CONSUMER
DATA
STANDARDS

Consumer Experience Guidelines

Document management

Endorsement

Version	Date	Endorsed by
0.9.5	16.07.2019	Chair of the Data Standards Body
1.0.0	30.09.2019	Chair of the Data Standards Body
1.2.0	31.01.2020	

Change log

Version	Date	Author(s)	Description of changes
0.9.5	15.07.2019	MP, EC, BC, MT	Working Draft CX Guidelines
1.0.0	30.09.2019	MP, EC, BC, NG	Update to incorporate: proposed CDR Rules; CX Standards; manage and withdrawal.
1.0.1	12.11.2019	MP, EC	'Account balance' permission added to basic scope; minor copy and design edits
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; For a detailed list of changes see the v1.2.0 change log

Requirement levels

The following conventions are used in this document as described in RFC2119.

Must – means an absolute requirement of this document.

Must not – means an absolute prohibition of this document.

Should – means there may exist valid reasons to ignore a particular item in this document, but the full implications need to be understood before choosing a different course.

Should not - means there may exist valid reasons when the particular item is acceptable or even useful, but the full implications need to be understood before implementing any item described with this label.

May - means that this is an informed suggestion but that the item is optional.

Key decisions

The below table contains a list of key decisions reflected in these guidelines and articulated in the technical standards

#	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. To indicate the direction of the CDR Rules, certain guidelines were listed as mandatory in v0.9.5 of the CX Guidelines. A number of these items have now been incorporated into the CDR Rules.
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 customer 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. Guidelines and standards for this authentication flow are contained in this document.
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. A consumer is able to make this election when giving consent, or, if they do not make the election at that point, at any other time before the expiry of their consent.
5	Re-authorisation	The CX Standards and Guidelines do not not cover re-authorisation. This position reflects the current CDR Rules. Further CX work is encouraged to provide further guidance on re-authorisation and to identify ways in which re-authorisation flows can be simplified without compromising the quality of consumer consent.

Contents

Contents

Contents

Contents

Contents

Glossary

Terms used in the CX Guidelines.

ACCC	*Australian Competition and Consumer Commission. ACCC is the lead regulator for the CDR regime.*
Accreditation	*The status provided to an organisation that has met the requirements to become an accredited data recipient.*
Authenticate	*When a consumer verifies themselves with a data holder.*
Authorise	*The act of a consumer consenting to the disclosure of CDR data by a data holder.*
CDR	*Consumer Data Right*
CDR logo	*Official Consumer Data Right branding to be provided by ACCC*
CDR rules	*Rules defined by ACCC, currently the Competition and Consumer (Consumer Data Right) Rules 2019, outlining how the consumer data right works.*
CDS	*Consumer Data Standards, technical advisor to the Data Standards Body.*
Consent	*Technically used to refer to when a consumer agrees to share their CDR data with an accredited data recipient for a specific purpose (i.e. collect and use); technically distinguished from the final affirmative action (i.e. 'authorise') in the Consent Flow. Consent is also used as a term in consumer-facing interactions to refer to sharing arrangements.*
Consumer	*An individual or business that uses CDR to establish a sharing arrangement.*
Consumer journey	*The stages a consumer moves through to establish a sharing arrangement. These include: pre-consent, consent, authenticate, authorise, and post-consent.*
CX	*The consumer experience (CX) that end users will have as they interact with the Consent Model and the CDR ecosystem.*
Data cluster	*The term used to refer to a grouping of data. 'Data cluster language' refers to the name of each group. See the Data Language Standards for examples.*
Data holder	*An organisation that holds a consumer's data.*
Data recipient	*An organisation that requests data (on behalf of a consumer) to provide a specific product or service.*

Glossary

Data sharing arrangement	*An instance of data sharing that a consumer has consented to and the terms that apply to this instance.*
Data request	*The stage where a data recipient asks the consumer to consent to share their CDR data. This includes the terms of the sharing arrangement, such as the duration and purpose.*
DSB	*The Data Standards Body. Mr Andrew Stevens was appointed as the first Data Standards Chair, and CSIRO's Data61 was appointed as the Data Standards Body to design the first iteration of open standards to support consumer-driven data sharing.*
Notification	*A notice sent to a consumer related to a data sharing arrangement.*
OAIC	*Office of the Australian Information Commissioner. OAIC has a number of roles in the CDR regime, including an advisory role, overview of the privacy protection elements, and consumer complaints handling once in operation.*
One Time Password	*A single-use password that is generated by a data holder and used by a consumer to authenticate.*
Permission	*The specific data in an authorisation scope is referred to as a permission. These are grouped by data cluster. See the Data Language Standards*
Purpose	*The reason(s) for the data request. The purpose specifies why the accredited data recipient needs the requested data to provide a product or service.*
Trust mark	*Official Consumer Data Right branding provided by the ACCC that may be used by an organisation to show that they are an accredited data recipient. Please refer to the CDR logo for more information.*
Value proposition	*A consumer's perception of the usefulness of a product or service offered by a data recipient.*
Wireframe	*An illustration of a page's interface that specifically focuses on space allocation and prioritisation of content, functionalities available, and intended behaviors.*
Withdrawal	*When a consumer stops a data sharing arrangement (i.e. 'consent/authorisation'). This can occur via a data recipient or a data holder. This was previously referred to as 'revocation'.*

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.

This right requires common data 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 four open work streams: API, Information Security, Engineering, and Consumer Experience (CX).

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 *CDR Rules (2nd September 2019)* into effect. CDR participants should refer to the CDR Rules for a complete list of requirements.

Following advice in the the Farrell report, 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 CX guidelines and design patterns in this document are provided as examples of how to put a range of key CDR rules into effect.

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 in consultation draft 1 and consultation draft 2, and in Decision number 87.

You can access major updates from the Data Standards Body in the standards section of our website, and by signing up to our 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 various government agencies.

In total, over 200 people across Australia and with diverse needs have been engaged in the CX research and their input has influenced the content and form of the guidelines.

In addition to this engagement with the community, the guidelines have been shaped by extensive collaboration across the CDS Working Groups (aligning with the API Standards and Information Security Profile) and across government with ACCC, OAIC, and Treasury.

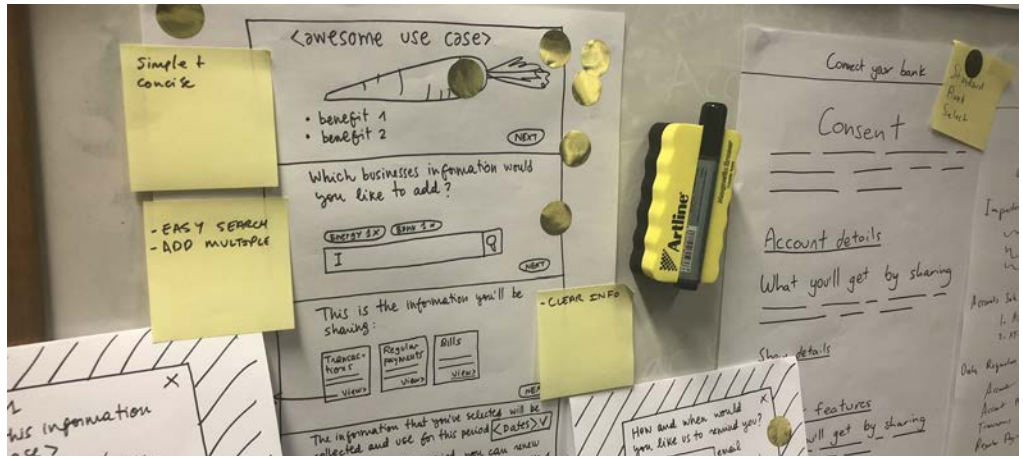
Feedback and guidance has also been provided by an Advisory Committee, spanning representatives from the financial sector, FinTechs, consumer groups, and software vendors.

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 that led to the creation of the DSB guidelines and CX Standards can be found in these reports, and in public updates on this website.

They include:

- Phase 1 CX Research on the consent flow;
- 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
- 4x industry workshops involving data holders, data recipients, and consumer advocacy groups.
- Formal consultation drafts and public submissions can be found in consultation draft 1 and consultation draft 2 and in Decision number 87.



CONSUMER DATA STANDARDS

How to use this document

The aim of the CX Workstream is to help organisations provide CDR consumers with simple, informed, and trustworthy data sharing experiences that provide consumers with positive outcomes over the short and long term. These guidelines are a manifestation of this intent and exist to help organisations participate in the CDR.

This document has been developed with data holders and data recipients in mind as the primary audience. These guidelines adopt an evidence-based approach and reflect leading practice design patterns to facilitate informed consent, enable consumer control, and to help build consumer trust.

The Key Decisions table contains important items reflected in the CX Guidelines and standards.

The Glossary contains key terms used throughout this document.

The Overview section details the process of developing the CX Guidelines and standards, and contains links to research reports, consultation drafts, and other CX Workstream artefacts.

The CX Standards table contain items that will be binding data standards for the purposes of s56FA and in accordance with the Consumer Data Right rules made by the ACCC. The making and commencement of the data standards and the CDR rules is subject to the Consumer Data Right legislation.

The body of the document contains detailed guidelines on how to put key CDR Rules and standards into effect for seeking consent, authentication, seeking authorisation, dashboards, and withdrawal of consents and authorisations.

The Appendix contains key CX Research references that informed the creation of the CX Guidelines and Standards.

The document contains three levels of requirement:

1 CDR Rule

A CDR Rule that **MUST** be followed. The rules referenced throughout the guidelines are detailed in the *Proposed CDR Rules*, published on 2nd September 2019.

2 CX Standard

A Data Standard that **MUST** be followed. These are outlined in Decision number 87, and in this document in the CX Standards section. These items will be binding data standards for the purposes of s56FA and in accordance with the Consumer Data Right rules made by the ACCC.

***NB** References are also made to technical data standards, including API standards and the Information Security Profile.*

3 CX Guideline

A guideline that **SHOULD** be followed. These are based on stakeholder consultation, heuristic evaluation, and CX Research findings. The CDR Rules Explanatory Statement include that 'it is expected that at a minimum, accredited persons will be guided by the language and processes of guidelines produced by the DSB.'

The key words **MUST**, **MUST NOT**, **SHOULD**, **SHOULD NOT**, and **MAY** are to be interpreted as described in RFC2119.

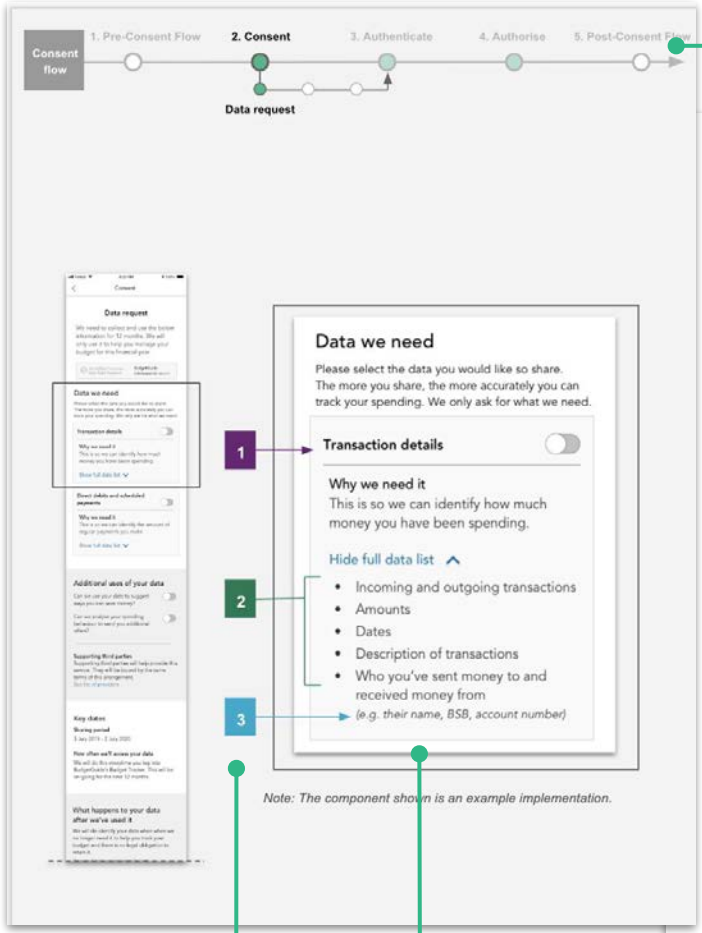
How to use this document

Wireframes are illustrated alongside rules, standards, and/or guidelines as examples of how to put key CDR Rules into effect.

Wireframes are presented as modular components to allow each component to be combined and deployed as appropriate.

The guidelines do not necessarily prescribe how to put the rules into effect, but aligning with these guidelines is recommended to help provide a consistent and familiar CDR ecosystem that consumers can trust.

The examples throughout these guidelines have been developed using a mobile-first approach to illustrate how information may be presented on a small screen. All CDR implementations must align to the rules and standards.



The navigation bar indicates the step the page relates to.

Consent Model Step | Section

Specific component

CDR Rule

1 CDR Rule that **MUST** be followed.

CDR Rule reference

CX Standard

2 Data Standard that **MUST** be followed.

Standards and/or CX reference

CX Guideline

3 CX Guideline that **SHOULD** be followed.

CX reference

Wireframes contain colour-coded numbers that correspond to CDR Rules, Data Standards, or CX Guidelines.

Each page refers to a specific step, component, or concept.

CONSUMER DATA STANDARDS

Consumer Experience Standards

Consumer Experience Standards

Version	Date	Endorsed by
1.0.0	30.09.2019	Chair of the Data Standards Body
1.2.0	31.01.2020	

The Data Standards Body (DSB) recognises that consumer adoption is critical to success for the CDR regime. This is particularly true in the early stages of implementation when consumers will not be familiar with the mechanisms and protocols required to engage with CDR participants and consent to share their CDR data.

To facilitate CDR adoption the DSB has developed Consumer Experience (CX) Standards and Guidelines that identify a number of key elements to be aligned to across the regime.

CDR Rules (8.11) also 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, 'at a minimum, accredited persons will be guided by the language and processes of guidelines produced by the DSB.' The CX Workstream 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.

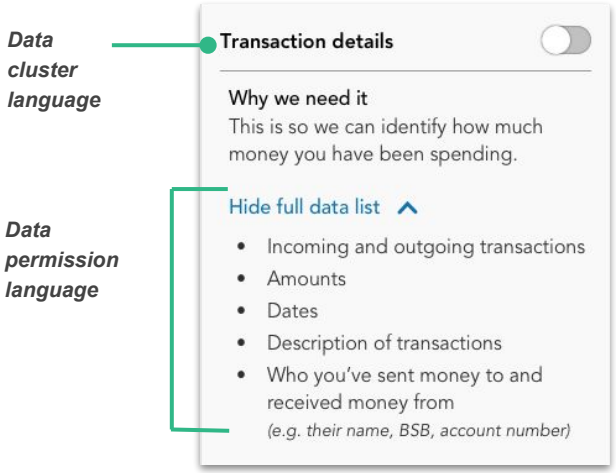
The CX Guidelines avoid being prescriptive to balance ecosystem consistency with the potential to innovate. The complete list of binding Consumer Experience Standards outlined in this section were created to balance these objectives. The CX Standards are available as a standalone document.

CX standards will be binding data standards for the purposes of s56FA and in accordance with the Consumer Data Right rules made by the ACCC. The making and commencement of the data standards and the CDR rules is subject to the Consumer Data Right legislation.

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, BSB, account number)†*	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 'verification code' and 'password' caused confusion and apprehension among consumers.
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). ● 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.
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.'*

Consent

Consent

Consumer consent to share data is central to the Consumer Data Right. Consent-driven data sharing will give consumers more control of their data, encourage more privacy conscious behaviour, and provide a more positive data sharing experience for consumers.

The CDR Rules propose a number of requirements in relation to consent, within which the practical guidance on consent design must sit.

An accredited data recipient **MUST** present each consumer with an active choice to give consent, and consent **MUST** not be the result of default settings, pre-selected options, inactivity or silence.

A request for consent **MUST** be presented to a consumer using language and/or visual aids that are concise and easy to understand.

An accredited data recipient **MUST** provide consumers with a straightforward process to withdraw consent and provide information about that process to each consumer prior to receiving the consumer's consent.

Consent **MUST** also be voluntary. Consent is voluntary if an individual has a genuine opportunity to provide or withhold consent. Consent is not voluntary where duress, coercion or pressure is applied by any party involved in the transaction.

Consent **MUST** also be *specific as to purpose*. The purpose of requesting the data should be directly associated with the specific data being requested. The broader purpose should also include information about the use case and the name of the product or service.

Comprehension is also fundamental to consent. As stated in the CDR Rules Explanatory Statement, the *'design of an accredited person's product or service should include consumer experience testing to ensure consumers' comprehension of the consent process.'*

The Consent Model

The key output of the CX Workstream will come in the form of CX Guidelines, which will provide data recipients and data holders with standards and guidelines for obtaining authorisations and consents, and withdrawing authorisations and consents. The Consent Model represents the current scope of the CX Workstream. 'Consent Model' refers to:

The Consent Flow

- Consent (where the consumer is asked to consent to a data recipient collecting and using their CDR data)
- Authentication (where the consumer is asked to authenticate themselves with the data holder)
- Authorisation (where the consumer is asked to authorise the disclosure of their CDR data to the data recipient)

Consent and Authorisation Management

- A consent management dashboard provided by the data recipient
- An authorisation management dashboard provided by the data holder

Withdrawal

- Withdrawing consent and authorisation

The CX Workstream will provide guidance on interrelated items within this scope, but this work will also help inform the broader CDR ecosystem.

A successful consumer experience will be fostered by an evidence-based Consent Model and a trustworthy CDR ecosystem that can help consumers:

- Understand what they are consenting to and why their data is being requested
- Understand what they are sharing and how it will be used
- Understand and trust who will have access to their data and the duration of that access
- Understand how to manage and withdraw consents and authorisations
- Understand the implications of withdrawing consents and authorisations
- Feel confident and informed about the sharing of their data
- Understand how to navigate the Consent Model

Consent

Control

CDR Rule 4.11 states that data recipients **MUST** allow consumers to choose, by actively selecting or otherwise clearly indicating:

- the types of data to be collected
- the specific uses of that data (including direct marketing)

CDR Rule 4.11 also states that data recipients **MUST** allow consumers to choose the period over which data will be collected and used by actively selecting or otherwise clearly indicating the period of that collection and use.

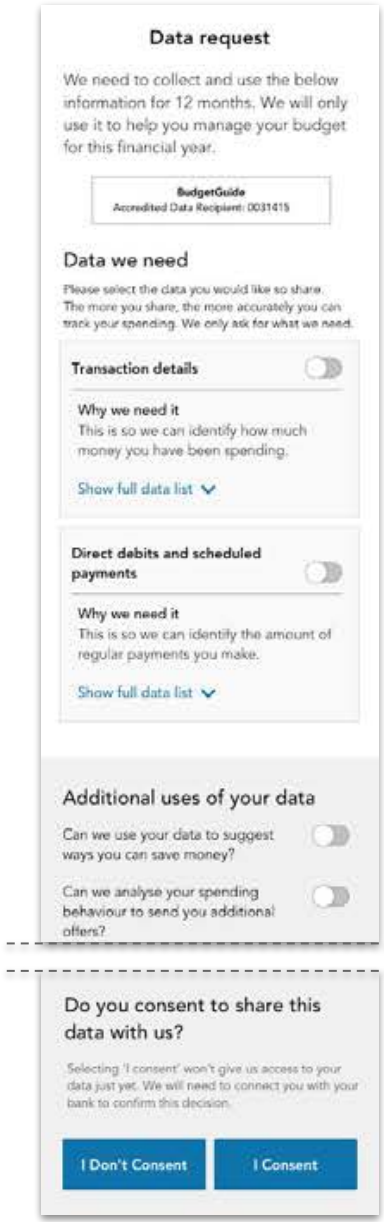
To meet these requirements, and as a way of providing additional control, CDR participants **MAY** consider the use of various consent capture design patterns to provide choice and allow consumers to opt-in such as checkboxes, toggles, scales, and binary yes/no choices.

The CX guidelines allow for the provision of consent at the level of data clusters and meet the requirements of the CDR rules.

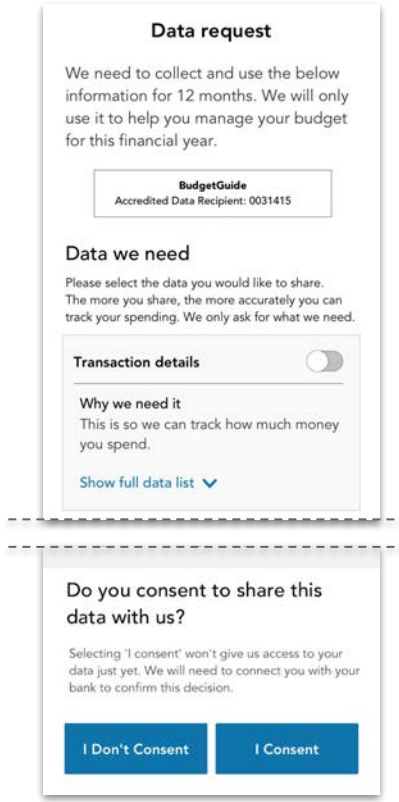
The CX Guidelines demonstrate the use of toggles for data cluster and additional uses (*Example 1)*, but data recipients **SHOULD** have regard to the use case in question, which may warrant an alternative implementation for simpler use cases (*Example 2)*.

Data recipients **SHOULD** also consider how additional controls may impact consent to data and uses that are 'required' for the use case, good, or service.

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 consumer experience research.



Example 1



Example 2

Consent

Simplicity

The CX Guidelines provide examples of how to put key CDR Rules into effect, and consider a range of scenarios. The level of detail required when a data recipient is seeking consent depends on a number of factors, including:

1. how the data recipient intends to use that data;
2. how the data recipient intends to handle redundant data;
3. how much data the data recipient is requesting; and
4. how the data recipient displays this information to the consumer

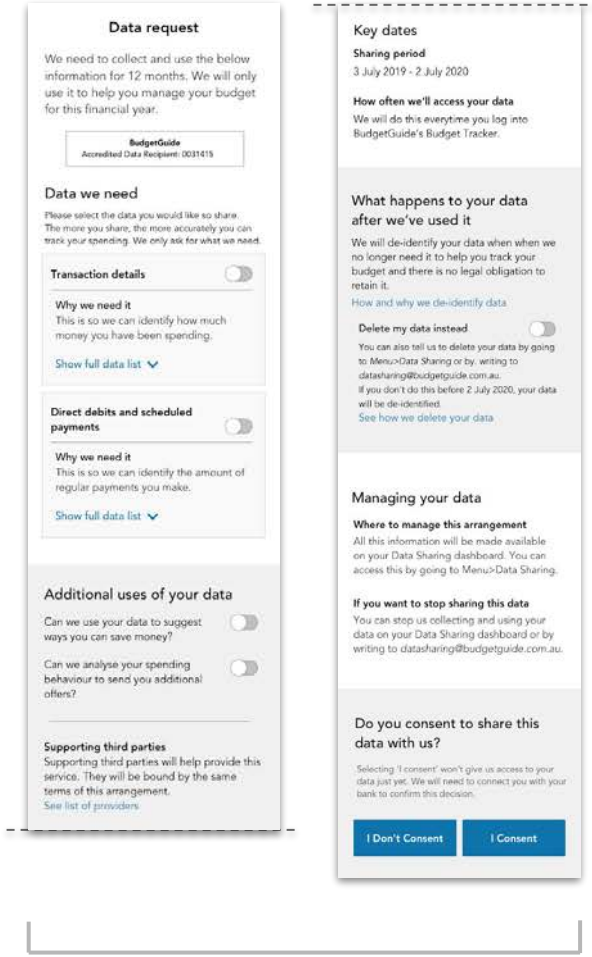
More detail and interaction is generally required if:

1. a range of uses are requested;
2. the data recipient does not have a general policy of deleting redundant data;
3. the data recipient is requesting extensive data; and
4. as a result of the above points, the data recipient requires additional elections and accompanying descriptions

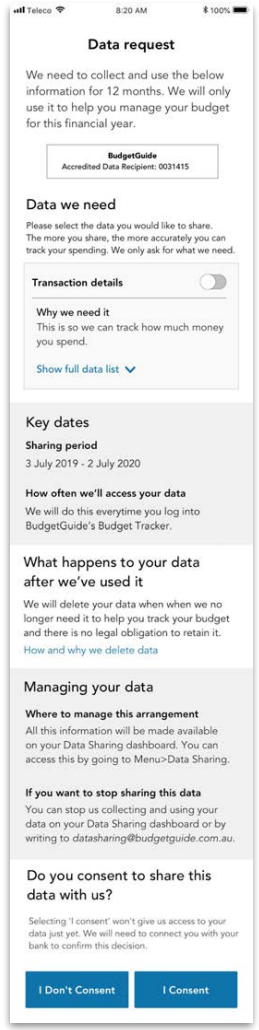
Example 1 demonstrates a consumer-facing data request where more detail and interaction is required.

Example 2 demonstrates the same step where less detail and interaction is required.

The CX Guidelines contain design options for how to put certain rules and use cases into effect. Data recipients and data holders may consider other design patterns where appropriate to further facilitate consumer comprehension and control, such as pagination, carousel cards, or Typeform-style patterns.



Example 1



Example 2

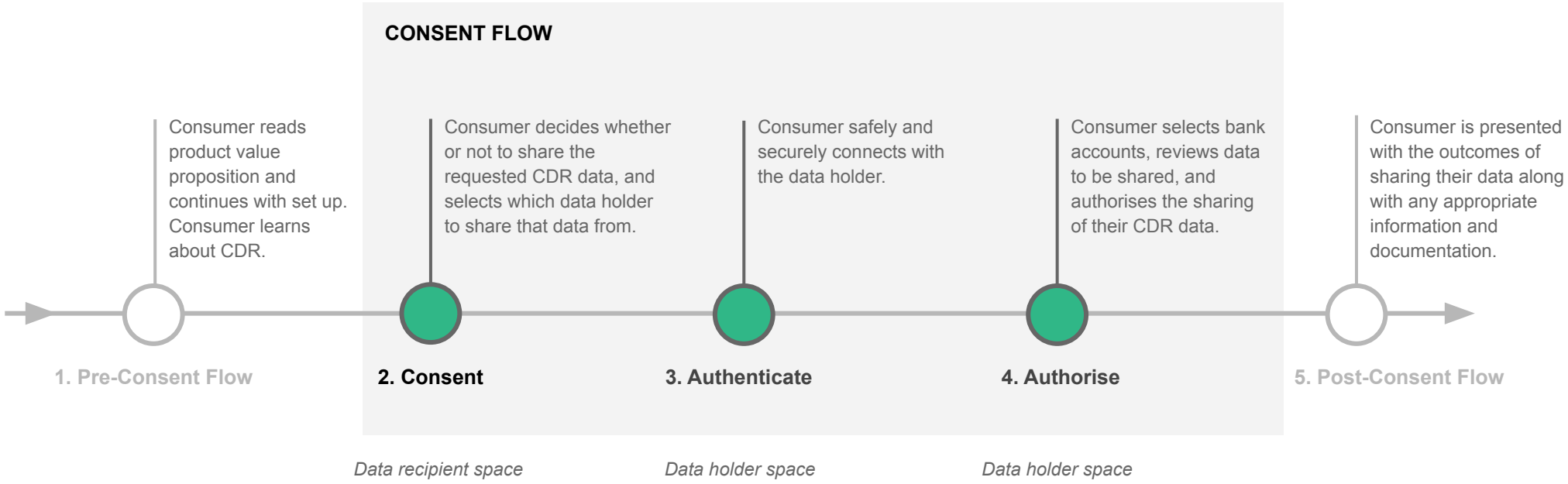
CONSUMER DATA STANDARDS

Consent Flow: Consumer journey

CONSENT FLOW: CONSUMER JOURNEY OVERVIEW

This section of the CX Guidelines are focused on the consent flow, but the CX research clearly showed the importance of the pre-consent and post-consent flow experience to consumer trust, confidence, and comprehension.

