendations to make content more accessible. Following these guidelines will help make content more accessible to a wide range of people with disabilities, but will also help make content more accessible to everyone. WCAG address accessibility of web content on desktops, laptops, tablets, and mobile devices.

CX Research 15, 16, 37

#	Area	CX Standard
3	**Accessibility**	At a minimum, all CDR participants **MUST** seek to comply with the following accessibility guidelines throughout the Consent Model. ● These standards **SHOULD** be assessed, tested, and refined further by accessibility consultants directly involved in implementation.
4	**Accessibility:** Content distinction	Data recipients and data holders **MUST** seek to have all aspects of the Consent Model comply with WCAG 1.4. This will make it easier to see and hear content, including separate foreground information from the background.
5	**Accessibility:** Keyboard functionality	Data recipients and data holders **MUST** seek to have all aspects of the Consent Model comply with WCAG 2.1. This will make all functionality available from a keyboard.
6	**Accessibility:** Pointer interactions	Data recipients and data holders **MUST** seek to have all aspects of the Consent Model comply with WCAG 2.5. This will make it easier to operate functionality using various input devices.
7	**Accessibility:** Reading experiences	Data recipients and data holders **MUST** seek to have all aspects of the Consent Model comply with WCAG 3.1. This will make text content readable and understandable
8	**Accessibility:** Input assistance	Data recipients and data holders **MUST** seek to have all aspects of the Consent Model comply with WCAG 3.3. This will help users avoid and correct mistakes.

Consumer Experience Standards

Consent, Authenticate, and Authorise Standards

#	Area	CX Standard
9	**Seeking consent**	Data recipients **MUST** notify consumers of redirection prior to authentication.
10	**Authentication:** 'One Time Password'	Data holders and data recipients **MUST** clearly refer to a "One Time Password" in consumer-facing interactions and communications. The use of the term "One Time Password" **MAY** be presented alongside an existing term used by a data holder (e.g. Netcode, one time pin etc.).
11	**Authentication:** Passwords	Data holders and data recipients **MUST** state in consumer-facing interactions and communications that services utilising the CDR do not need access to consumer passwords for the purposes of sharing data. The exact phrasing of this is at the discretion of the data holder and data recipient.
12	**Authentication:** Password link	Data holders **MUST NOT** include forgotten details links in redirect screens. The inclusion of such links is considered to increase the likelihood of phishing attacks.
13	**Authentication**: OTP expiry	Data holders **MUST** communicate the expiry period of the OTP to the consumer in the authentication flow.
14	**Authorisation** Account selection	Data holders **MUST** allow the consumer to select which of their accounts to share data from if the data request includes account-specific data and if there are multiple accounts available. The Data holder **MAY** omit this step if none of the data being requested is specific to an account (e.g. Saved Payees). Data holders **MAY** add a 'profile selection' step or equivalent prior to the account selection step if a single identifier provides access to different customer accounts. For example, one customer ID may give access to business customer and individual customer accounts. The 'profile selection' step **SHOULD** only be considered if it is an existing customer experience, and **SHOULD** be as minimal as possible to avoid introducing unwarranted friction (having regard to CDR Rule 4.24). ● If certain accounts are unavailable to share, data holders **SHOULD** show these unavailable accounts in the account-selection step. ○ Data holders **SHOULD** communicate why these accounts cannot be selected, and this **SHOULD** be communicated as in-line help or as a modal to reduce on-screen content. ○ Data holders **MAY** provide instructions on how to make these accounts available to share, and this **SHOULD** be communicated as in-line help or as a modal to reduce on-screen content. ○ *Note: Unavailable accounts are to be interpreted in accordance with the rules on eligible consumers and required consumer data.*
15	**Authorisation** Account confirm	Data holders **MUST** show which accounts the data is being shared from prior to confirming authorisation if the data request includes account-specific data. The data holder **MAY** omit this information if none of the data being requested is specific to an account (e.g. Saved Payees).

Consumer Experience Standards

Withdrawal Standards

#	Area	CX Standard
16	**Withdrawing consent**	If a data recipient does not have a general policy to delete redundant data, and the consumer has not already requested that their redundant data be deleted: ● Data recipients **MUST** allow consumers to elect to have their redundant data deleted as part of the withdrawal process prior to the final withdrawal step. ● Data recipients **SHOULD** consider prompting consumers to exercise this right at appropriate times (e.g. when inaction on the part of the consumer may cause them to lose the opportunity to exercise the right to delete their redundant data).
17	**Withdrawing authorisation:** Consequences	As part of the withdrawal process, the data holder **MUST** advise the consumer to review the consequences of withdrawal with the data recipient before they stop sharing their data. ● The data holder MAY consider using or paraphrasing the following message(s): ○ *'You should check with [Data Recipient] before you stop sharing to understand the consequences.'* ○ *'You should check with [Data Recipient] to see if your service will be impacted before you stop sharing.'*
18	**Withdrawing authorisation:** Redundant data	As part of the withdrawal process, the data holder **MUST** inform the consumer about the handling of redundant data and the right to delete. ● The Data Holder **MAY** consider using or paraphrasing the following message(s): ○ *'CDR data is either deleted or de-identified when it is no longer required.'* ○ *'[Data recipient] will have specific policies on how to handle your data once it's no longer required.'* ○ *'If you haven't already, you can ask [data recipient] to delete your data when they no longer need it, but you must do this before you stop sharing.'*

CONSUMER
DATA
STANDARDS

Data Standards Body | Consumer Experience Workstream

t +61 2 9490 5722

e cx@consumerdatastandards.gov.au

w consumerdatastandards.gov.au

www.consumerdatastandards.gov.au