The core components of the consent flow begin with the 'Data Request', where the data recipient asks the consumer to consent to certain data being collected and used for specific purposes. The CX Guidelines provide additional guidelines that precede this critical step to help organisations provide consumers with a simple, informed, and trusted data sharing experience.

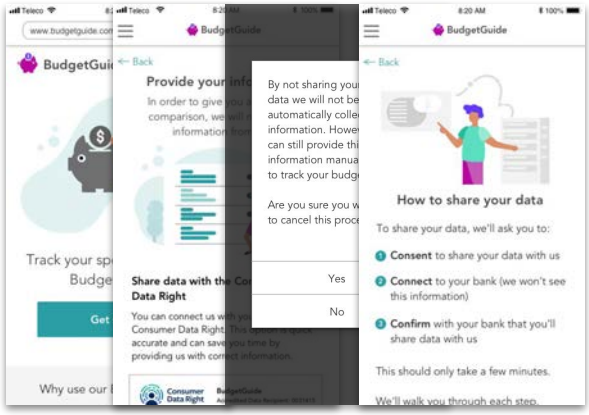


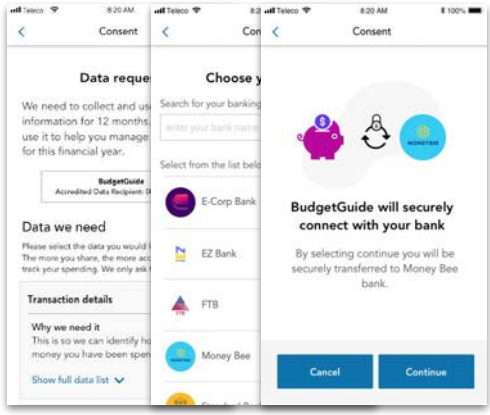
CONSENT FLOW: CONSUMER JOURNEY OVERVIEW

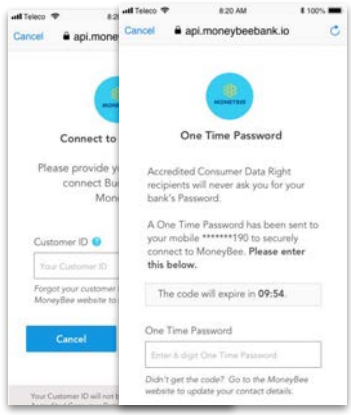
See InVision prototype

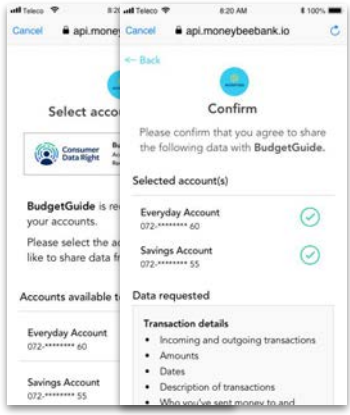
The following are screens for the consent flow featured in this document. These screens are examples how to put key rules, standards, and CX recommendations into effect.

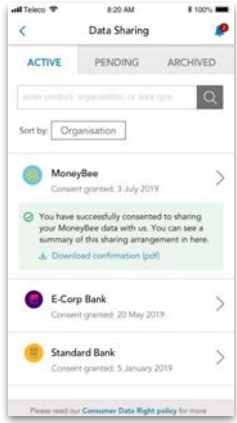
1. PRE-CONSENT | **2. CONSENT** | **3. AUTHENTICATE** | **4. AUTHORISE** | **5. POST-CONSENT**











The consumer may sign up for the service and download the app between these screens.

Data recipient space — *Data holder space* — *Data recipient space*

CONSUMER DATA STANDARDS

1. PRE-CONSENT FLOW

The pre-consent stage consists of a general onboarding experience and takes place prior to the Consent Flow. Consumer trust is critical to CDR adoption. Trust **SHOULD** be built prior to an ADR requesting CDR data, and when this occurs depends on whether or not the consumer has a pre-existing relationship with the ADR.

Product value proposition

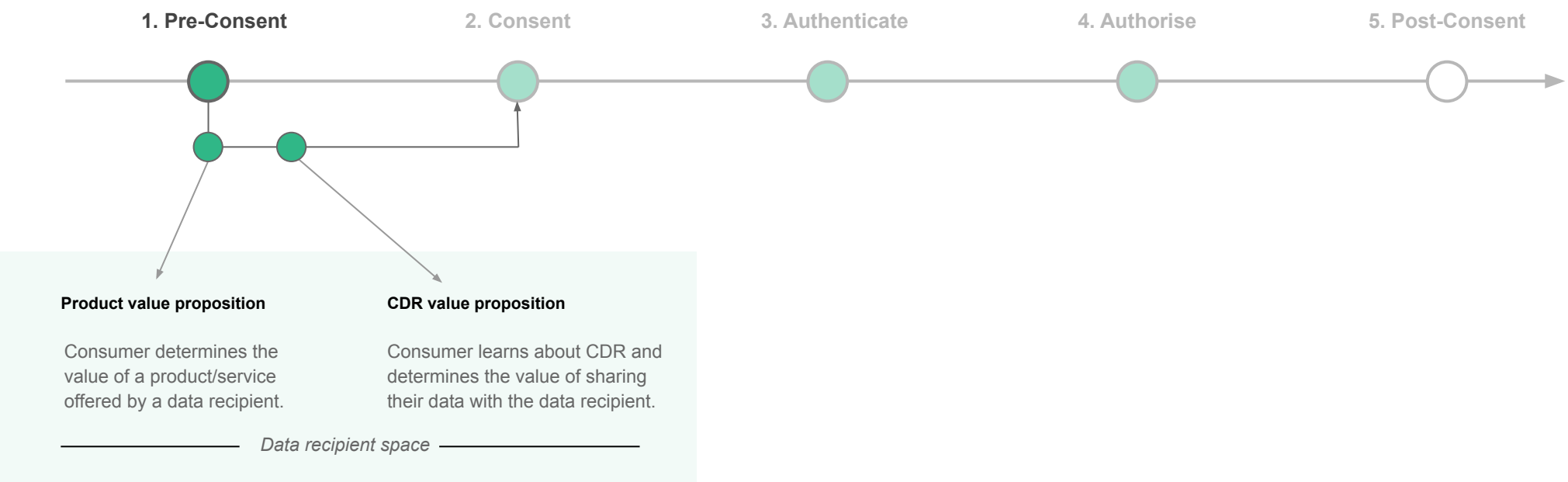
This stage **MAY** occur prior to the data recipient seeking consent from the consumer, and **MAY** involve onboarding, offers, or other product-oriented interactions that are separate to data sharing requests.

CDR value proposition

The propensity to share CDR data will depend on how much a consumer trusts the ADR, and the expected benefit of sharing that data with the ADR.

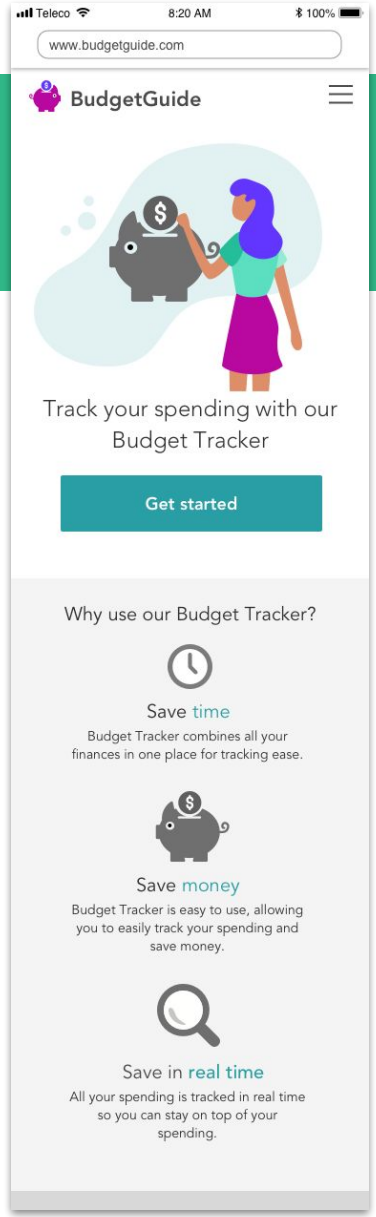
At this step, the data recipient **SHOULD** communicate the value and purpose of sharing CDR data, the product or service this request relates to, and general information about the CDR for consumer education.

In addition to the relationship with the data recipient, this step is a critical point where the utility of data sharing can be assessed and trust in the process and ecosystem can be developed.

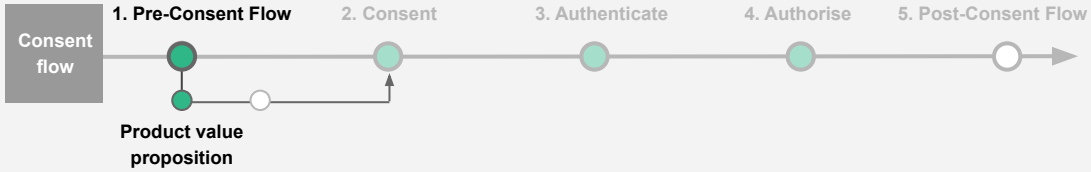


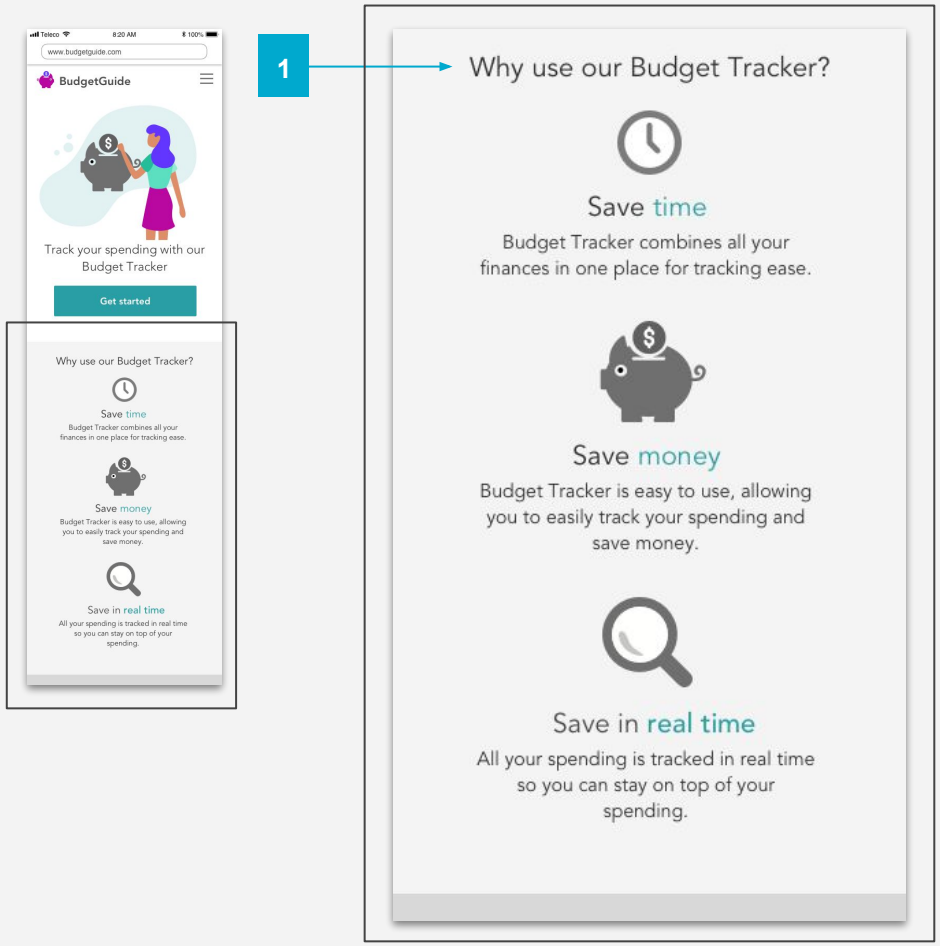
Pre-consent flow | Product value proposition

This section highlights the importance of data recipients building trust prior to requesting consumer data, and the requirement to separate data requests from other processes so as to not bundle consent.



Example wireframe





Note: The component shown is an example implementation.

Pre-consent | Product value proposition

Product value proposition

CX Guideline

1 Data recipients **SHOULD** build trust and onboard the consumer to the service itself before presenting a data request.

CX Research 1, 25, 28, 31

RULE

Data recipients **MUST NOT** bundle consent with unrelated purposes.

Data recipients **MUST NOT** infer consent or rely on an implied consent.

CDR Rules 4.10(b)(ii), 4.11(1)(Note 1) | CX Research 36

Pre-consent flow | CDR value proposition

CDR value proposition

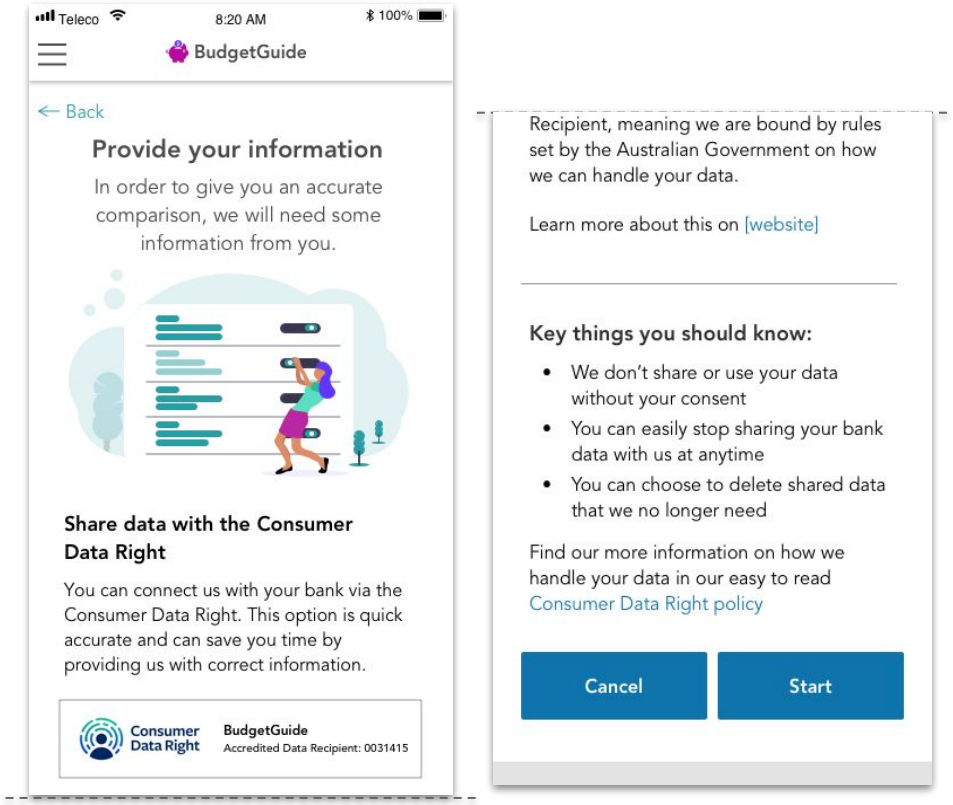
This section provides guidelines on how data recipients may provide upfront information about the CDR.

Consumer participation in the CDR will depend heavily on trust, confidence, and how compelling value propositions are:

- Clearly explaining the value of sharing data as part of the CDR
- The presentation of CDR logo* and accreditation information to help build trust.
- Information on how consumer data will be handled
- Clearly explaining how CDR data *won't* be used

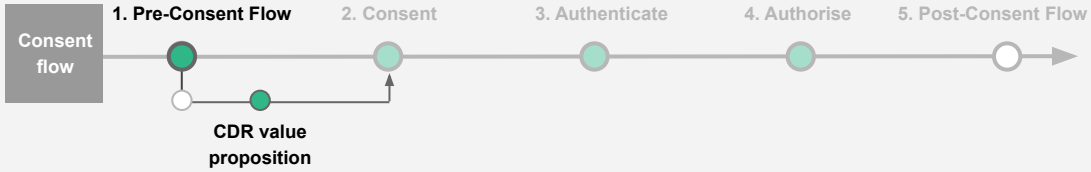
Educational information about the CDR should be presented in an easy to understand and digestible manner (such as simple and standardised documents, videos, infographics, or comic contracts).

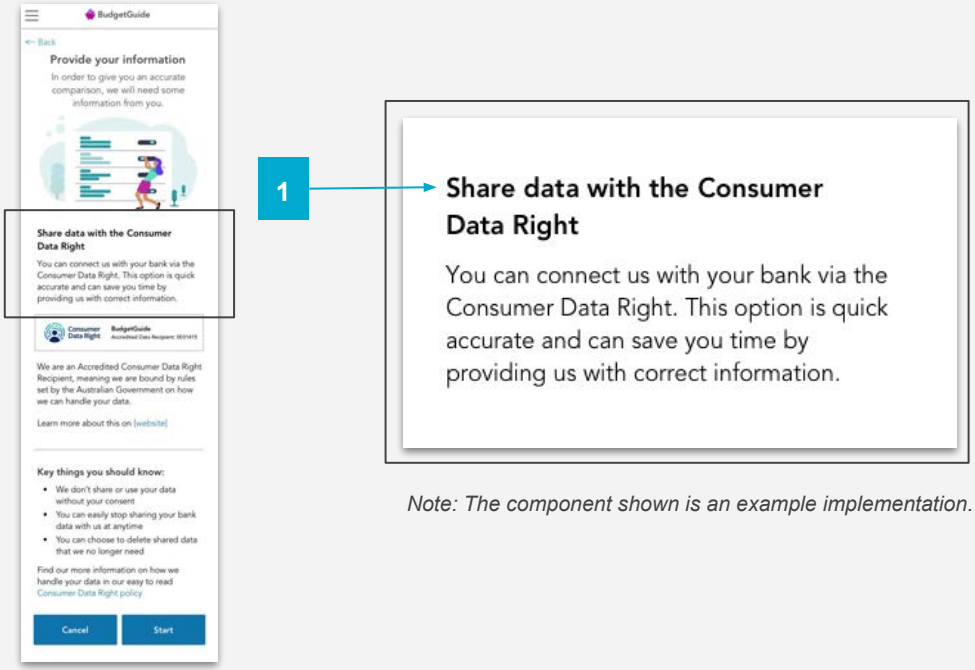
**CDR branding will be provided to CDR participants by the ACCC.*



Example wireframe

CONSUMER DATA STANDARDS





Note: The component shown is an example implementation.

Pre-consent | CDR value proposition

CDR information

"Without not knowing much more about it I'll probably not proceed... I'll just close it"

CX Research 26

CDR Rule

Data recipients **MUST** conform with the CDR Rules on consent, including that consent must be voluntary; express; informed; specific as to purpose; time limited; and easily withdrawn.

CDR Rules 4.9

CX Guideline

1 Data recipients **SHOULD** clearly communicate the value of sharing data as part of the CDR.

CX Research 25

CX Guideline

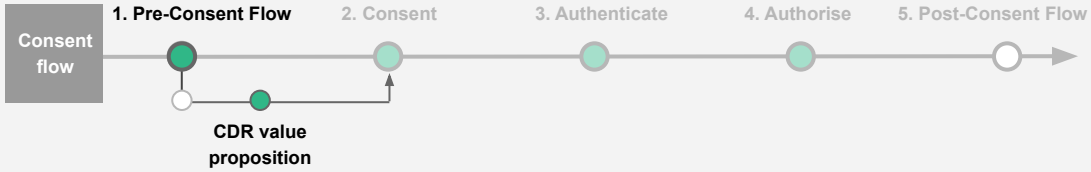
Consent **SHOULD** be a genuine choice. Data recipients **SHOULD** avoid making consent a precondition of service.

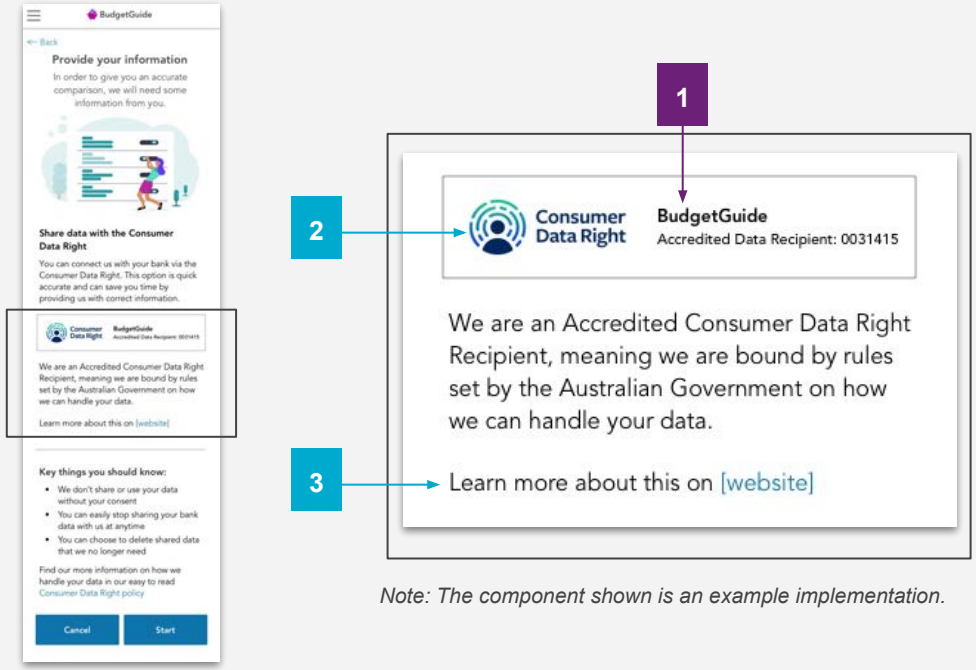
CX Research 26

CX Guideline

The data recipient **SHOULD** include CDR branding (for example, a CDR logo) as provided by the ACCC where appropriate.

CX Research 23





Note: The component shown is an example implementation.

Pre-consent | CDR value proposition

Accreditation information

CDR Rule

1 The data recipient **MUST** present their name and accreditation number to the consumer.

CDR Rules 4.11(3)(a),(b)

CX Guideline

The data recipient **MUST NOT** include documents or references to other documents that reduce comprehension.

CDR Rules 4.10(b)(i)

CX Guideline

2 The data recipient **SHOULD** use CDR branding provided by the ACCC to facilitate consistency, familiarity, and trust in the CDR ecosystem.

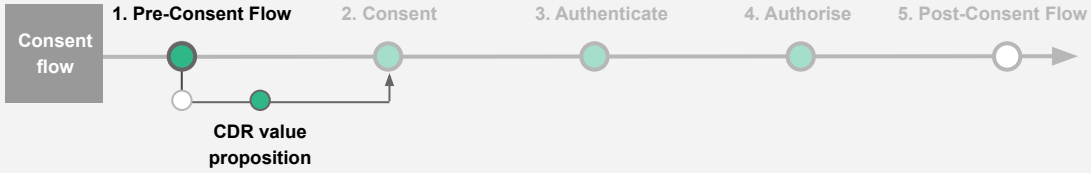
3 The data recipient **SHOULD** provide instructions for how consumers can verify a data recipient's accreditation via an ACCC-provided URL once the ACCC makes this functionality available.

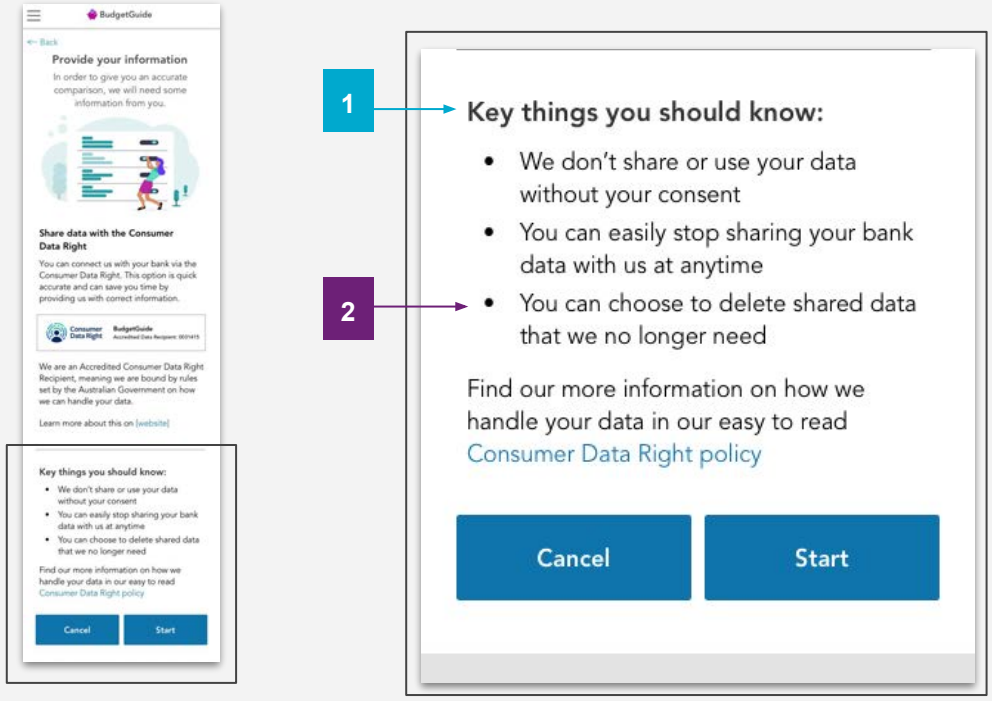
CX Research 13, 23

CX Guideline

The ability to go backwards **SHOULD** be present and visible wherever possible throughout the consent flow to ensure user control and freedom.

10 Usability Heuristics for User Interface Design: User control and freedom (Nielsen)





Note: The component shown is an example implementation.

Pre-consent | CDR value proposition

Data sharing rules (1)

CDR Rule

2 Data recipients **MUST** include clear and unambiguous information on how CDR data will be handled upon consent expiry/withdrawal. This **SHOULD** be presented up front, and wherever applicable throughout the consent model.

CDR Rules 4.9, 4.11(3)(h) | CX Research 33

CX Guideline

Data recipients **SHOULD** provide information, where applicable, about measures taken in case of security breaches.

CX Research 14

CX Guideline

1 Data recipients **SHOULD** clearly state key things that are important to their customers. This should include how data will ***not*** be used, even if these uses are prohibited CDR. Examples may include:

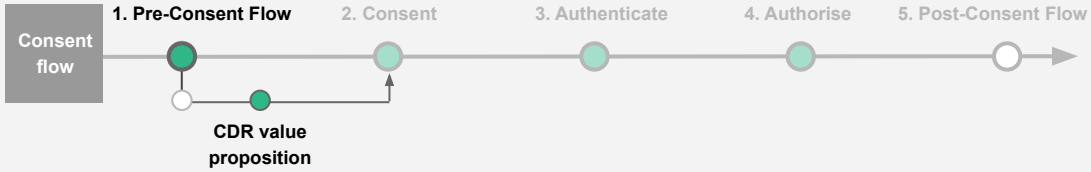
- We don't share or use your data without your consent
- We don't sell your data to anyone
- We don't share your data for marketing purposes

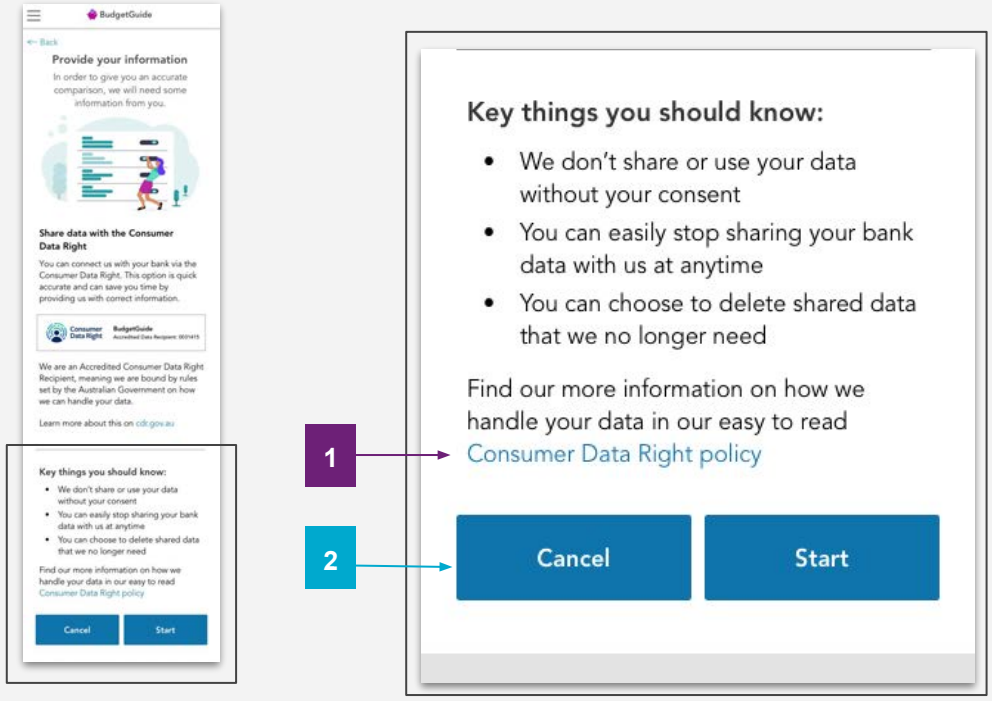
CX Research 24

CX Guideline

CDR information **SHOULD** have full translation functionality and be fully screen-reader accessible.

CX Research 16





Note: The component shown is an example implementation.

Pre-consent | CDR value proposition

Data sharing rules (2)

CDR Rule

1 The CDR policy **MUST** be available through online services where the data recipient ordinarily deals with CDR consumers.

It **MUST** be in the form of a document that is separate from the data recipient's private policy

CDR Rules 7.2(8), 7.2(2)

CX Guideline

2 Consent **SHOULD** be a genuine choice. Data recipients **SHOULD** avoid making consent a precondition of service.

CX Research 26

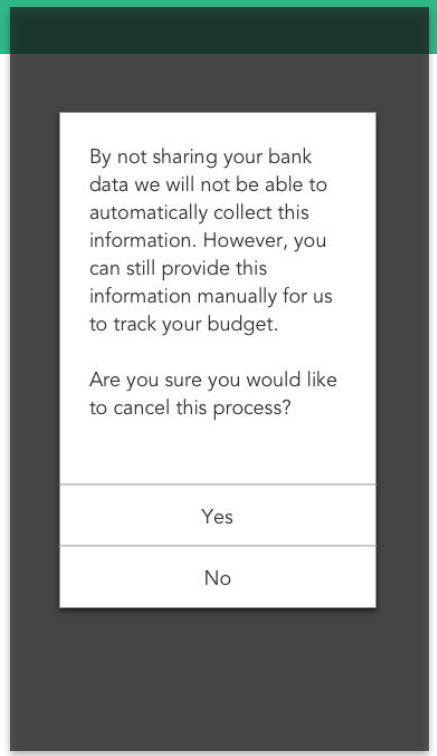
Pre-consent flow | CDR value proposition

Cancellation screen

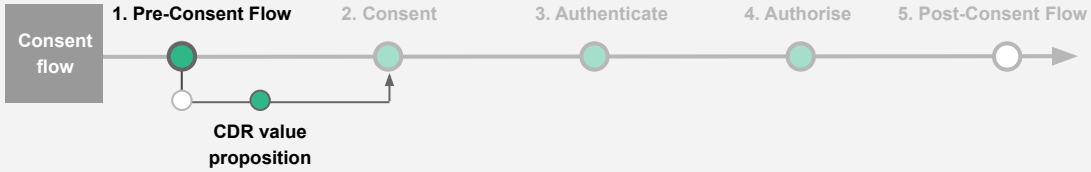
This section provides examples illustrating how the guidelines may be implemented, in particular focusing on the step for cancelling a data request mid-way through the process.

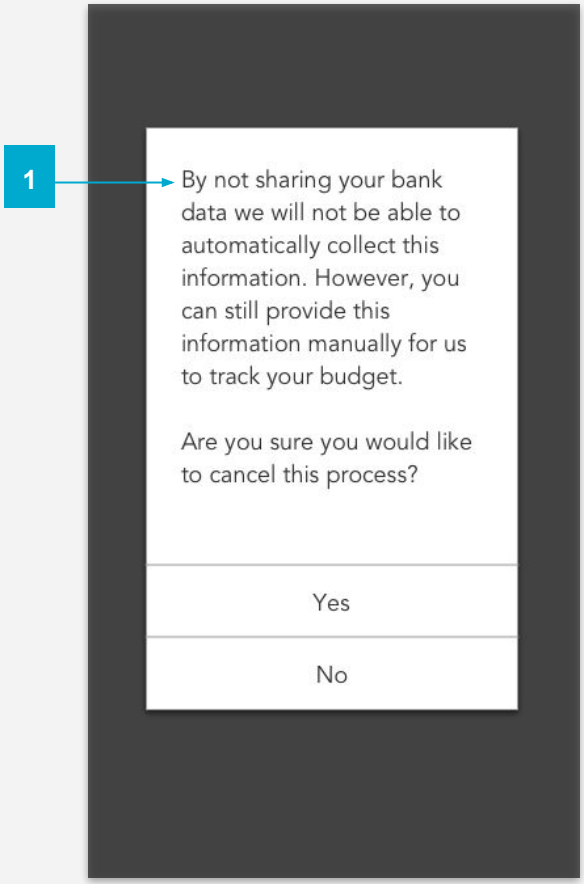
The process **SHOULD** ensure that is is clear to the consumer what alternative options (if appropriate) are available to them if they choose not to share their data via CDR.

The rules and recommendations outlined on the next page **SHOULD** be implemented where possible whenever the cancel option is selected throughout the consent flow.



Example wireframe





Note: The screen shown is an example implementation.

Manual data sharing as an alternative is an example for this specific scenario. The offering of alternatives is at the discretion of the data recipient.

Pre-consent | CDR value proposition

Cancellation

CDR Rule

Data recipients **MUST** conform with the CDR Rules on consent, including that consent must be voluntary, express, informed, specific as to purpose, time limited and easily withdrawn.

CDR Rules 4.9

CX Guideline

1 Consent **SHOULD** be a genuine choice. Data recipients **SHOULD** avoid making consent a precondition of service.

CX Research 26

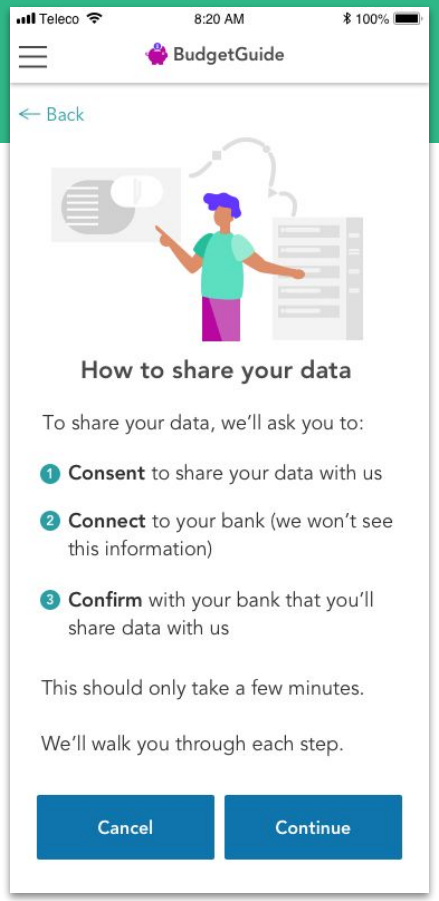
Pre-consent flow | CDR value proposition

CDR data sharing instructions

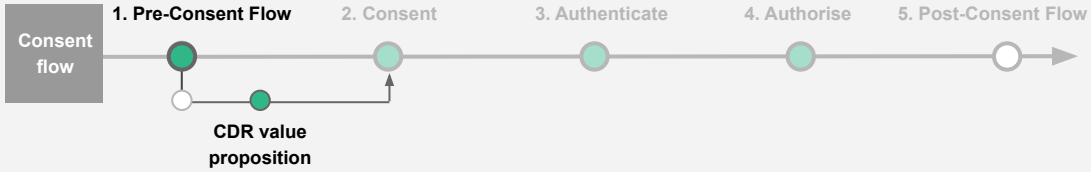
This section provides examples illustrating how the guidelines may be implemented, in particular focusing on providing consumers with an overview of the Consent Flow stages.

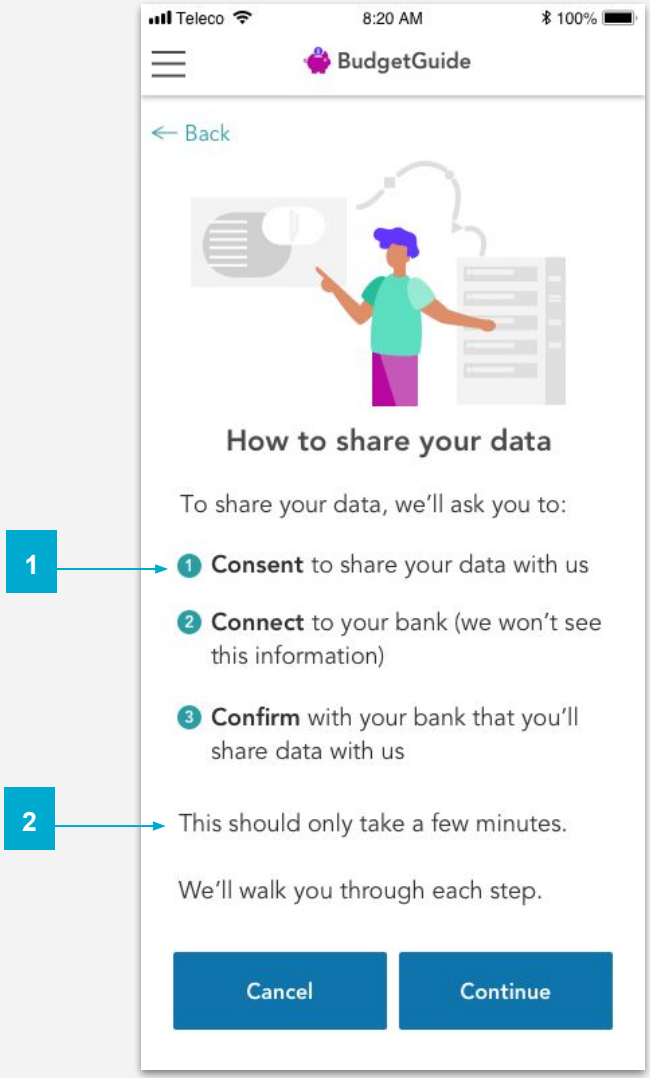
It is important to provide consumers with an indication of the approximate time it will take them to complete the Consent Flow as well as the different stages of the process they will progress through.

While the Consumer Data Right regime refers to the Consent Flow stages using the language: *Consent, Authenticate, Authorise*; the CX research has suggested that *Consent, Connect, and Confirm* are more intuitive terms and **SHOULD** be used within any consumer-facing descriptions of the Consent Flow.



Example wireframe





Note: The screen shown is an example implementation.

Pre-consent | CDR value proposition

CDR data sharing instructions

CX Guideline

1 Data recipients **SHOULD** use the terms *Consent, Connect, Confirm* to represent each major stage of the consent flow. These terms **SHOULD** be used throughout the flow to maintain consistency and to help users to become familiar with sharing steps.

10 Usability Heuristics for User Interface Design: Consistency and standards (Nielsen)

CX Guideline

2 Data recipients **SHOULD** provide simple, up front instructions on how to share data with the CDR, including the time it takes to complete the process. For example: 'This should only take a few minutes.'

Consent Flow

CONSENT FLOW OVERVIEW

The Consent Flow is divided into three discrete stages: Consent; Authenticate; and Authorise.

Consent

The Consent stage occurs within the data recipient space. At this stage, a consumer will be able to:

- see that the data recipient is accredited
- review details of the data request
- select which data holder they will share their data from

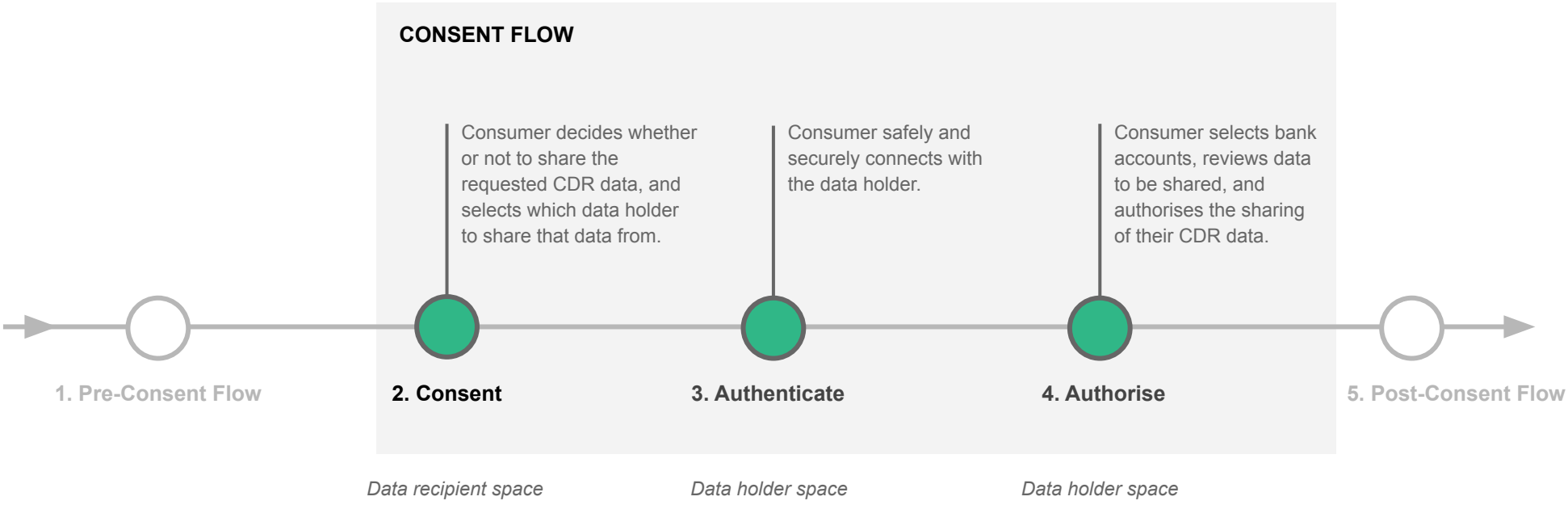
Authenticate

The Authenticate stage occurs within the data holder space. At this stage, the consumer will securely connect with the data holder.

Authorise

The Authorise stage occurs within an authenticated data holder space. At this stage, the consumer will be able to:

- select the accounts they wish to share data from;
- review a summary of the data that will be shared; and
- authorise the sharing of their data from the data holder to the data recipient.



CONSUMER DATA STANDARDS

2. CONSENT

The Consent stage contains several steps, which may include a CDR value proposition; the data request; selecting a data holder; and the step before authentication.

Data request

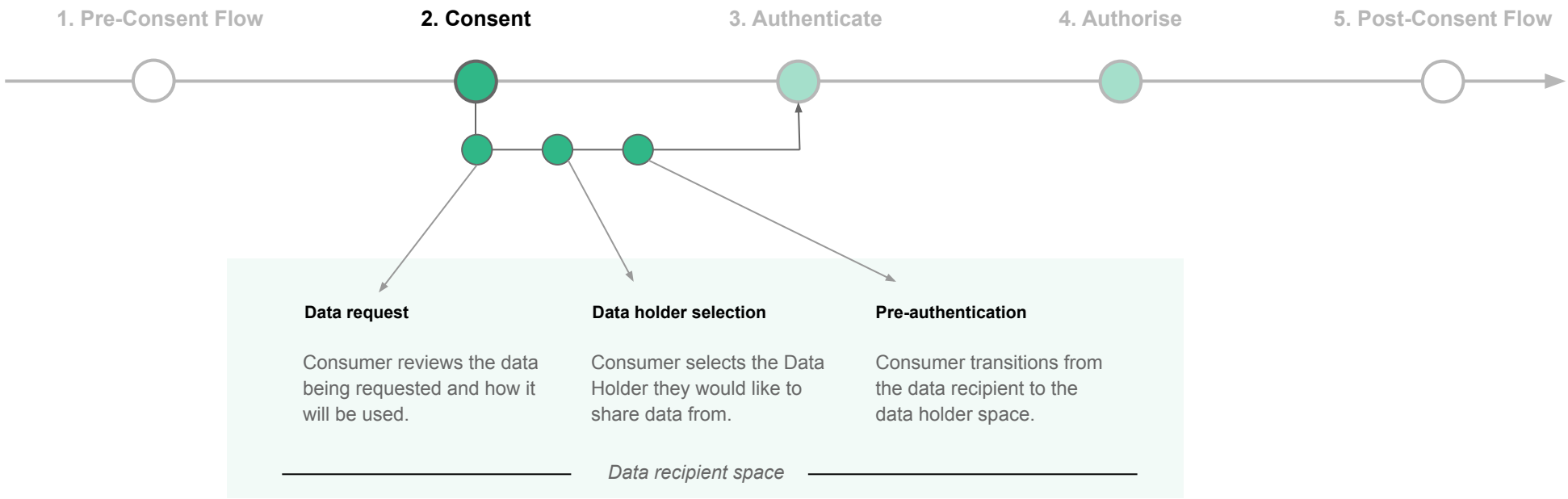
At this step, the consumer will be able to review a summary of the data that the Data Recipient is requesting.

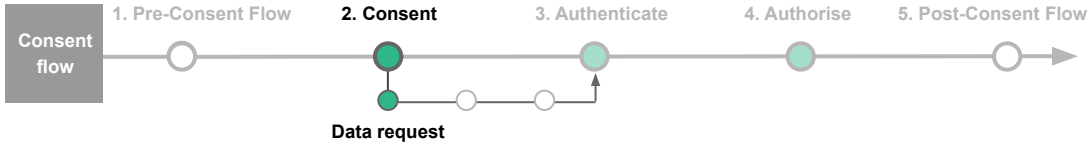
Data holder selection

At this step, the consumer will be able to select the Data Holder that they would like to share their data from.

Pre-authentication step

This step will provide an overview of what authentication will entail.





Consent | Data request

This section provides examples illustrating how the guidelines may be implemented. A data recipient's processes for asking a CDR consumer to give consent **MUST**:

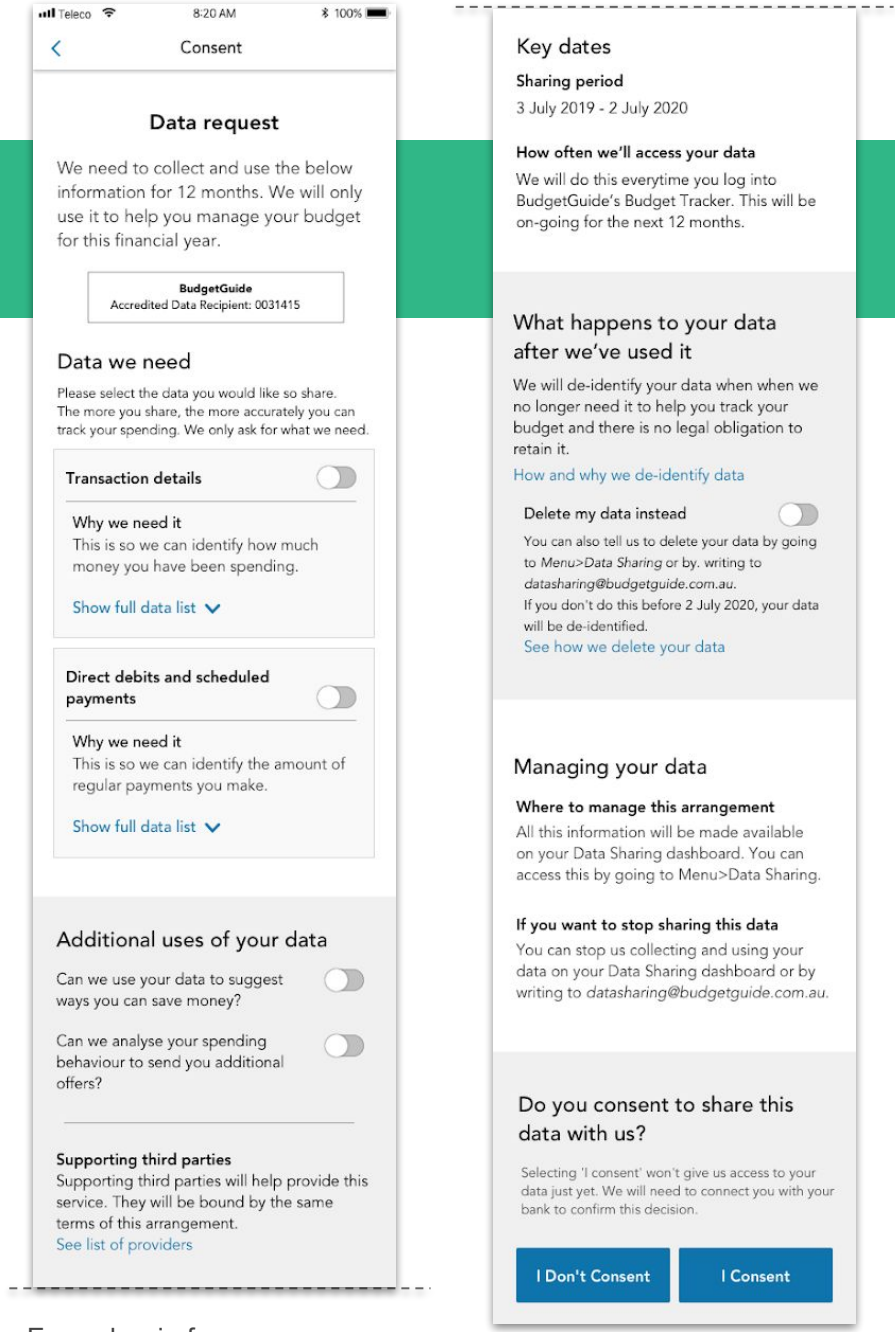
- accord with the data standards;
- have regard to any consumer experience guidelines developed by the Data Standards Body
- be as easy to understand as practicable, including by use of concise language and, where appropriate, visual aids;

Example implementation

The components contained in this section are based on the example to the right, where two data clusters are being requested: 'Transaction details' and 'Direct debits and scheduled payments'. These data clusters are presented on a single screen. The consumer is required to select "I Consent" to agree to the data request.

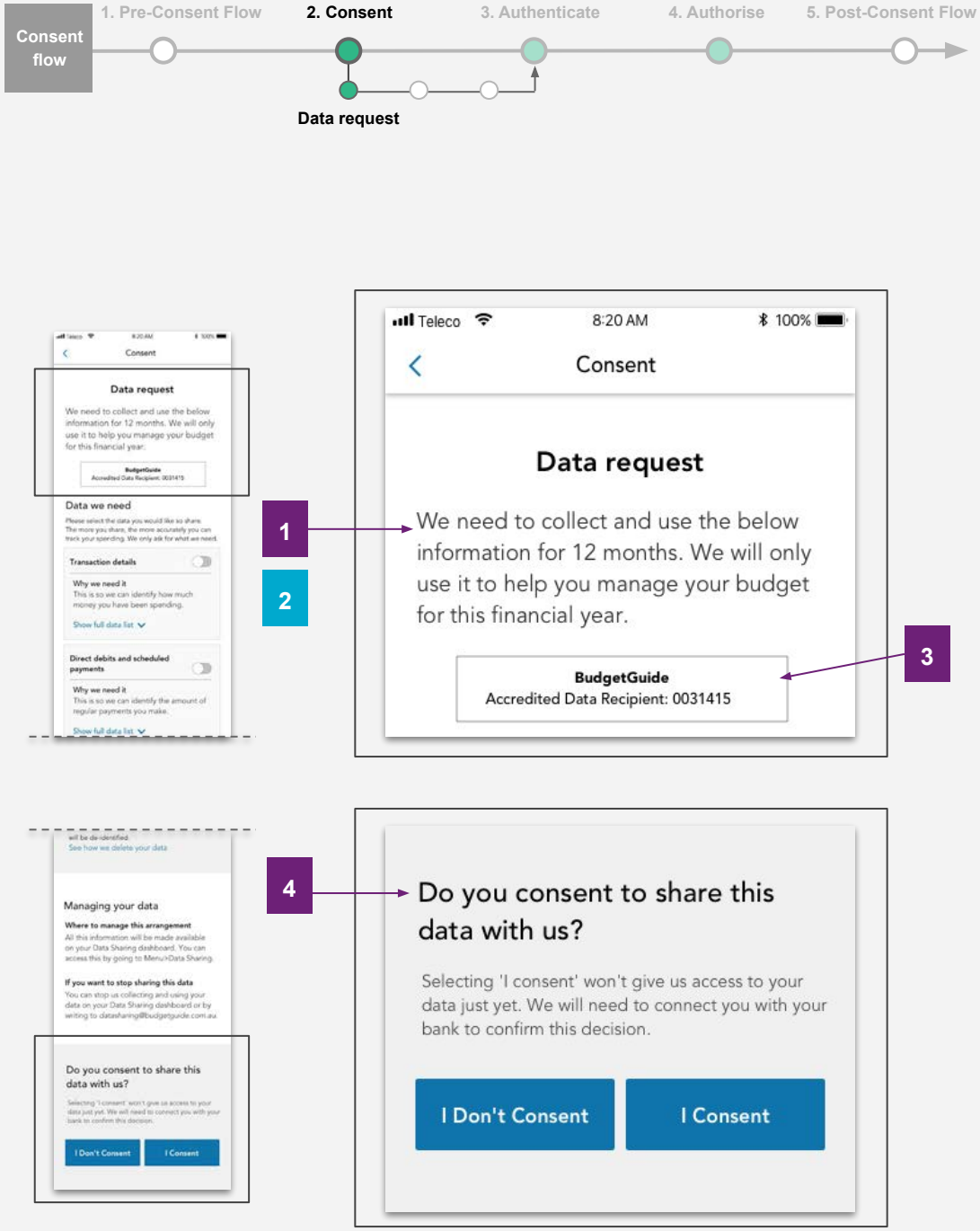
CX research suggests that having all information available on one page made participants feel the process of data sharing was more transparent and easier to understand.

To prevent cognitive overload, data recipients and data holders **MAY** consider other design patterns to further facilitate comprehension and control. These **MAY** include patterns that use pagination, carousel cards, or ones similar to Typeform.



Example wireframe

CONSUMER DATA STANDARDS



Note: The components shown are examples of implementation.

Consent | Data request

Active consent

CDR Rule

1 When asking a consumer to consent to the collection and use of their CDR data, data recipients **MUST** ask the consumer's express consent to collect those types of data over a specified period of time.

CDR Rule 4.11(1)(c)(i)

CDR Rule

Consent **MUST NOT** be inferred or implied.

CDR Rule 4.11(1)(e)(Note 1)

CX Guideline

2 Data recipients **SHOULD** structure the 'purpose' and 'use' statements in ways that:
1. Are specific as to purpose *(e.g. 'Why we need it' for each data cluster)*
2. Refer to the broader 'use case' or 'uses' *(e.g. 'to pre-populate your application')*
3. Relate to the product/service being provided *(e.g. 'so BudgetGuide can help you manage your budget')*

This information **SHOULD** be framed in a way that communicates the benefit of data sharing to the consumer.

CDR Rule

3 When asking for the consent, data recipients **MUST** give the CDR consumer their name and accreditation number.

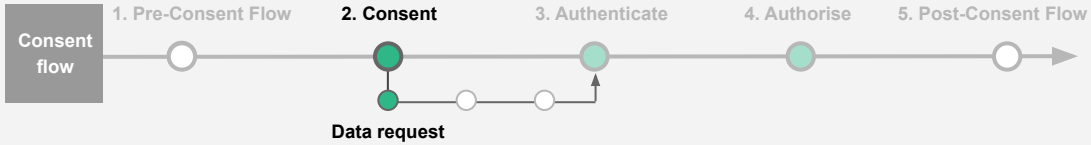
CDR Rule 4.11(3)(a), (b)

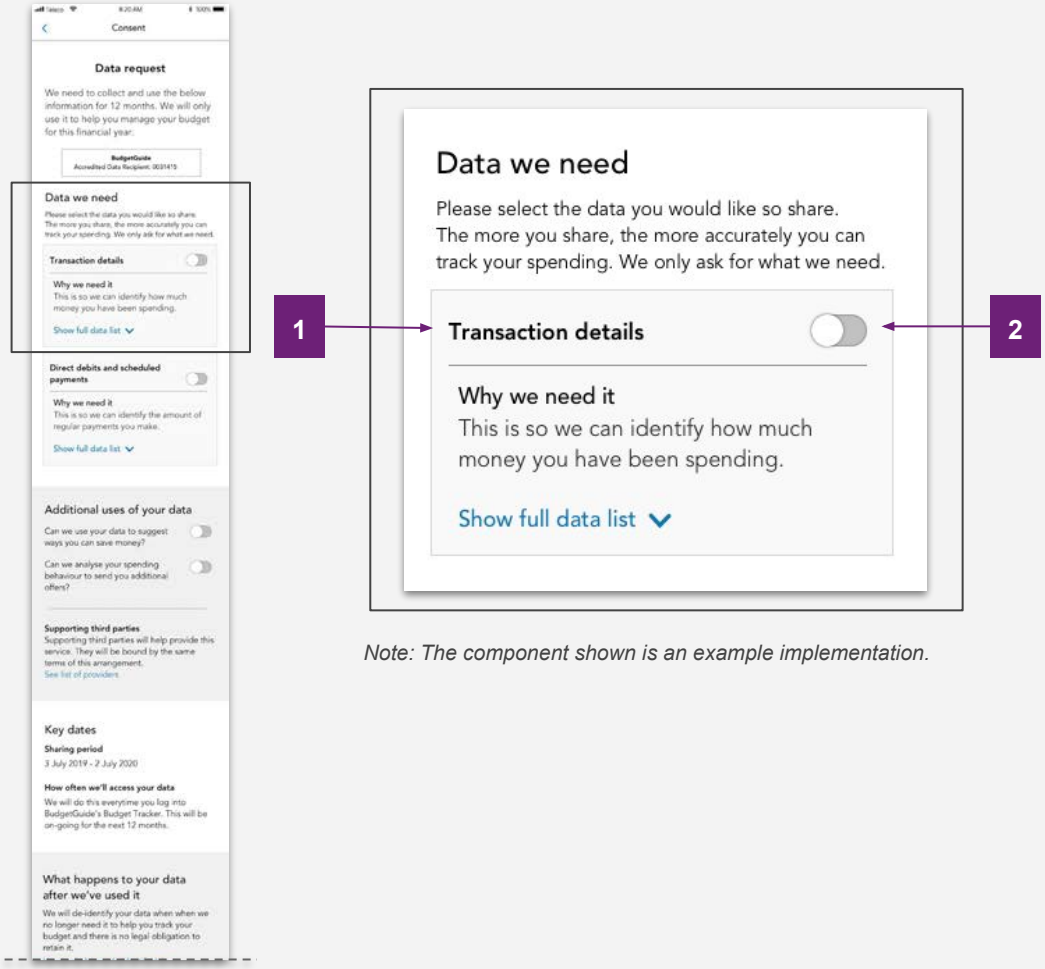
CDR Rule

4 Data recipients **MAY**, in accordance with Subdivision 4.3.2, ask the consumer to give their consent to the data recipient collecting and using their CDR data in order to provide those goods or services.

In giving the consent in response to such a request, the consumer gives the data recipient a valid request to seek to collect that CDR data from a data holder.

CDR Rule 4.3(2), (3)





Note: The component shown is an example implementation.

Consent | Data request

Data clusters and permissions (1)

CDR Rule

1 Data recipients **MUST** identify the types of CDR data for which consent is sought.

CDR Rule 4.11(1)(a)(i)

CDR Rule

1 Data language standards **MUST** be used to describe data.

CDR Rule 8.11(1)(d) | Data Language Standards

CDR Rule

2 Data recipients **MUST** allow the consumer to choose the type of CDR data to be collected and used, allowing the consumer to actively select or otherwise clearly indicate which data types they are consenting to being collected and what specific uses they are consenting their data to be used for.

2 Data recipients **MUST NOT** present pre-selected options to the consumer when asking for consent

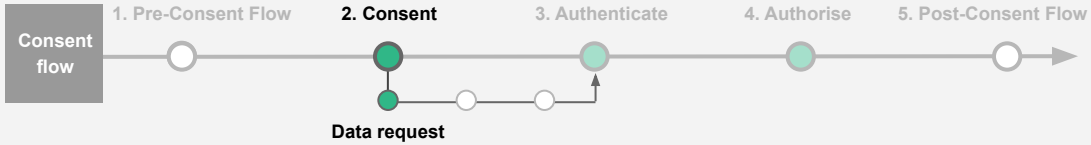
2 Achieving the above **MAY** involve using various consent capture design patterns that allow consumers to opt-in such as checkboxes, toggles, and binary yes/no choices.

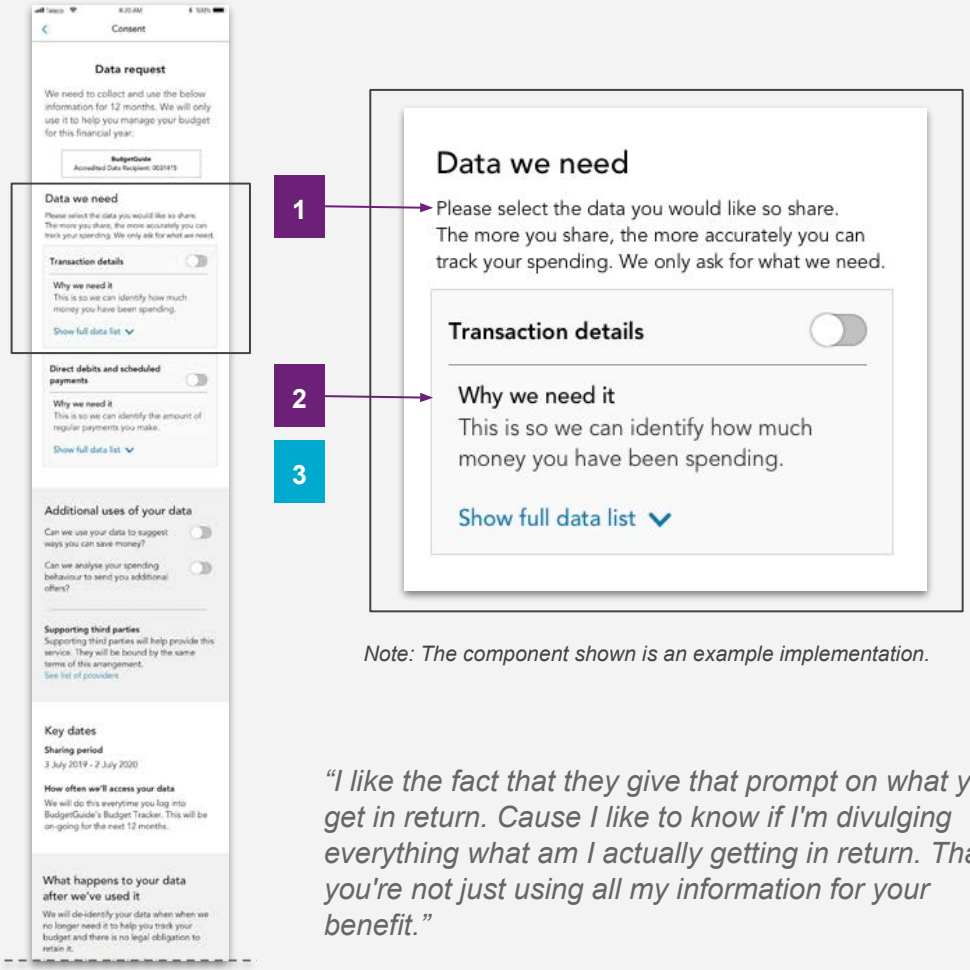
CDR Rules 4.11(1)(a), 4.11(2) | CX Research 2, 3, 4, 5, 6

CDR Rule

Data recipients **MUST** not infer consent or rely on an implied consent.

4.11(1)(e)(Note 1)





Note: The component shown is an example implementation.

"I like the fact that they give that prompt on what you get in return. Cause I like to know if I'm divulging everything what am I actually getting in return. That you're not just using all my information for your benefit."

CX Research 2

Consent | Data request

Data clusters and permissions (2)

CDR Rule

Data recipients **MUST** comply with the data minimisation principle when requesting, collecting, and using CDR data.

1 Data recipients **MUST** give the consumer information on how the collection and use of CDR data complies to the data minimisation principle by indicating that the collection and use of data will not go beyond what is reasonably needed.

CDR Rules 1.8, 4.4(1)(d), 4.12(2), 4.11(3)(c) | CX Research 1, 2, 3

CDR Rule

2 Data recipients **MUST** be specific as to purpose when requesting data.

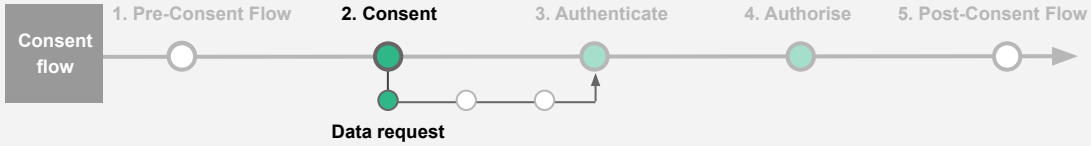
2 Data recipients **must** identify the specific uses of the CDR data from which the consumer will be able to select or specify.

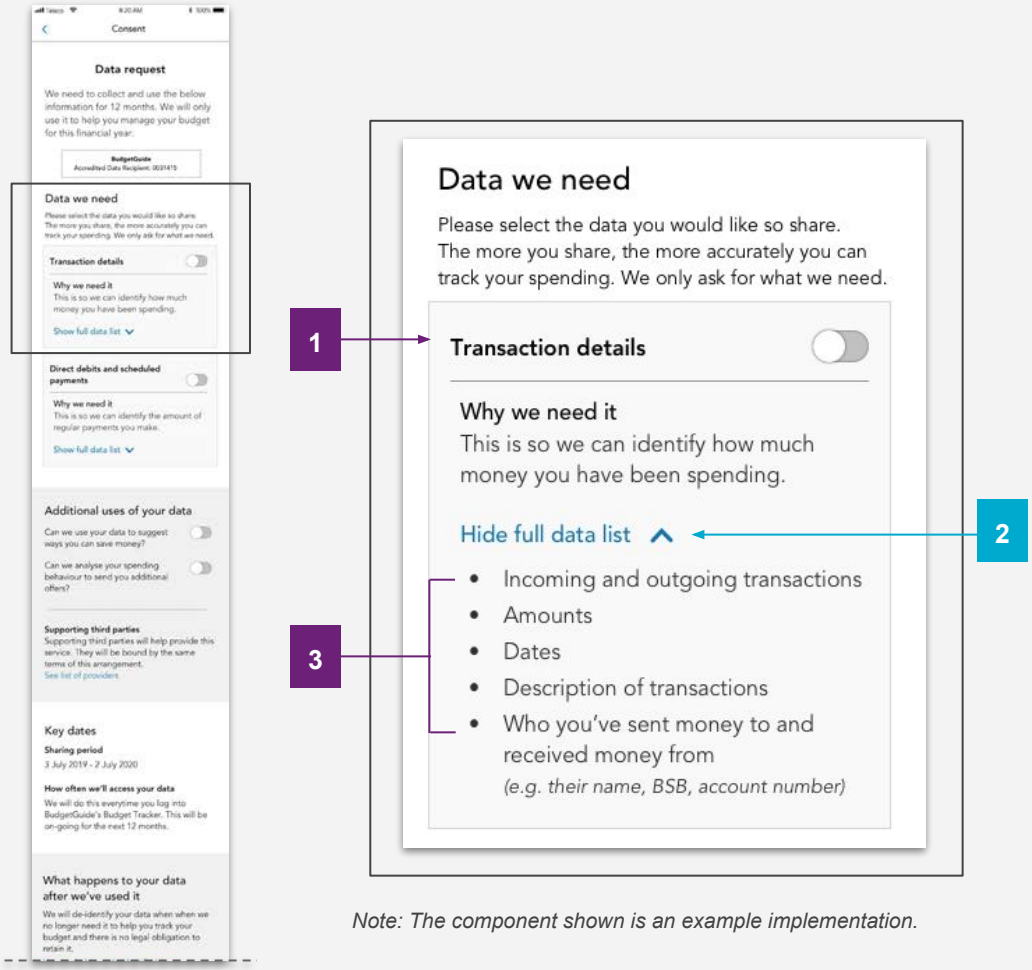
CDR Rule 4.11(1)(a)(ii), 4.11(1)(c)(ii) | CX Research 1, 2, 3

CX Guideline

3 Data recipients **SHOULD** structure the 'purpose' and 'use' statements in ways that:
1. Are specific as to purpose *(e.g. 'Why we need it' for each data cluster)*
2. Refer to the broader 'use case' or 'uses' *(e.g. 'to pre-populate your application')*
3. Relate to the product/service being provided *(e.g. 'so BudgetGuide can help you manage your budget')*

This information **SHOULD** be framed in a way that communicates the benefit of data sharing to the consumer.





Note: The component shown is an example implementation.

Consent | Data request

Data clusters and permissions (3)

CDR Rule

1 3 Data recipients **MUST** identify the types of CDR data for which consent is sought.

CDR Rules 4.11(1)(a)(i), and 4.11(1)(c)(i)

CDR Rule

Data recipients **MUST** comply with the data minimisation principle when requesting, collecting, and using CDR data.

CDR Rules 1.8, 4.4(1)(d),4.12(2) | CX Research 1, 2, 3

CDR Rule

1 3 Data language standards **MUST** be used to describe data.

CDR Rule 8.11(d) | Data Language Standards

CDR Rule

Data recipients **MUST** seek to make the consent process as easy to understand as is practicable.

CDR Rule 4.10(a)(ii)

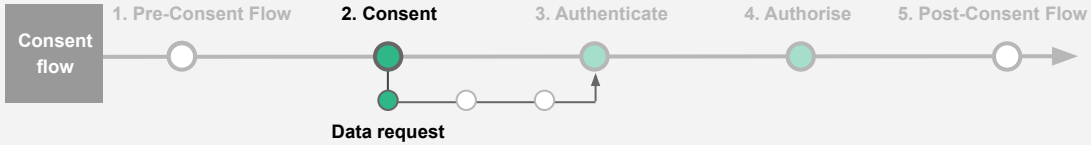
CX Guideline

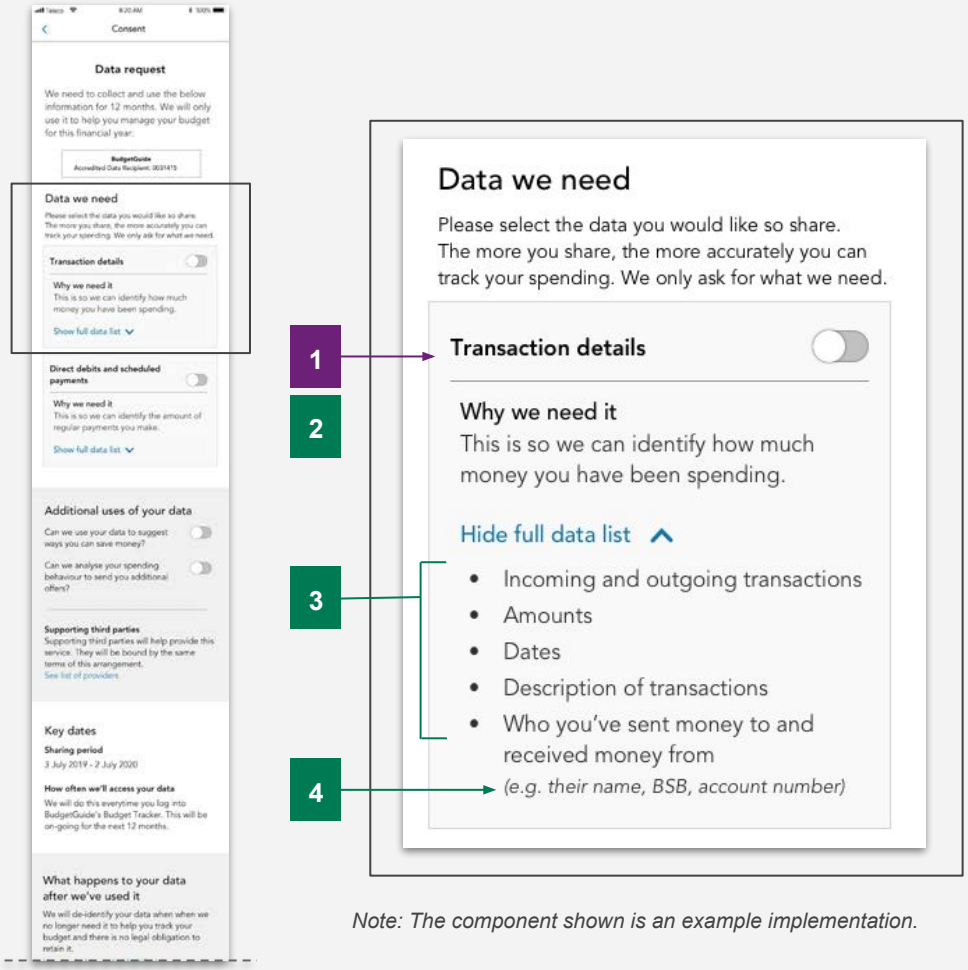
2 Data recipients **SHOULD** make the consent process as easy to understand as possible.

Data recipients **SHOULD** nudge consumers to be more privacy conscious and **SHOULD** use appropriate interventions to mitigate cognitive overload, facilitate comprehension, and provide transparency and consumer control.

This can be done in a variety of ways, including through the use of design patterns like progressive disclosure, micro and/or descriptive copy, and with the use of microinteractions.

CX Research 8, 19





Note: The component shown is an example implementation.

Consent | Data request

Data clusters and permissions (4)

CDR Rule

1 Data Language Standards **MUST** be used for data clusters and permission language.

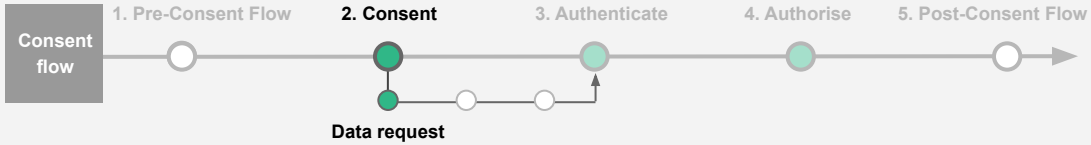
CDR Rule 8.11(d)

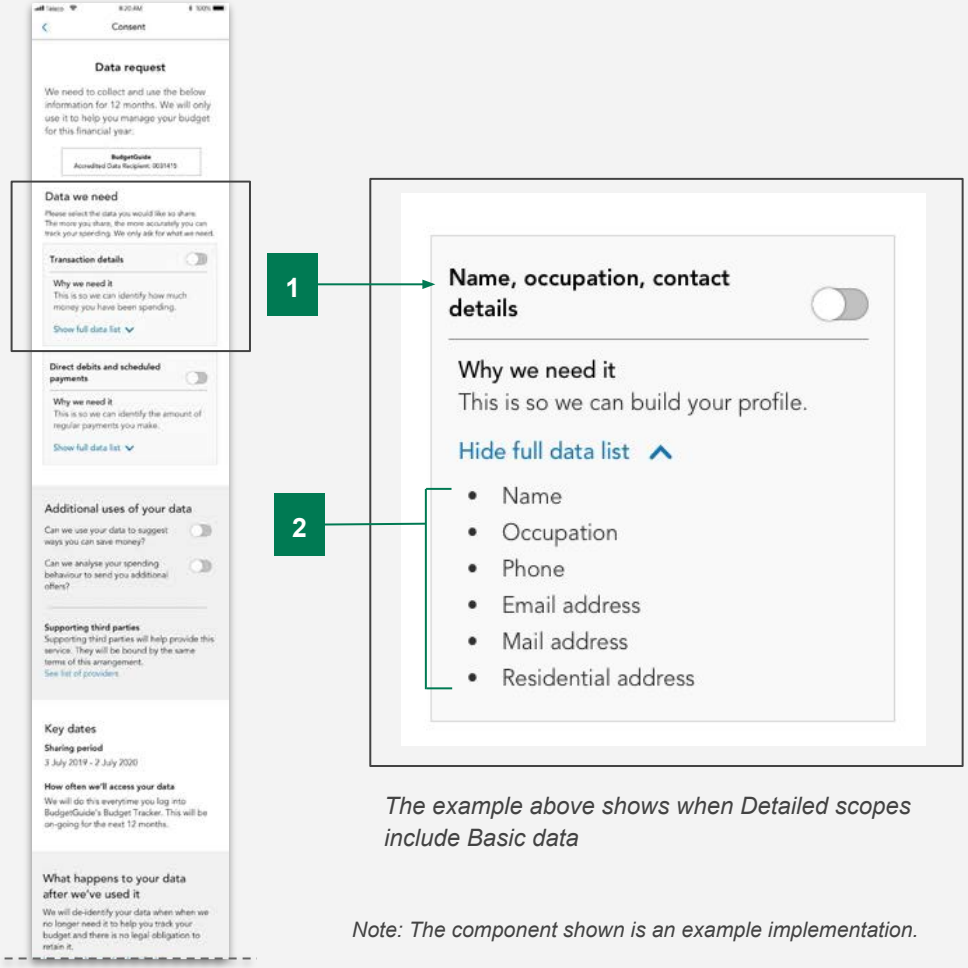
CX Standard

2 3 Data recipients and data holders **MUST** use Data Language Standards to describe data clusters and permissions in consumer-facing interactions as outlined in the Data Language Standards table.

- 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 the table.
- Data recipients and data holders **SHOULD** expand on the proposed language where appropriate to communicate further details of what is being shared.
    - 4 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 the table

Data Language Standards





The example above shows when Detailed scopes include Basic data

Note: The component shown is an example implementation.

Consent | Data request

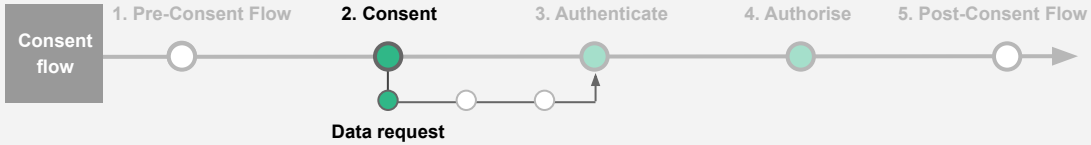
Data clusters and permissions (5)

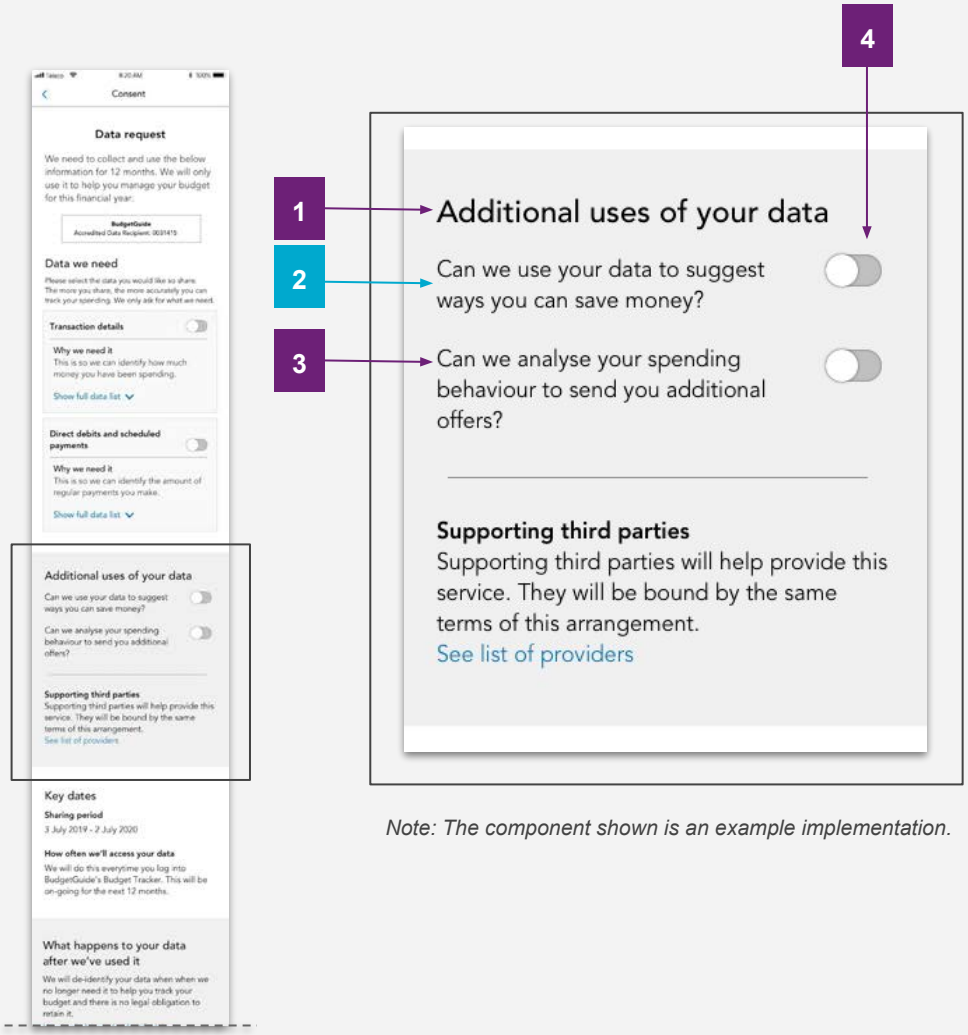
CX Standard

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.

1 **2** Data holders and data recipients **MUST** use the alternative language denoted with an '‡' in the Data Language Standards table.

Data Language Standards





Note: The component shown is an example implementation.

Consent | Data request

Additional usage of data (1)

CDR Rule

1 Data recipients **MUST NOT** ask the consumer to give consent for the purpose of selling their CDR data unless it is de-identified in accordance with the CDR de-identification process.

CDR Rules 4.12(3)(a)

CX Guideline

2 Data recipients **SHOULD** structure the 'purpose' and 'use' statements in ways that:

1. Are specific as to purpose *(e.g. 'Why we need it' for each data cluster)*
2. Refer to the broader 'use case' or 'uses' *(e.g. 'to pre-populate your application')*
3. Relate to the product/service being provided *(e.g. 'so BudgetGuide can help you manage your budget')*

This information **SHOULD** be framed in a way that communicates the benefit of data sharing to the consumer.

CDR Rule

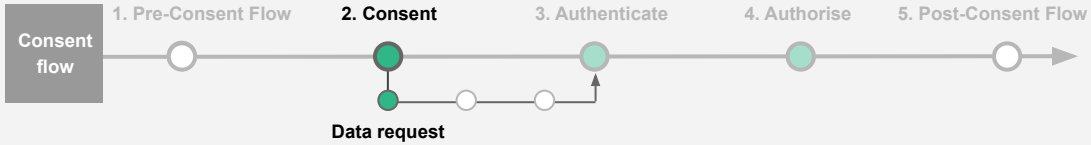
3 Data recipients **MUST** ask to consent to any direct marketing the data recipient intends to undertake.

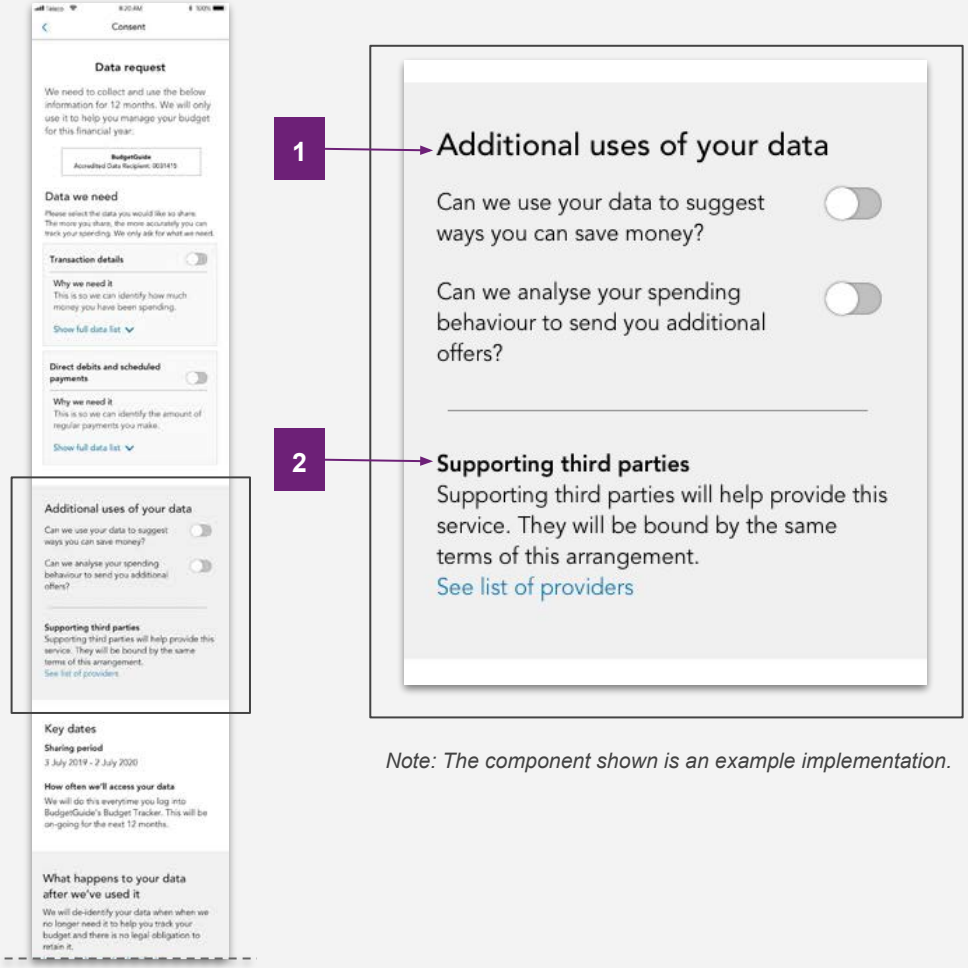
CDR Rules 4.11(1)(c)(iii), 7.5(3)(a), (b)

CDR Rule

4 Data recipients **MUST** allow the consumer to choose the types of CDR data to be collected and used by enabling the CDR consumer to actively select or otherwise clearly indicate the specific uses of that data to which they are consenting.

CDR Rule 4.11(1)(a)(ii)





Note: The component shown is an example implementation.

Consent | Data request

Additional usage of data (2)

CDR Rule

1 If data recipients seek consumer consent to de-identify some or all of their CDR data for the purpose of disclosing (including by selling) that de-identified data, they **MUST** provide the following information:

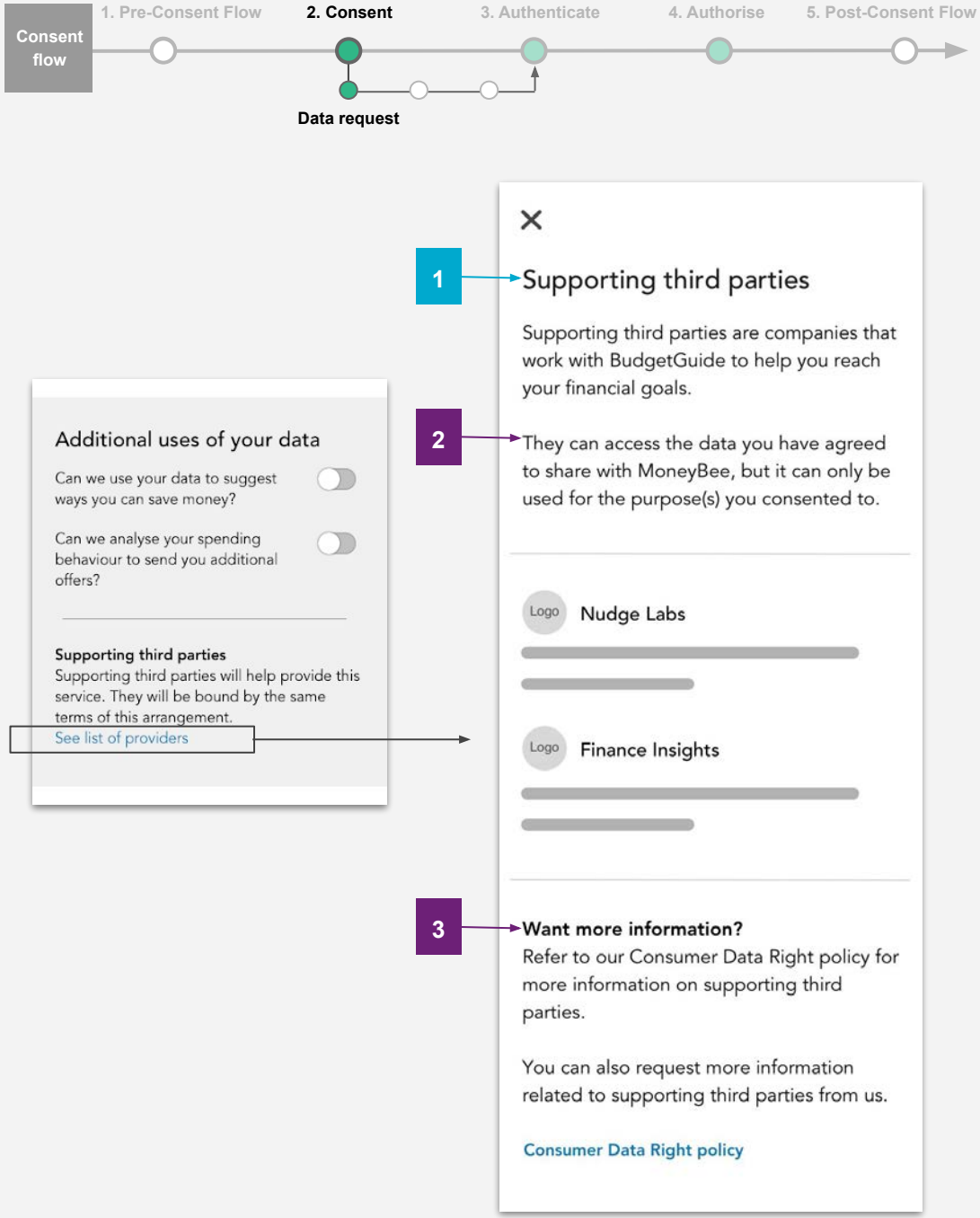
- what the CDR data de-identification process is;
- that it would disclose (by sale or otherwise) the de-identified data to one or more other persons;
- the classes of persons to which it would disclose that data;
- why it would so disclose that data;
- that the CDR consumer would not be able to elect, in accordance with rule 4.16, to have the de-identified data deleted once it becomes redundant data.

CDR Rules 4.11(3)(e); 4.15

CDR Rule

2 Data recipients **MUST** ensure that if it discloses CDR data to an outsourced provider, those providers must comply with the same requirements as the data recipient. See the section on outsourced providers for more information.

CDR Rules 1.16



Note: The component shown is an example implementation.

Consent | Data request

Outsourced providers

CX Guideline

1 Data recipients **SHOULD** present useful information regarding outsourced providers found in the CDR policy to consumers so they can easily access this information.

CDR Rule

2 Data recipients **MUST** ensure that if it discloses CDR data to an outsourced provider, those providers must comply with the same requirements as the data recipient.

CDR Rules 1.16

CDR Rule

3 If data may be disclosed to outsourced providers data recipients **MUST** state this, provide a link to the data recipient's CDR policy and a statement that the consumer can obtain further information relating to this policy.

CDR Rules 4.11(3)(f)

CDR Rule

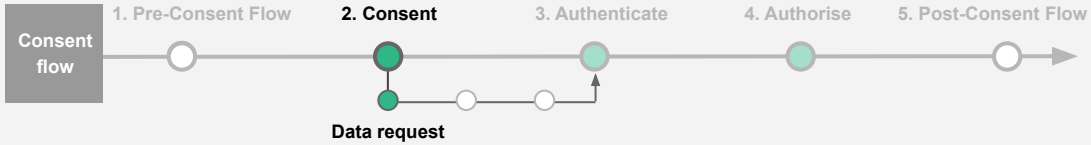
If data becomes redundant, data recipients **MUST** direct any outsourced provider that has been provided with a copy of such data to either:

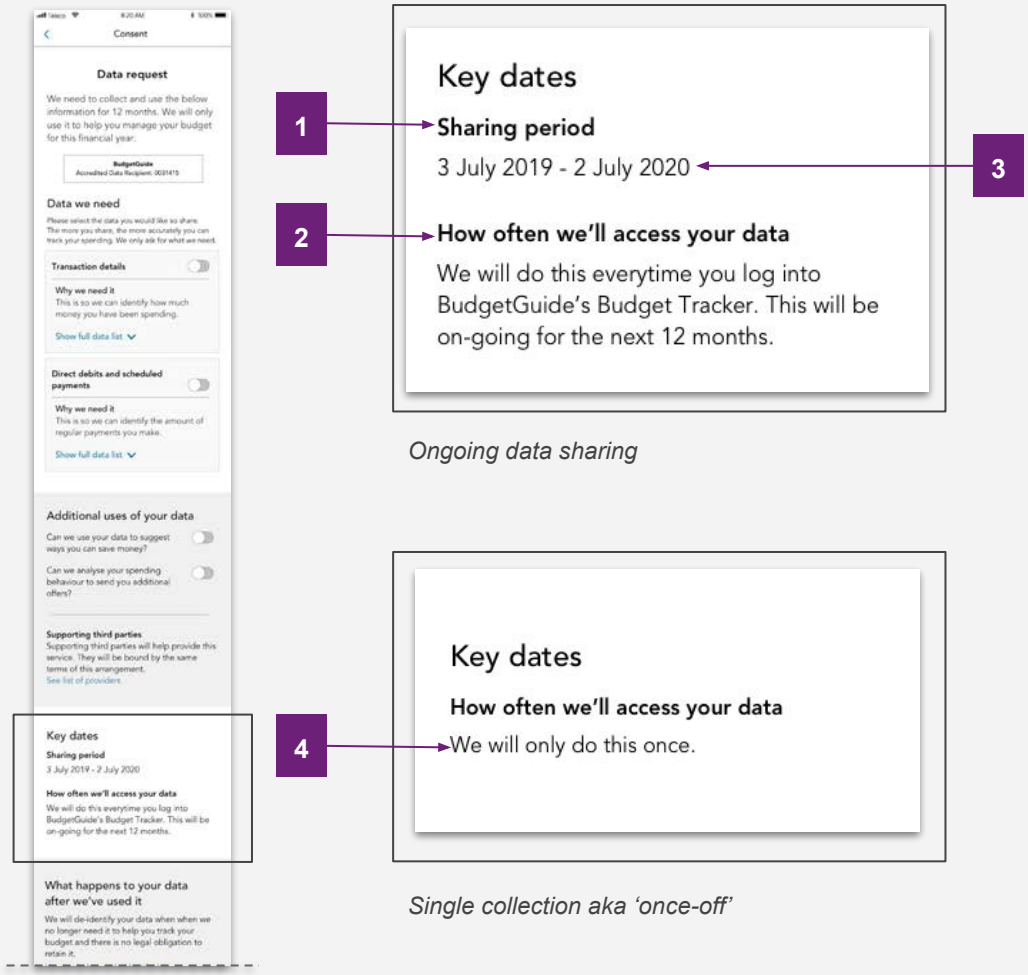
- return the redundant data to the data recipient; or
- delete the redundant data, as well as any CDR data that has been directly or indirectly derived from it, and notify the data recipient of the deletion

If the outsourced provider has provided any such data to another person, the data recipient **MUST** direct the outsourced provider to direct said person to:

- take either of the above mentioned steps; and
- cause similar directions to be made to any person to whom such data has been further disclosed

CDR Rules 7.12(2)(b)





Ongoing data sharing

Single collection aka 'once-off'

Note: The components shown are examples of implementation.

Consent | Data request

Duration

CDR Rule

1 Data recipients **MUST** allow the consumer to choose the period over with CDR data will be collected and used by enabling the consumer to actively select or otherwise clearly state if they are requesting consent for a single collection (aka once-off) or for collection over a period of time of not more than 12 months (aka ongoing).

CDR Rule 1.14(3)(d), 4.11(1)(b), 4.12(1) | CX Research 4, 5, 6

CDR Rule

2 4 Data recipients **MUST** outline how often data is expected to be collected over that period.

CDR Rule 1.14(3)(e) | CX Research 3, 4, 5, 6

CDR Rule

Data recipients **MUST** apply the data minimisation principle to the collection of historical data as well as the sharing duration into the future.

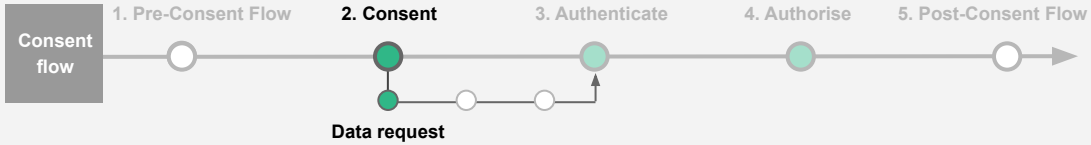
CDR Rule 1.8, 4.4(1)(d), 4.12(2) | CX Research 3, 4, 5, 6

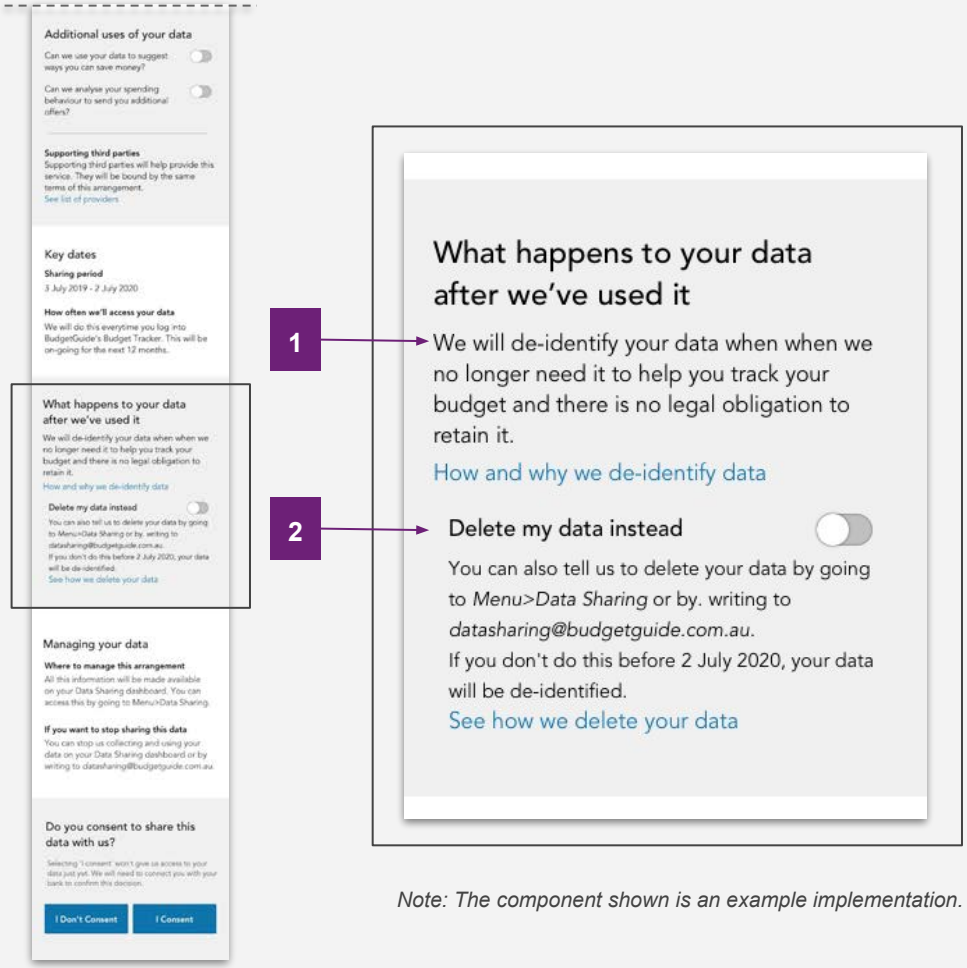
CDR Rule

Consent to collect and use CDR data expires:

- When the data recipient actioned on the consumer's withdrawal request
- When the data recipient was notified by the data holder that the consumer has withdrawn authorisation
- 3 12 months after consent was given or the end of the duration period consented by the consumer
- When the data recipient's accreditation is revoked or surrendered

CDR Rule 4.14(1)(a)-(e), 4.14(2)





Note: The component shown is an example implementation.

Consent | Data request

Handling of redundant data

CDR Rule

1 2 Data recipients **MUST** outline what is the intended treatment of redundant data and a statement that outlines the consumer's right to have this data deleted and instructions on how to to make this request.

CDR Rule 4.11(3)(h)

CDR Rule

1 Data recipients **MUST** state whether they have a general policy, when collected CDR data becomes redundant data, of:

A. deleting the redundant data; or
B. de-identifying the redundant data; or
C. deciding, when the CDR data becomes redundant, whether to delete it or de-identify it.

CDR Rule 4.17(1)

CDR Rule

2 Data recipients **MUST** allow the consumer to choose to have their redundant data deleted if they do not have a general policy of deleting redundant CDR data.

The consumer **MAY** choose to have redundant data deleted during the process of giving consent to the collection and use of data.

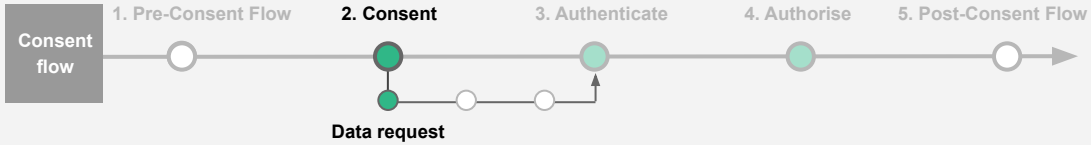
CDR Rules 4.11(1)(e), 4.16(1)(a), 4.16(3) | CX Research 18

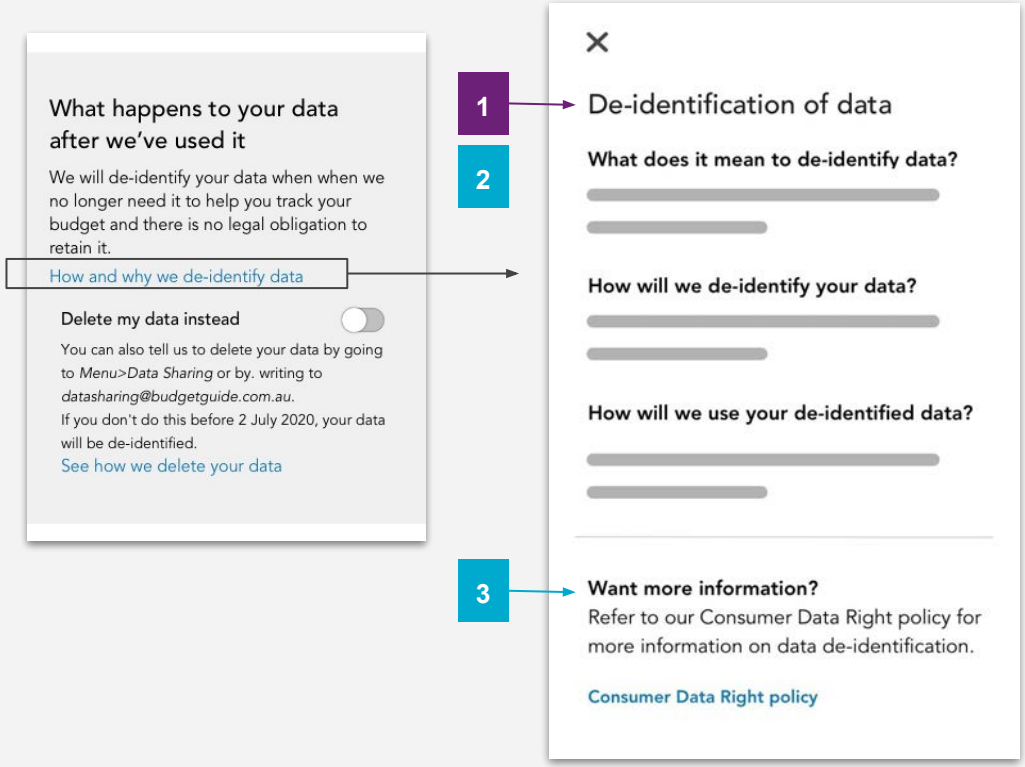
CX Guideline

Most research participants expected their data to be deleted when sharing was withdrawn or expired. Data recipients can avoid the election step within the consent flow if they have general policy of deletion.

If data recipients need to include this in-flow election, they **SHOULD** allow the consumer to elect that they 'remember' their preference for subsequent requests.

CX Research 18





Note: The component shown is an example implementation.

Consent | Data request

De-identification

CDR Rule

1 When asking for consent, data recipients **MUST** give information on the handling of de-identified data if they plan to de-identify some or all of the consumer's collected CDR data for the purpose of disclosing this data.

The **MUST** also indicate how it would comply with the data minimisation principle.

CDR Rules 4.11(3)(e), 4.11(3)(Note), 4.15

CDR Rule

1 Data recipients **MUST** state the following if redundant data is to be de-identified:

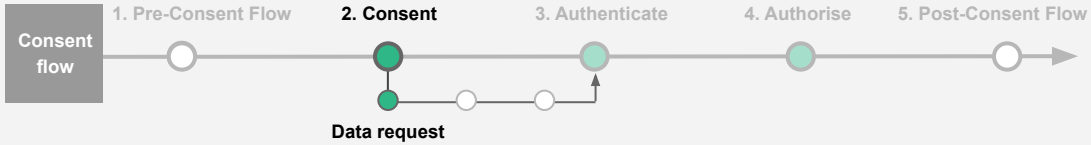
- That they will apply the CDR de-identification process
- That de-identified data will be used without further consent
- What de-identification of CDR data de-identification process means
- Examples of how they plan to use the de-identified data

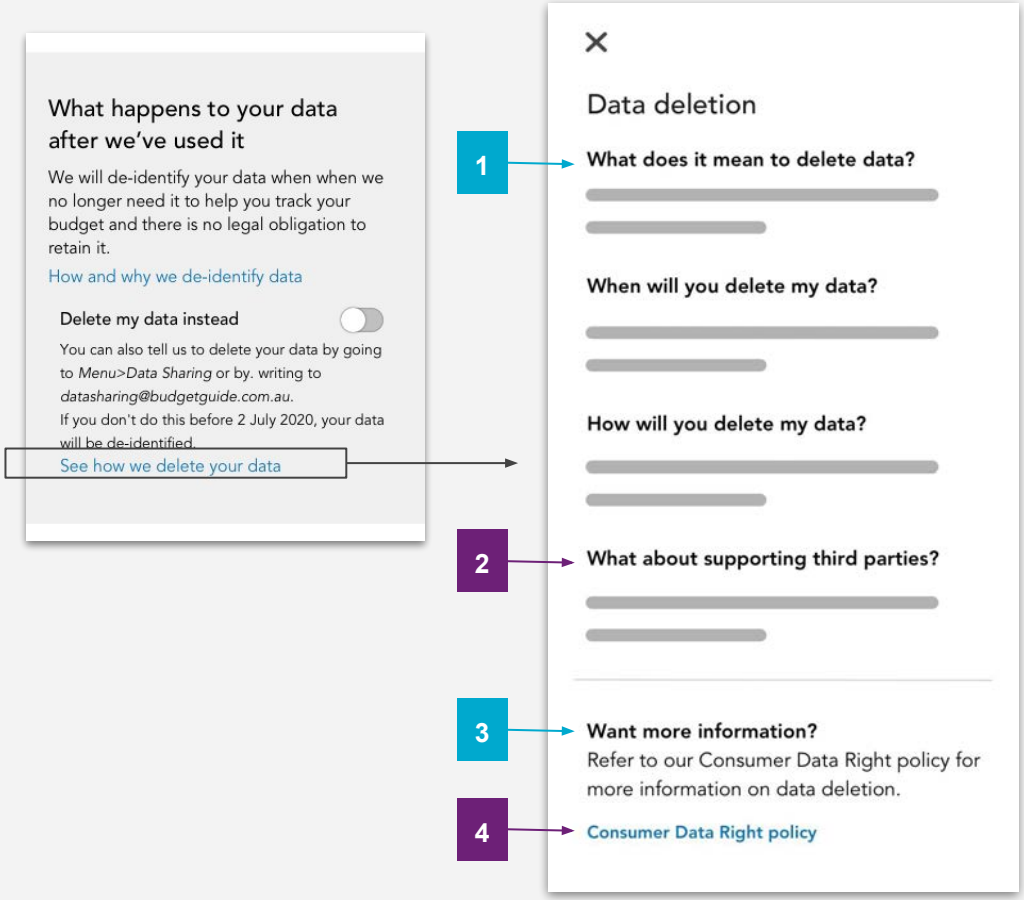
CDR Rules 4.17(2)

CX Guideline

2 Data recipients **SHOULD** present useful information regarding de-identification of data found in the CDR policy to consumers so they can easily access this information.

3 Data recipients **SHOULD** also provide a link to the CDR policy.





Note: The component shown is an example implementation.

Consent | Data request

Data deletion

CX Guideline

1 Data recipients **SHOULD** present useful information regarding deletion of data found in the CDR policy to consumers so they can easily access this information.

3 Data recipients **SHOULD** also provide a link to the CDR policy.

CDR Rule

2 Data recipients **MUST** direct any outsourced provider that has been provided with a copy of the redundant data to either:

- return the redundant data to the data recipient; or
- delete the redundant data, as well as any CDR data that has been directly or indirectly derived from it, and notify the data recipient of the deletion

If the outsourced provider has provided any such data to another person, the data recipient **MUST** direct the outsourced provider to direct said person to:

- take either of the above mentioned steps; and
- cause similar directions to be made to any person to whom such data has been further disclosed

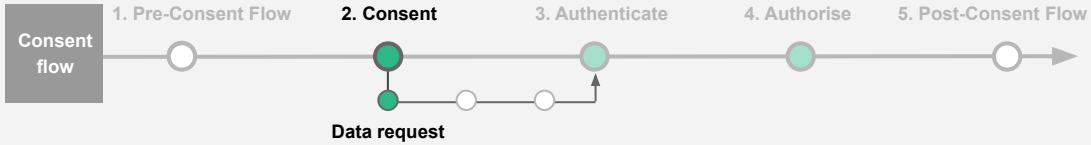
CDR Rules 7.12(2)(b)

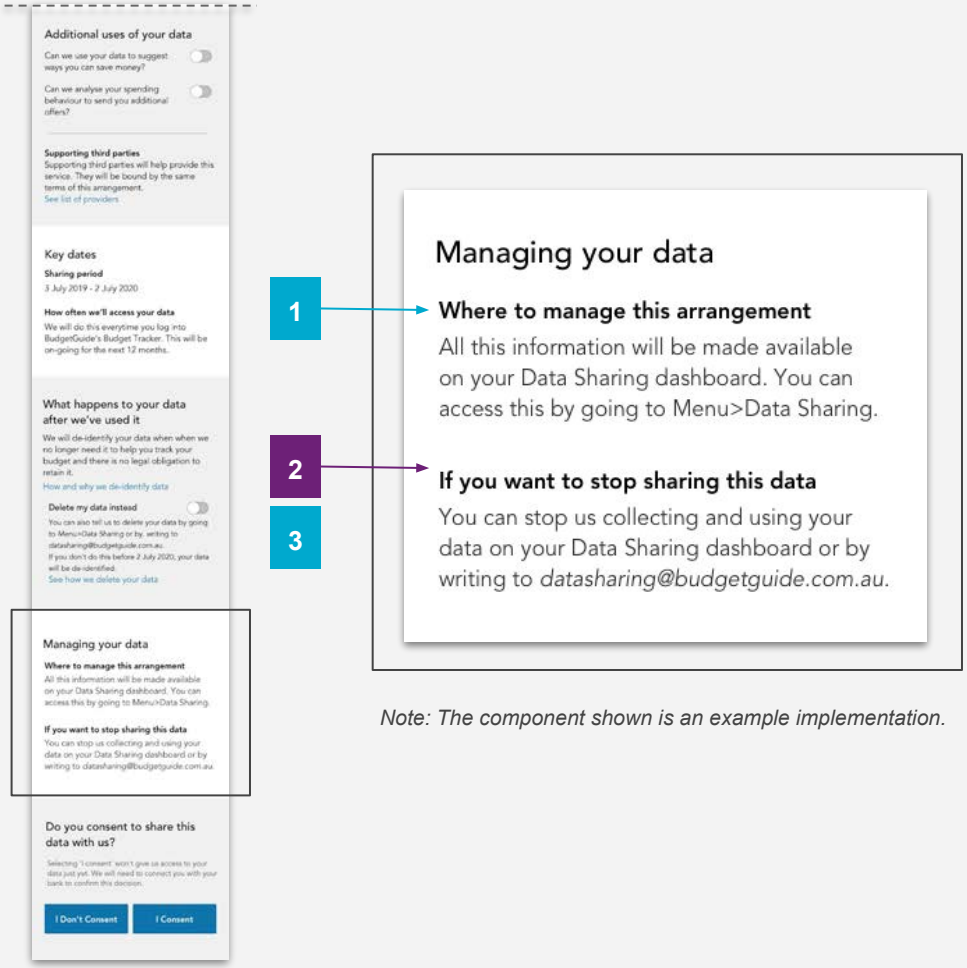
CDR Rule

4 A data recipient's CDR policy **MUST** include, if and where applicable, the following information about the deletion of redundant CDR data:

- when redundant data is deleted
- how a CDR consumer may elect for deletion to occur
- how redundant data is deleted

CDR Rules 7.2(4)(f)





Note: The component shown is an example implementation.

Consent | Data request

Review and Withdraw

CX Guideline

1 Data recipients **SHOULD** state that the sharing arrangement would be made available on the consumer dashboard.

CX Research 26

CDR Rule

2 Data recipients **MUST** include a statement that consent can be withdrawn at anytime, instructions on how to do it and any consequences arising from consent withdrawal.

CDR Rules 4.11(3)(g)

CDR Rule

2 Data recipients **MUST** allow consent to be withdrawn by the consumer at any time by communicating the withdrawal to the data recipient in writing or by using the data recipient's consumer dashboard.

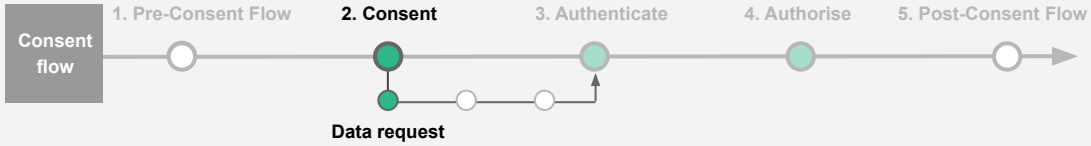
If consent is withdrawn via communication in writing, the data recipient **must** do so as soon as possible or within 2 business days of receiving this request.

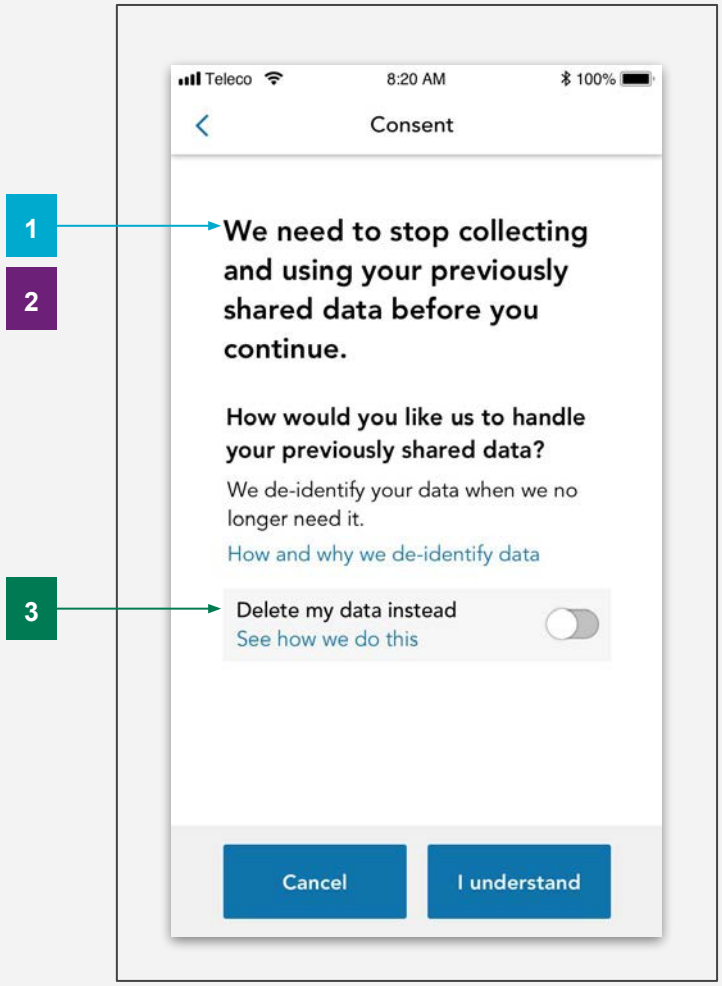
CDR Rules 4.13(1), 4.13(2)(a) | CX Research 15, 31, 32

CX Guideline

3 Data recipients **SHOULD** use the phrase 'Stop Sharing' to refer to how a consumer can withdraw authorisation.

CX Research 29





Note: The component shown is an example implementation.

Consent | Subsequent Consent

Withdrawal of Previous Consent

CX Guideline

1 Prior to November 2020, at which time concurrent consents will be given effect under the rules and standards, an existing consent **MUST** be withdrawn before a new consent can be established.

Data recipients **MAY** choose to do this by providing a step prior to or in the course of providing a new consent.

Data recipients **SHOULD** determine the appropriate location, language, and presentation of this withdrawal process.

This process **MUST** have regard to the relevant CDR Rules, CX Standards, and CX Guidelines for withdrawal of consent to collection and use.

CDR Rule

2 Data recipients **MUST** allow consent to be withdrawn by the consumer at any time by communicating the withdrawal to the data recipient in writing or by using the data recipient's consumer dashboard.

Where a consumer chooses to replace an existing consent with a new consent, data recipients **MUST** similarly enable consent to be withdrawn by the consumer prior to or in the course of providing a new consent.

If consent is withdrawn via communication in writing, the data recipient **must** do so as soon as possible or within 2 business days of receiving this request.

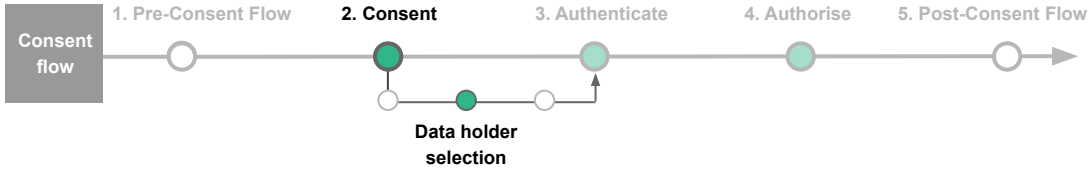
CDR Rules 4.13(1), 4.13(2)(a) | CX Research 15, 31, 32

CX Standard

3 If a Data recipient does not have a 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).



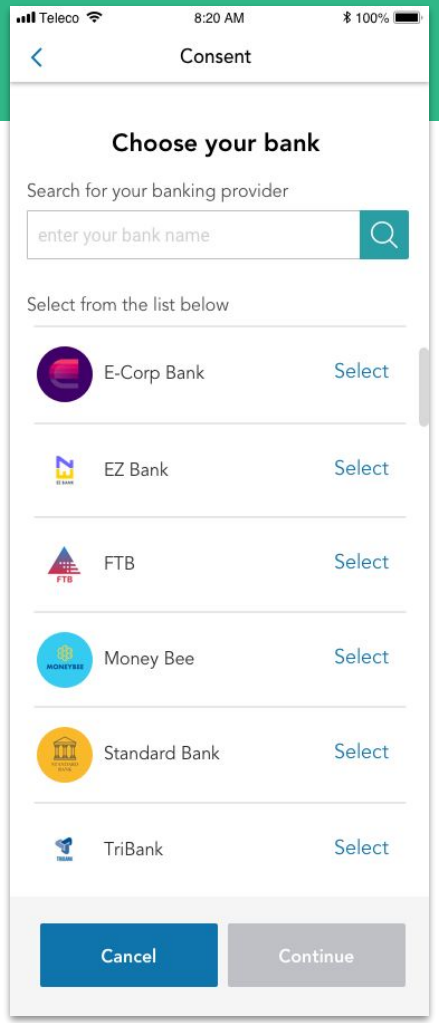
Consent | Data holder selection

This section provides examples illustrating how the guidelines may be implemented, in particular focusing on providing consumers with the ability to select a data holder to share data from.

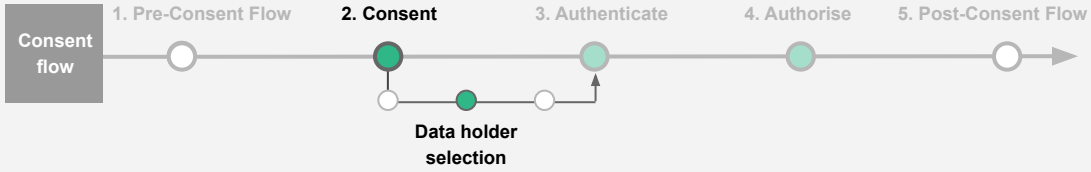
Selecting a data holder can occur before or after the data request.

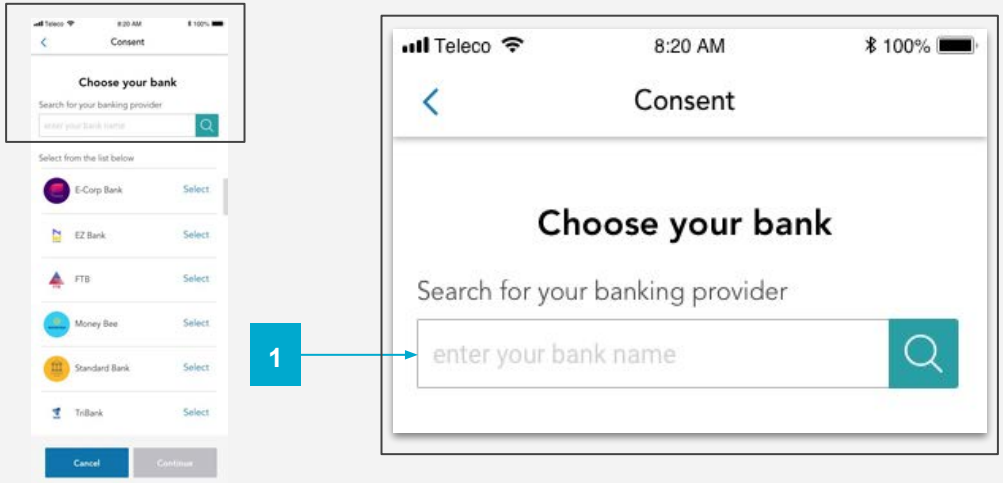
In this version of the CX Guidelines, guidance is only provided for selecting one data holder at a time.

Data recipients should consider the implications of allowing multiple data holders to be selected as part of the consent process. This method of reducing friction would compromise the quality of consent in certain scenarios.



Example wireframe





Note: The component shown is an example implementation.

Consent | Data holder selection

Data holder selection 1

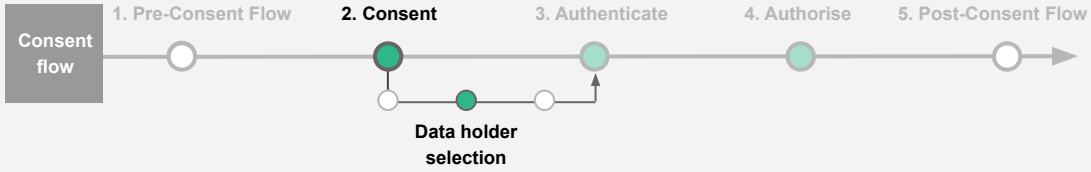
CX Guideline

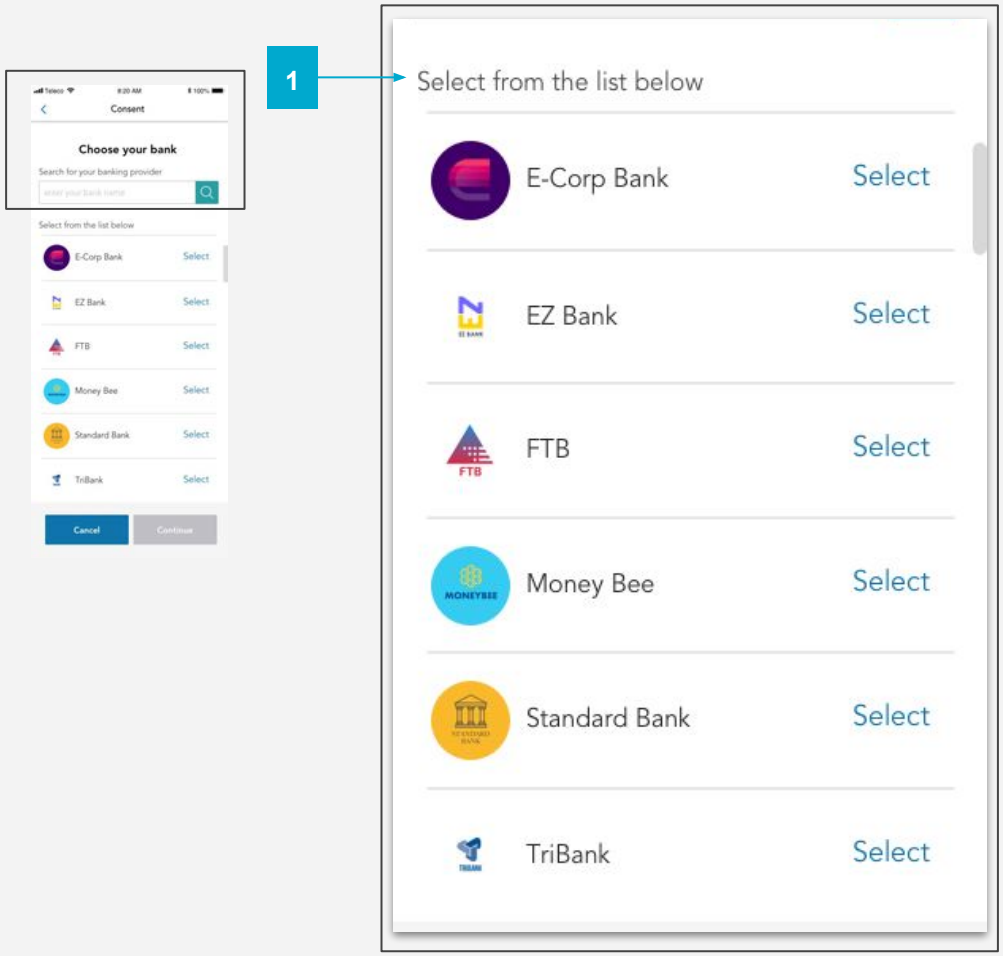
Data recipients **MAY** choose to present data holder selection screens before or after the data request occurs.

CX Guideline

1 Data recipients **SHOULD** make the data holder list searchable if the number of data holders exceeds what can be displayed on the screen.

10 Usability Heuristics for User Interface Design: Flexibility and efficiency of use (Nielsen)





Note: The component shown is an example implementation.

Consent | Data holder selection

Data holder selection 2

CDR Rule

In order to provide goods or services that the consumer as requested, it **MAY** be necessary for data recipients to request CDR data from more than one data holder.

CDR Rule 4.3(2)(Note 1), 4.4(2)(Note 1)

CX Guideline

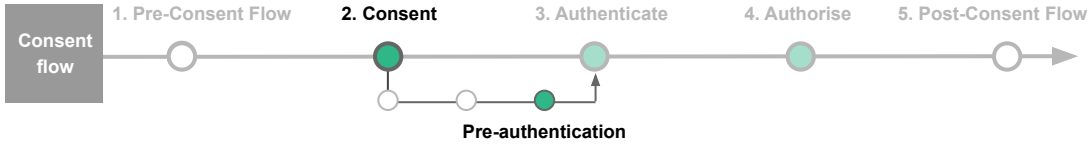
Data recipients **SHOULD** consider the implications of allowing multiple data holders to be selected in this step as it may impact the quality of consent.

Example: The data recipient allows the consumer to select several data holders at once, complete the authentication and authorisation process for one, and then allow the consumer to return at some point in the future to connect more data holders without reviewing the terms of consent again. This method of reducing friction would compromise the quality of consent if the time between data holder selection and authentication is too great.

CX Guideline

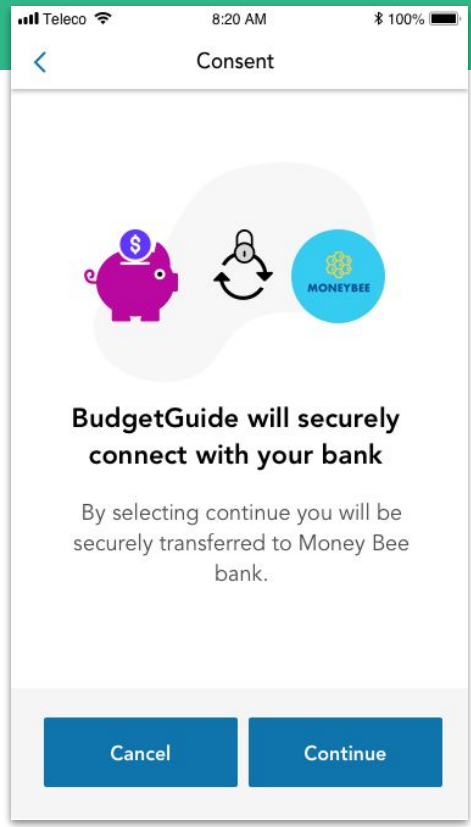
1 Data recipients **SHOULD** list data holders in alphabetical order.

10 Usability Heuristics for User Interface Design: Flexibility and efficiency of use (Nielsen)

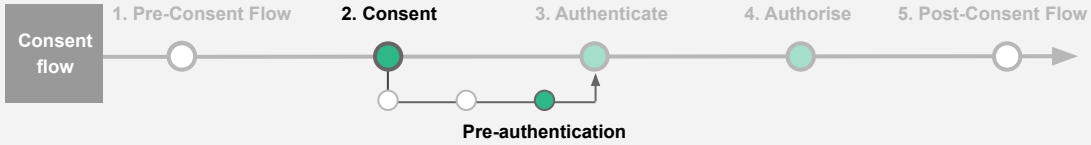


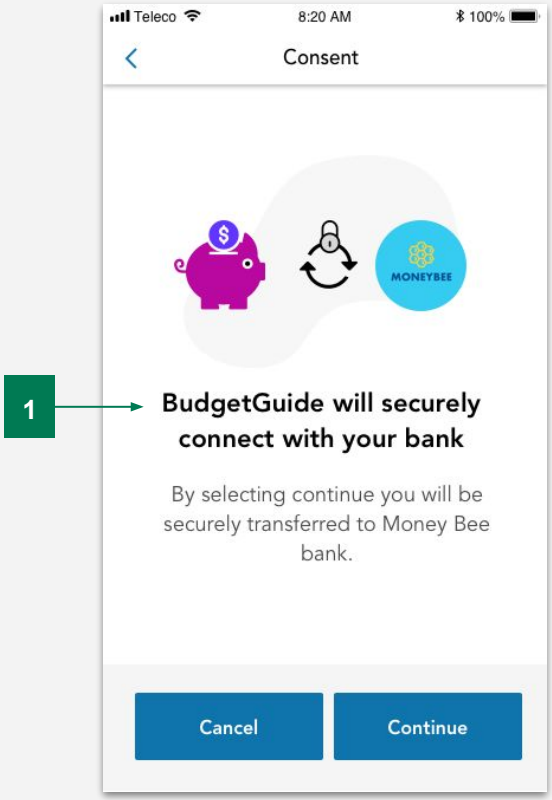
Consent | Pre-authentication

This section provides examples illustrating how the guidelines may be implemented, in particular focusing on how a consumer is redirected from the data recipient to a data holder for the purposes of authentication.



Example wireframe





Note: The screen shown is an example implementation.

Consent | Pre-authentication

Pre-authentication

CX Standard

1 Data recipients **MUST** notify consumers of redirection prior to authentication.

CX Research 21, 22

3. AUTHENTICATE

The DSB has determined that a single, consistent, authentication flow will be adopted by the CDR regime. The Security Profile supports the authentication flows specified by OpenID Connect as constrained further by FAPI (specifically the Hybrid Flow outlined in section 3.3). No other flows are currently supported.

The supported authentication flow is a type of redirection flow where the consumer's user agent is redirected from a data recipient's web site to a data holder's authorisation end point in the context of an authentication request. This flow incorporates aspects of both the implicit flow and authorisation code flow detailed under OpenID Connect.

Note that additional requirements for this flow are contained in the Authentication Flow section of the Security Profile.

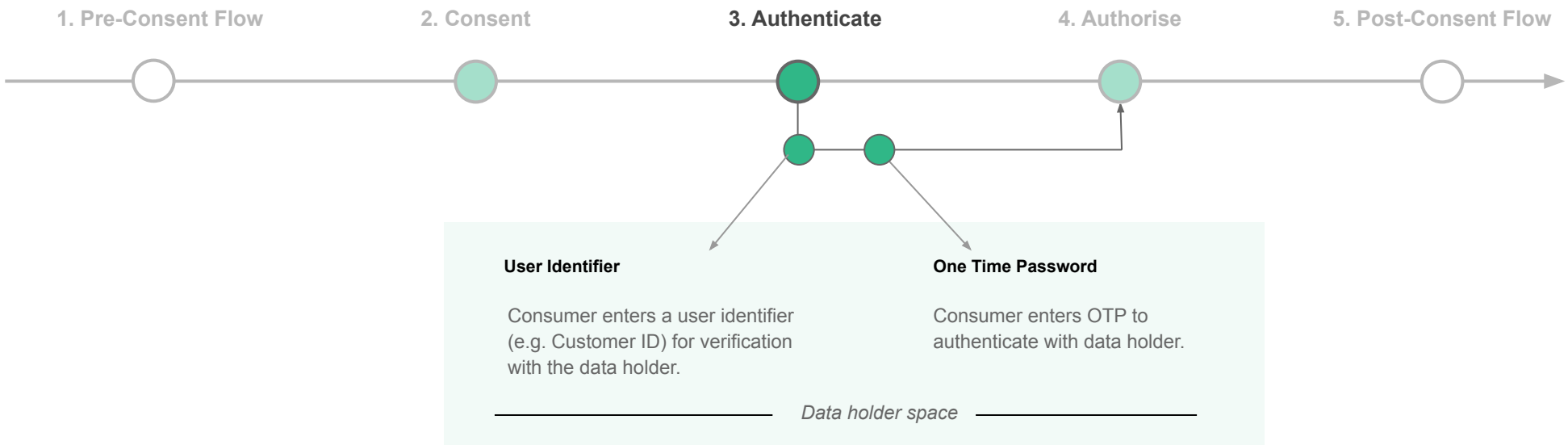
Using this model, the authentication stage is broken into two steps:

User Identifier

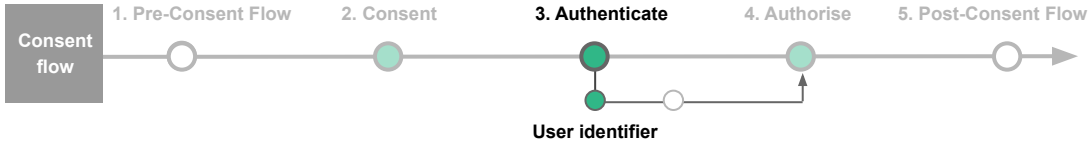
At this step, the consumer will be able to enter their user identifier (e.g. Customer ID) for verification with the data holder.

One Time Password

At this step, the consumer will be able to enter a One Time Password to complete the authentication step and securely connect to the data holder.



CONSUMER DATA STANDARDS



Authenticate | User identifier

This section provides examples of the flow where the consumer inputs a user identifier (e.g. customer ID).

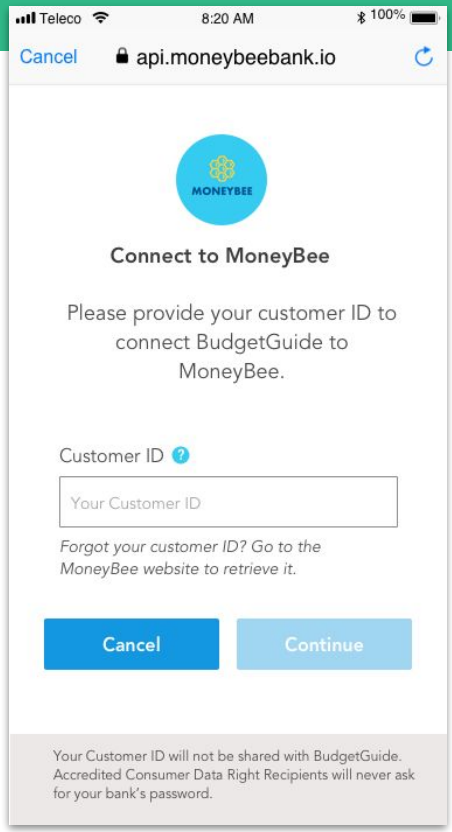
To build trust and consumer awareness across the CDR ecosystem, it is important that consumer education materials consistently emphasise that Accredited Consumer Data Right Recipients will never ask for a consumer's password to share CDR data.

Data Standard

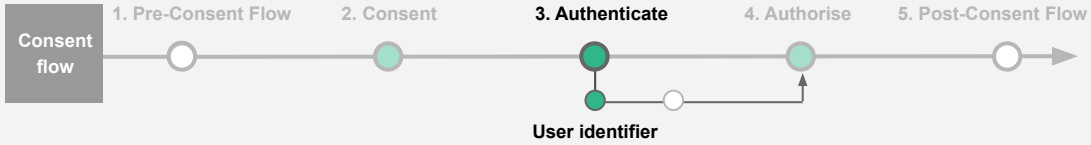
Data holders **MUST** request a user identifier that can uniquely identify the customer and that is already known by the customer in the redirected page.

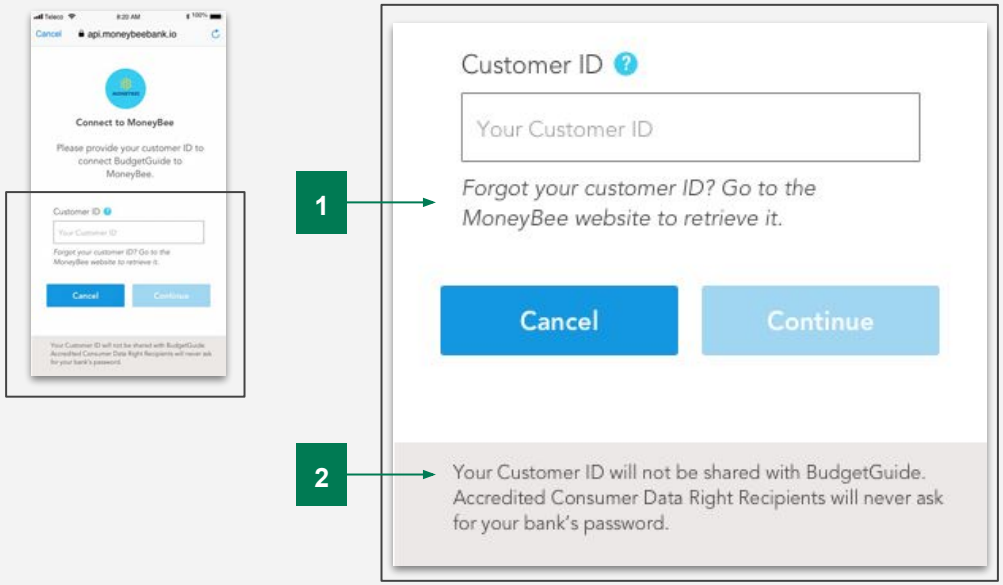
Data holders **SHOULD** implement additional controls to minimise the risk of enumeration attacks via the redirect page.

Security Profile



Example wireframe





Note: The component shown is an example implementation.

Authenticate | User identifier

User identifier request

CX Standard

1 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.

CX Research 21

CX Standard

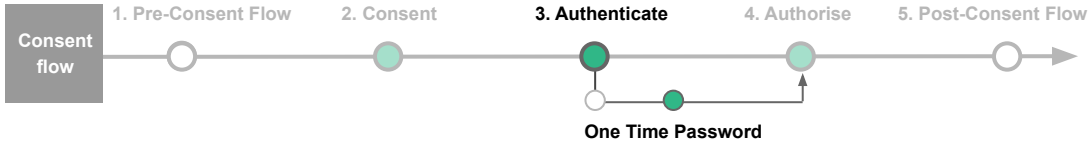
2 Data holders and data recipients **MUST** state in consumer-facing interactions and communications that services utilising the CDR do not need access to consumer passwords for the purposes of sharing data. The exact phrasing of this is at the discretion of the Data Holder and Data Recipient.

CX Research 21

CX Standard

2 The term(s) used to refer to a data recipient **SHOULD** align with any language proposed by the ACCC. These terms **SHOULD** be consistent throughout the consent flow.

10 Usability Heuristics for User Interface Design: Consistency and standards (Nielsen)



Authenticate | One Time Password

This section provides examples of how to use a One Time Password (OTP) to authenticate with a data holder.

The OTP **MUST** be delivered to the consumer through existing and preferred channels and be clearly described as a “One Time Password”.

Data Standard

Data Holders **MUST NOT** request that the customer enter an existing password in the redirected page.

Data Holders **MUST** provide a one-time password (OTP) to the customer through an existing channel or mechanism that the customer can then enter into the redirected page.

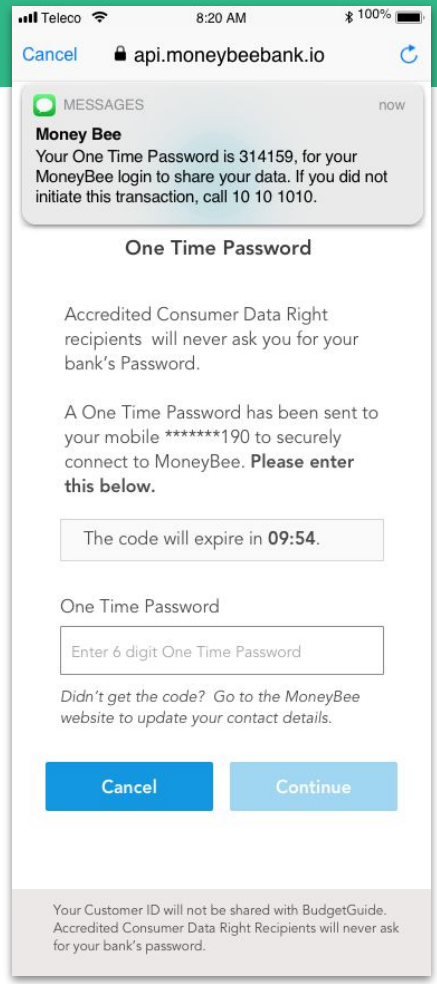
Data Holders **SHOULD** implement additional controls to minimise the risk of interception of the OTP through the selected delivery mechanism.

The provided OTP **MUST** be used only for authentication for CDR based sharing and **MUST NOT** be usable for the authorisation of other transactions or actions

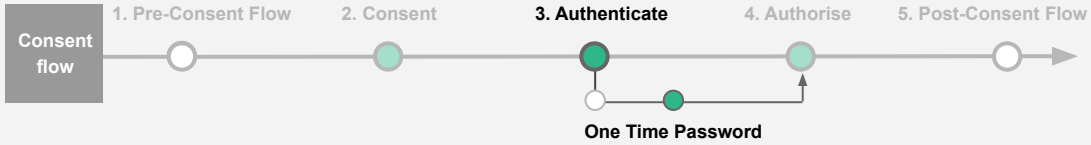
The provided OTP **MUST** be numeric digits and be between 4 and 6 digits in length

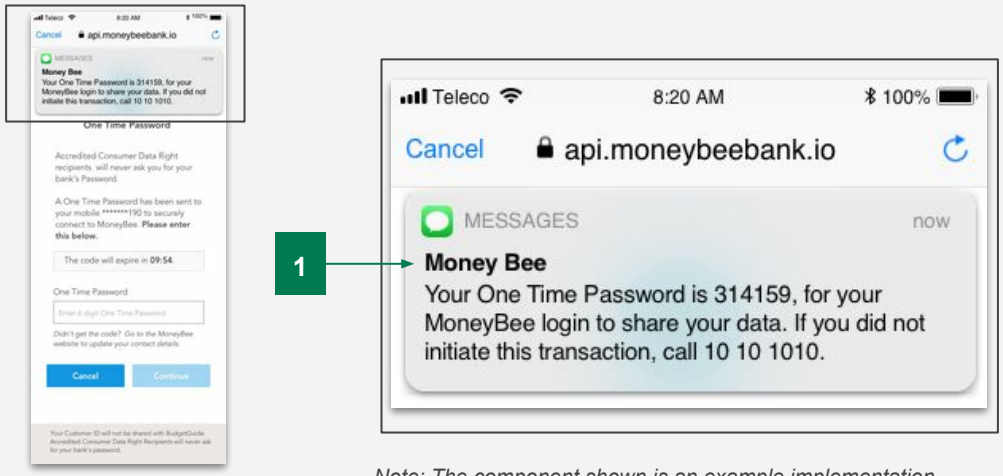
The algorithm for the creation of the OTP is at the discretion of the Data Holder but **SHOULD** incorporate a level of pseudorandomness appropriate for the use case

Security Profile



Example wireframe





Note: The component shown is an example implementation.

Authenticate | One Time Password

One Time Password delivery

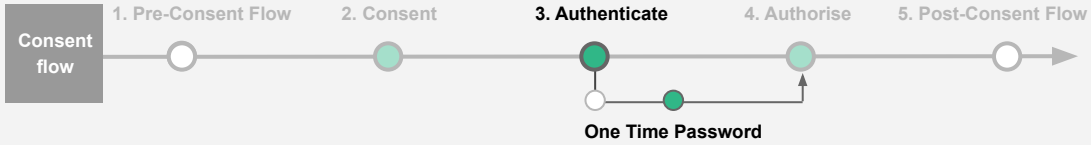
Data Standard

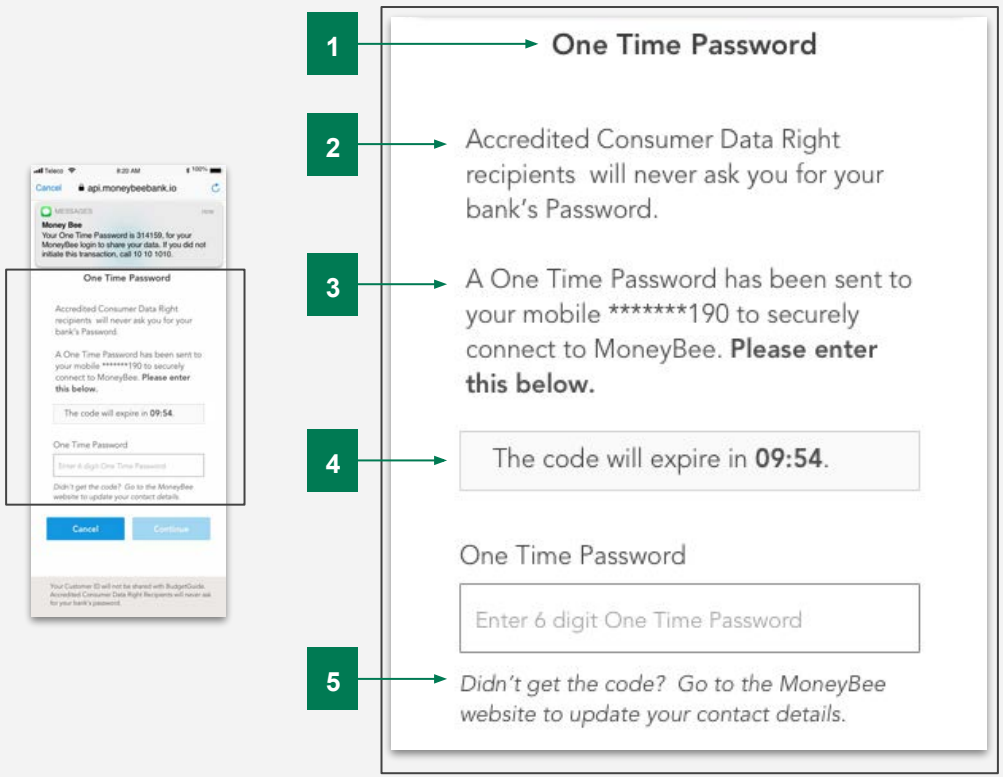
1 The delivery mechanism for the One Time Password (OTP) is at the discretion of the data holder but **MUST** align to existing and preferred channels for the customer and **MUST NOT** introduce unwarranted friction into the authentication process.

In line with CDR Rule 4.24 on restrictions when asking CDR consumers to authorise disclosure of CDR data, unwarranted friction for OTP delivery is considered to include:

- the addition of any requirements beyond normal data holder practices for verification code delivery
- providing or requesting additional information beyond normal data holder practices for verification code delivery
- offering additional or alternative services
- reference or inclusion of other documents

CX Research 12, 27 | Security Profile | CDR Rule 4.24





Note: The component shown is an example implementation.

Authenticate | One Time Password

One Time Password instructions

CX Standard

1 3 Data holders and data recipients **MUST** clearly refer to a "One Time Password" in consumer-facing interactions and communications. The use of 'verification code' and 'password' caused confusion and apprehension among consumers.

CX Research 10

CX Standard

2 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.

CX Research 21

Data Standard

4 The provided OTP **MUST** be invalidated after a period of time at the discretion of the Data Holder. This expiry period **SHOULD** facilitate enough time for the customer to reasonably complete the authorisation process.

CX Research 12, 27 | Security Profile

CX Standard

4 Data holders **MUST** communicate the expiry period of the OTP to the consumer in the authentication flow.

CX Research 12, 27

CX Standard

5 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.

CX Research 11

4. AUTHORISE

The data holder must seek authorisation from the consumer to disclose CDR data to an accredited data recipient. In accordance with CDR Rule 4.24, this process MUST NOT:

- add any requirements to the authorisation process beyond what is outlined in the data standards and the CDR rules.
- provide or request additional information during the authorisation process beyond what is specified in the data standards and the CDR rules.
- offer additional or alternative services as part of this authorisation process.
- include or refer to other documents.

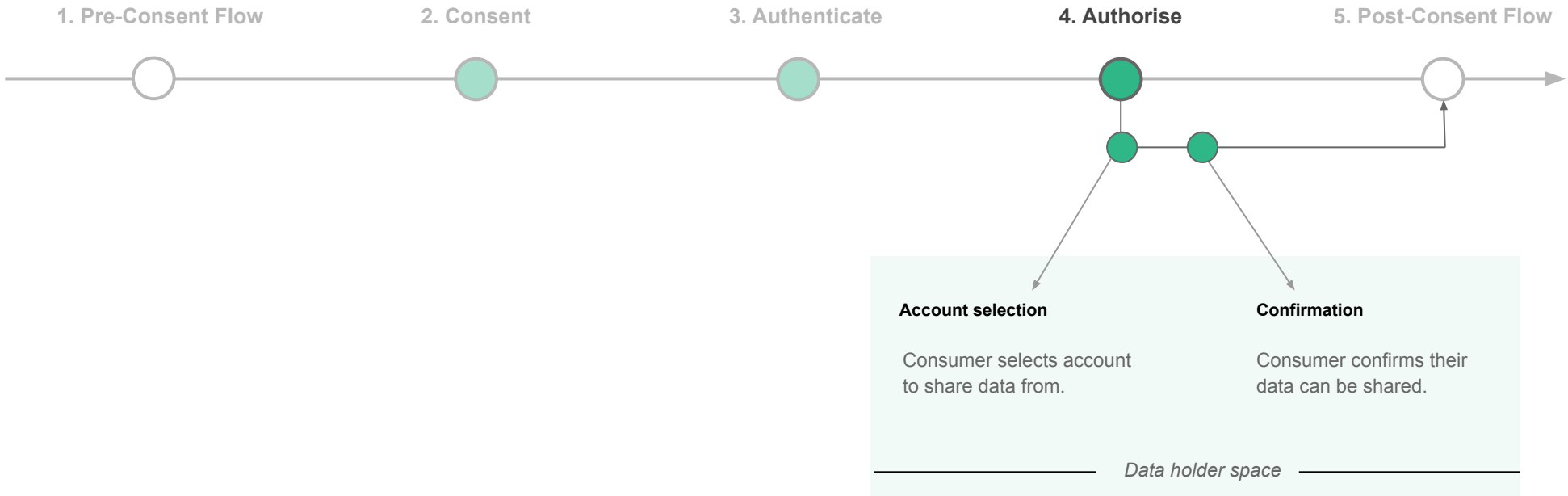
The Authorise stage is further broken down into two steps:

Account selection

At this step, the consumer will be able to select the account that they would like to share their data from.

Confirmation

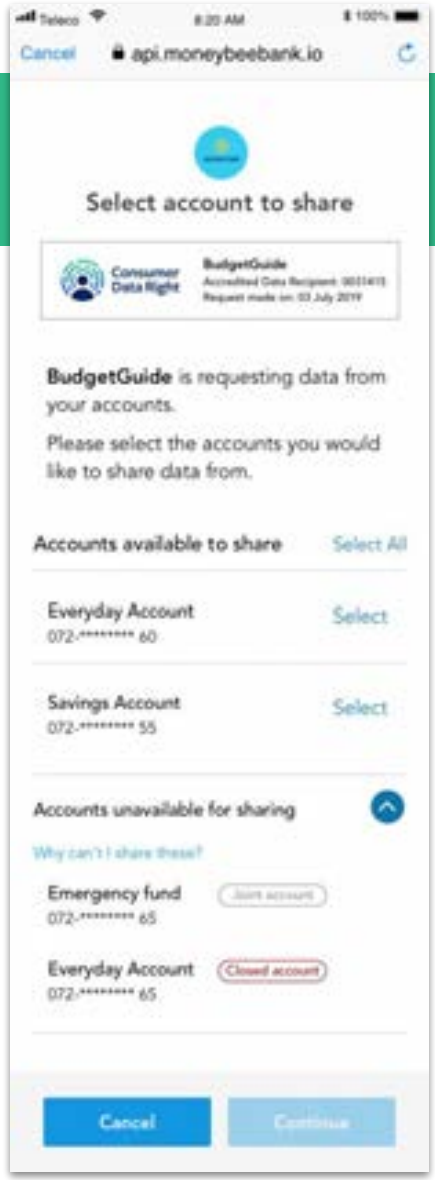
At this step, the consumer will be able to review and confirm the data from their account(s) that will be shared with the data recipient.



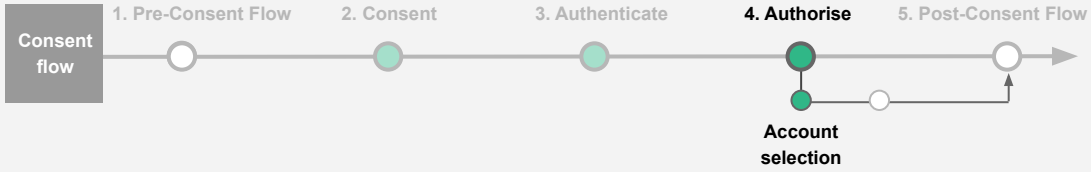
Authorise | Account selection

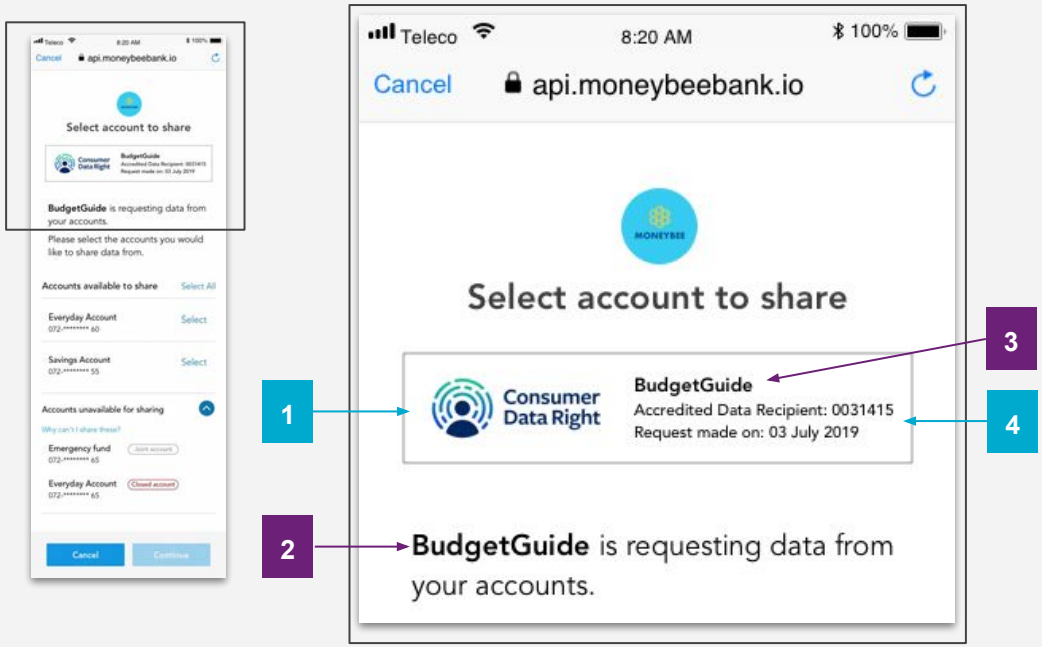
This section provides examples illustrating how the guidelines may be implemented, in particular focusing on the selection of account(s) from which data will be shared.

The data holder **MAY** add a 'profile selection' step prior to account selection if a single identifier provides access to different customer accounts (e.g. one customer ID gives access to business customer and an individual customer accounts). This addition **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).



Example wireframe





Note: The component shown is an example implementation.

Authorise | Account selection

Data recipient information

CDR Rule

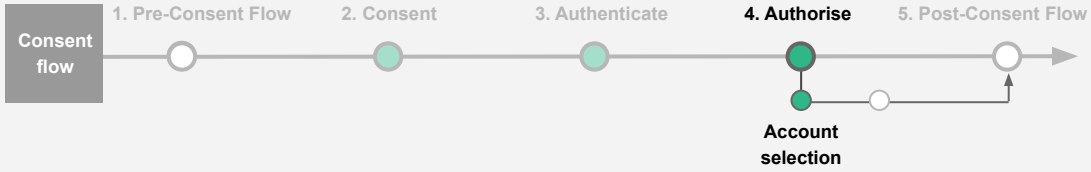
2 3 Data holders **MUST** state which data recipient is making the request. The data holder **SHOULD** show this information as soon as the authorisation flow begins.

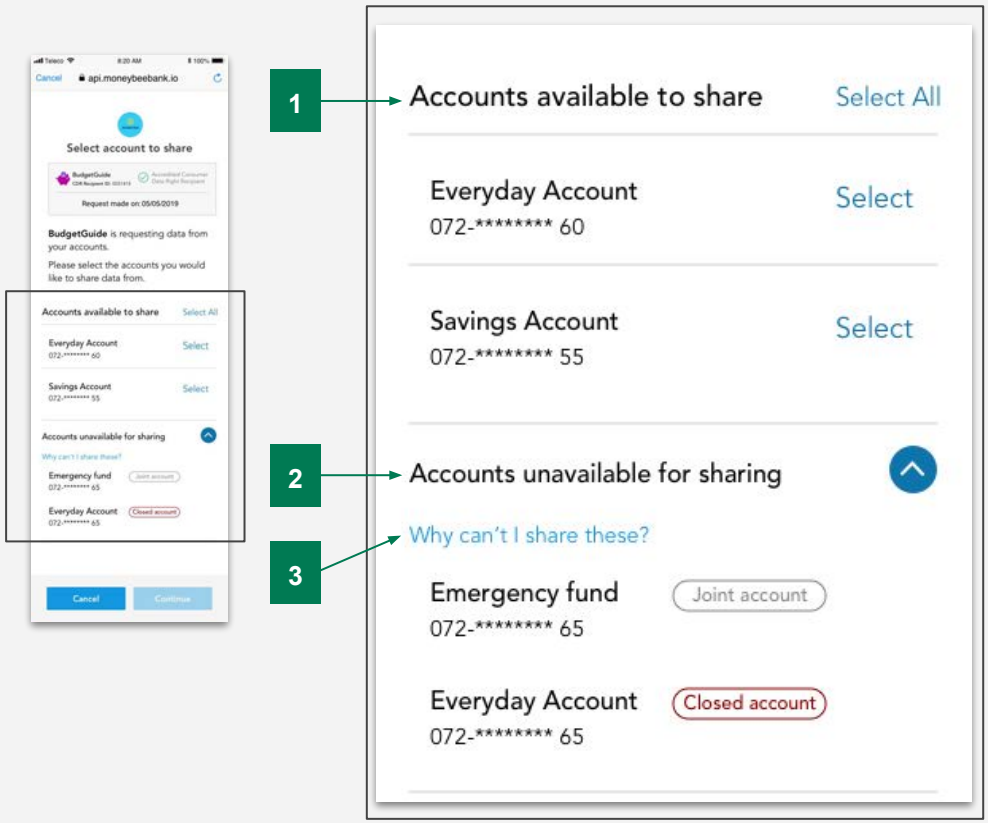
CDR Rule 4.23(a)

CX Guideline

1 4 Data holders **SHOULD** show the ACCC provided CDR branding and details of the request including a data recipient identifier, and the date the request was made.

CX Research 13, 23





Note: The component shown is an example implementation.

Authorise | Account selection

Account selection

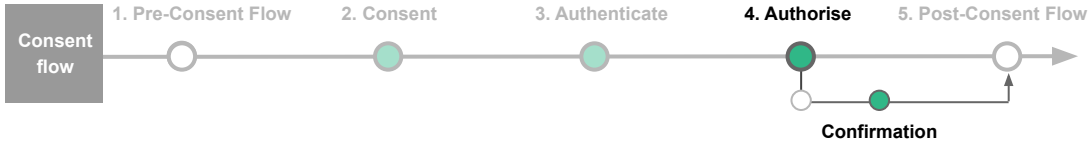
CX Standard

1 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.

Data holders **MAY** omit this step if none of the data being requested is specific to an account (e.g. Saved Payees).

- 2 If certain accounts are unavailable to share, data holders **SHOULD** show these unavailable accounts in the account-selection step.
    - 3 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.

CX Research 9



Authorise | Confirmation

This section provides examples illustrating how the guidelines may be implemented, in particular focusing on how the data holder should disclose information on data sharing authorisation.

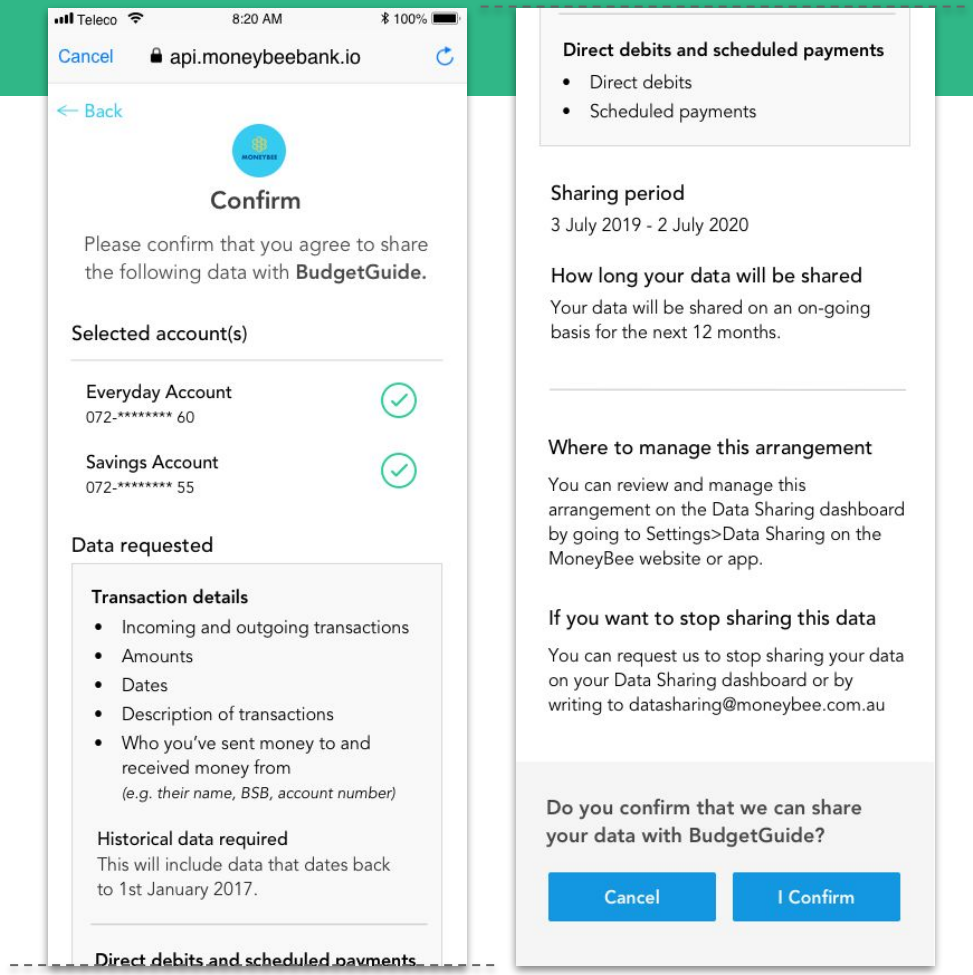
The data holder **SHOULD NOT** introduce any additional consumer-facing interactions, instructions, or communications except where legally required. This includes copy that may call into question the security of sharing data as part of the CDR, or introducing unnecessary friction (*CDR Rule 4.24*).

It must be clear to the consumer which data clusters are being requested and the language used to describe each data cluster **MUST** also align with the language recommendations presented earlier in the guidelines (refer to the section on Language requirements).

The sharing duration **SHOULD** be clearly stated in addition to whether data will be shared for a single instance or on an ongoing basis.

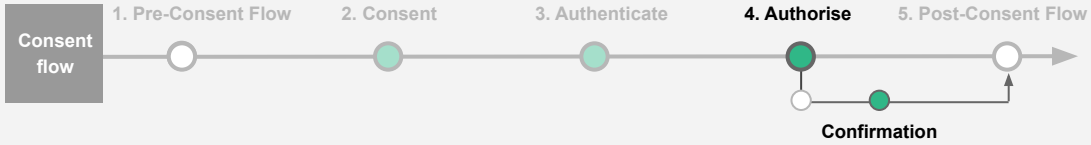
The actions required to withdraw consent **SHOULD** be clearly communicated to the consumer.

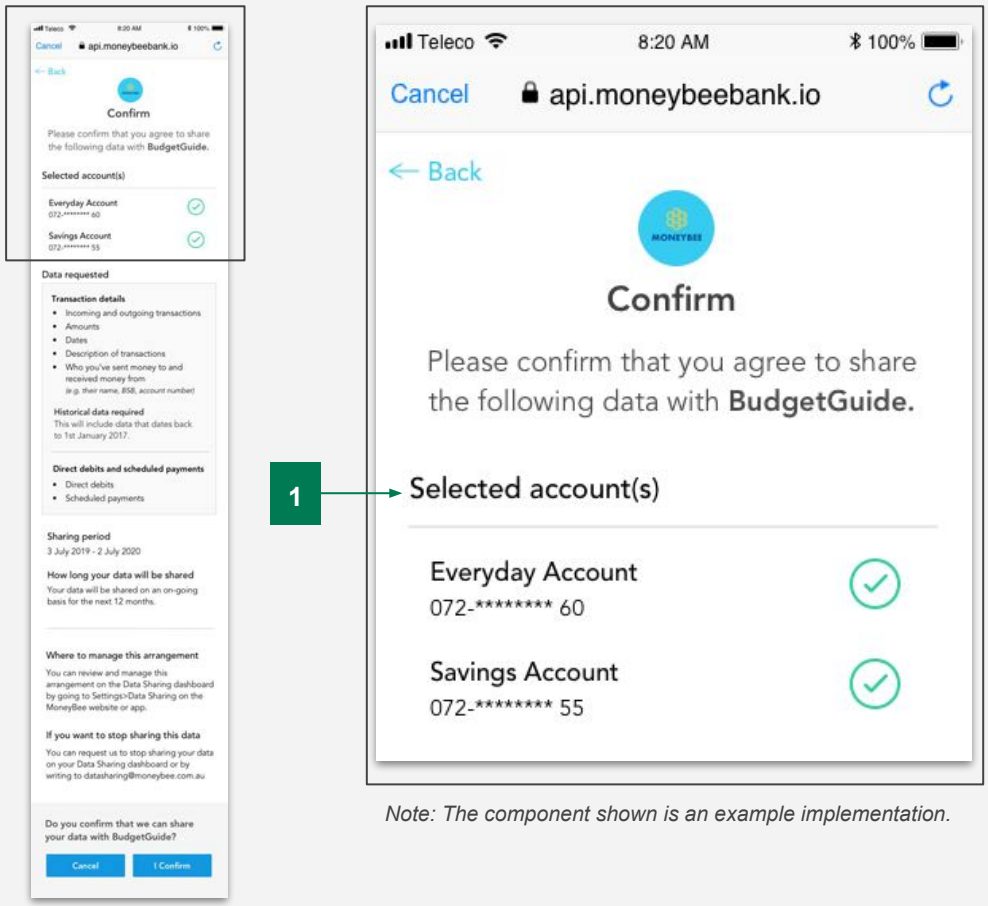
Confirmation **SHOULD** be presented as an explicit action for the consumer to take as a final step to authorise the data sharing.



Example wireframe

CONSUMER DATA STANDARDS





Note: The component shown is an example implementation.

Authorise | Confirmation

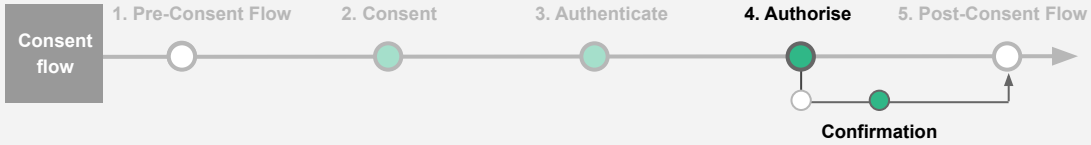
Selected accounts confirmation

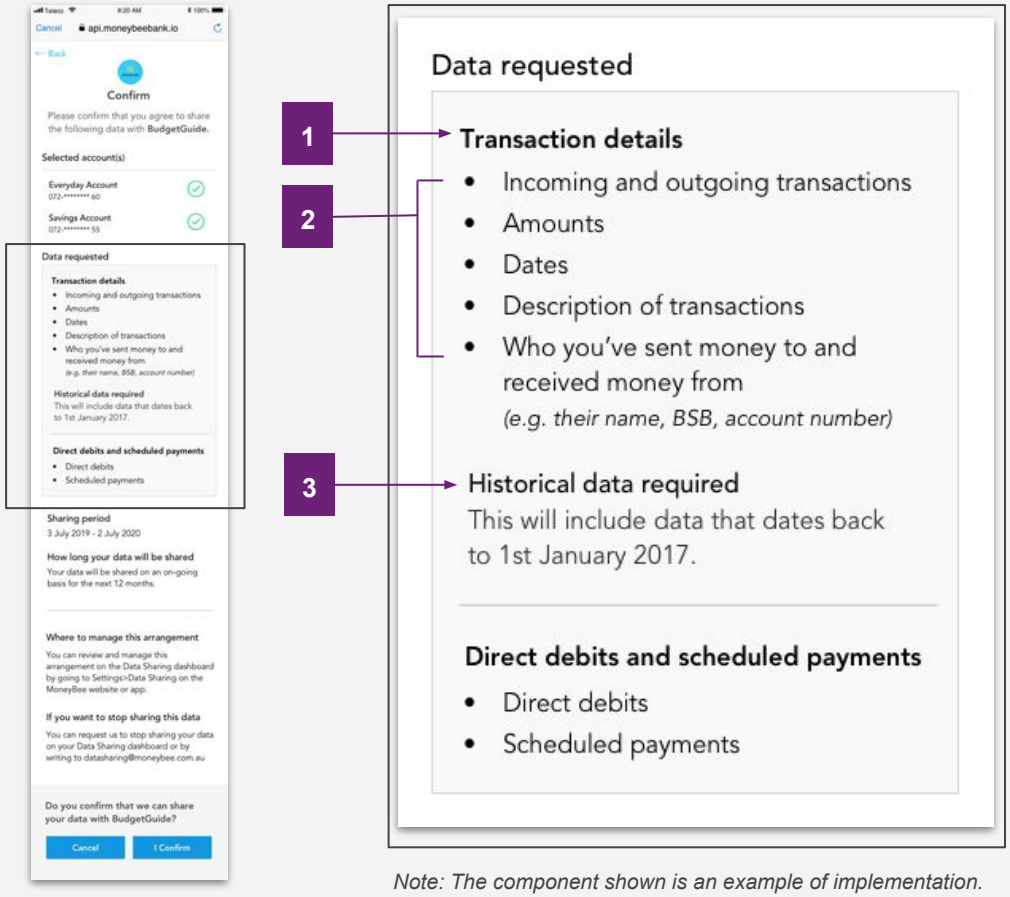
CX Standard

1 Data holders **MUST** show which accounts the data is being shared from prior to confirming authorisation if the data request includes account-specific data.

Data holders **MAY** omit this information if none of the data being requested is specific to an account (e.g. Saved Payees).

Community consultation





Note: The component shown is an example of implementation.

Authorise | Confirmation

Data clusters confirmation (1)

CDR Rule

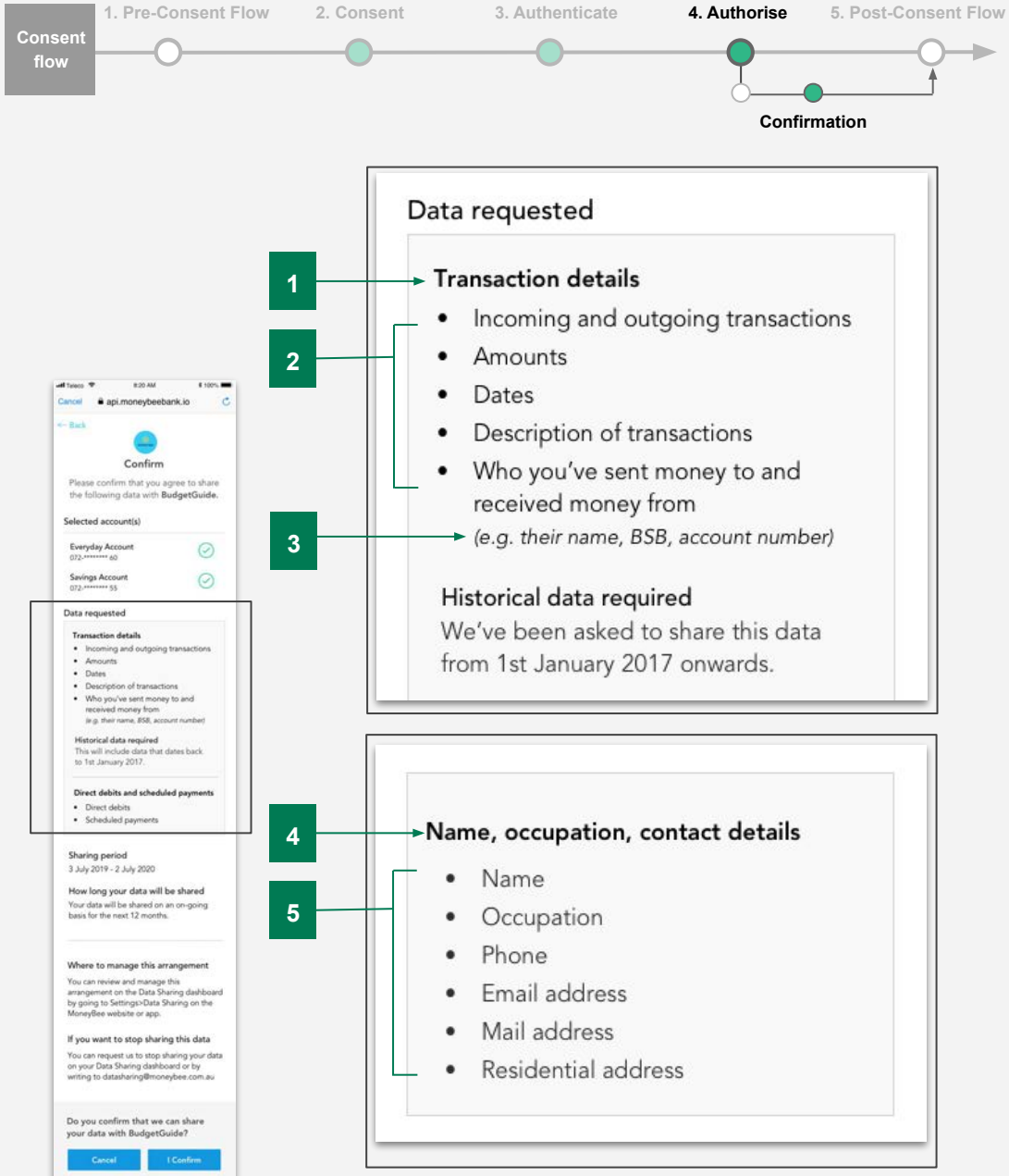
1 2 Data holders **MUST** state the types of CDR data they are asking the consumer to authorise sharing.

CDR Rule 4.23(c)

CDR Rule

3 When asking a consumer to authorise the disclosure of CDR data, data holders **MUST** state the period of time to which the CDR data that was the subject of the request relates.

CDR Rule 4.23(b)



The example above shows when Detailed scopes include Basic data

Note: The components shown are examples of implementation.

Authorise | Confirmation

Data clusters confirmation (2)

CX Standard

1 2 Data recipients and data holders **MUST** use data language standards to describe data clusters and permissions in consumer-facing interactions as outlined in the Data Language Standards table.

- 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 the table.
- Data recipients and data holders **SHOULD** expand on the proposed language where appropriate to communicate further details of what is being shared.
    - 3 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 the table

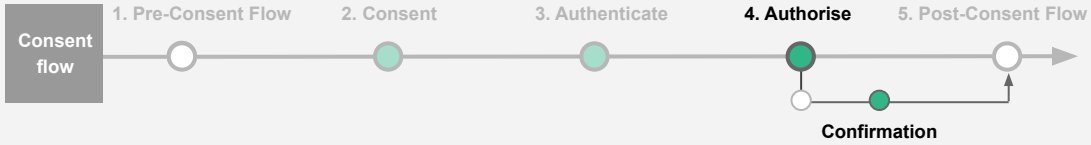
Data Language Standards

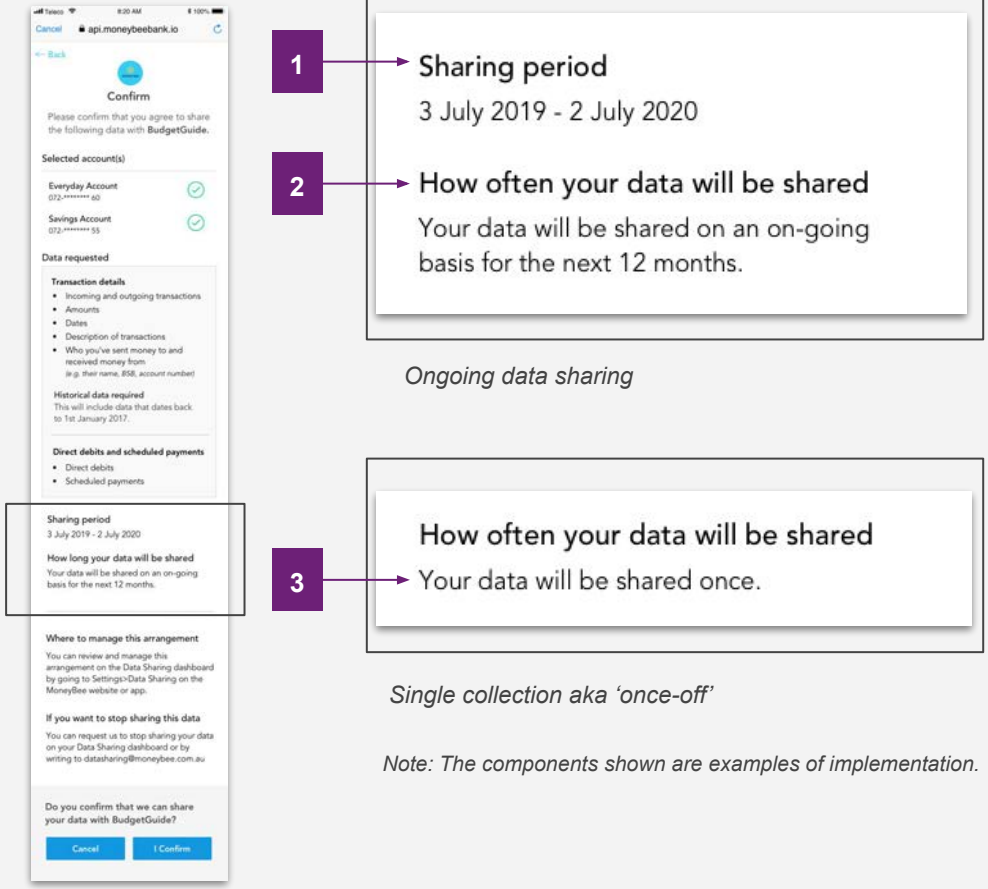
CX Standard

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.

4 5 Data holders and data recipients **MUST** use the alternative language denoted with an '‡' in the Data Language Standards table.

Data Language Standards





Ongoing data sharing

Single collection aka 'once-off'

Note: The components shown are examples of implementation.

Authorise | Confirmation

Duration

CDR Rule

1 Data holders **MUST** state which time period of CDR data will be disclosed if authorisation is being sought for disclosure over a period of time.

CDR Rule 4.23(e)

CDR Rule

2 3 Data holders **MUST** state whether data will be shared for single or ongoing collection.

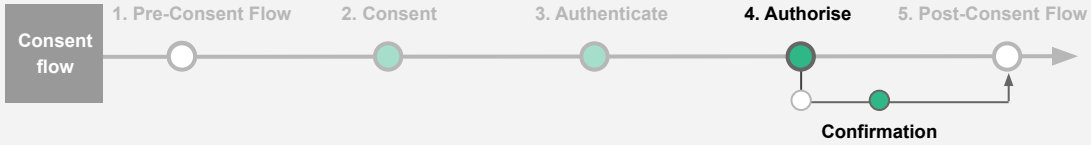
CDR Rule 4.23(d)

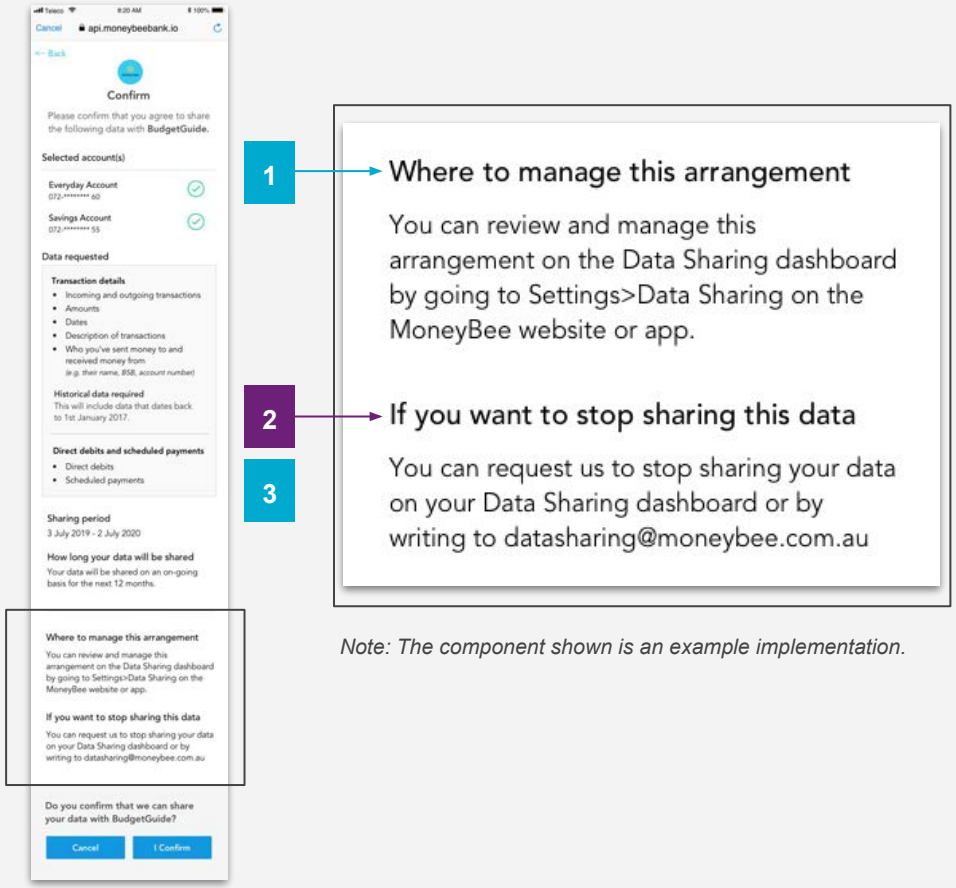
CDR Rule

Authorisation of CDR data expires when:

- The withdrawal of authorisation comes into effect
- 1 For an ongoing authorisation: At the end of the authorisation period (limit of 12 months)
- For a single occasion authorisation: after CDR data has been disclosed
- When the data recipient's accreditation is revoked or surrendered

4.26(1)(a-b), (d-g), 4.26(2)





Note: The component shown is an example implementation.

Authorise | Confirmation

Review and Withdraw

CX Guideline

1 Data holders **SHOULD** state that sharing arrangements can be reviewed via authorisation management dashboards.

CX Research 20

CX Guideline

3 Data holders **SHOULD** use the phrase 'Stop Sharing' to refer to how a consumer can withdraw authorisation.

CX Research 29

CDR Rule

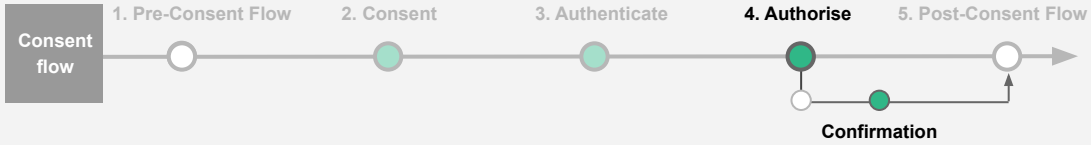
2 Data holders **MUST** state that authorisation can be withdrawn at any time and provide instructions for how to withdraw authorisation.

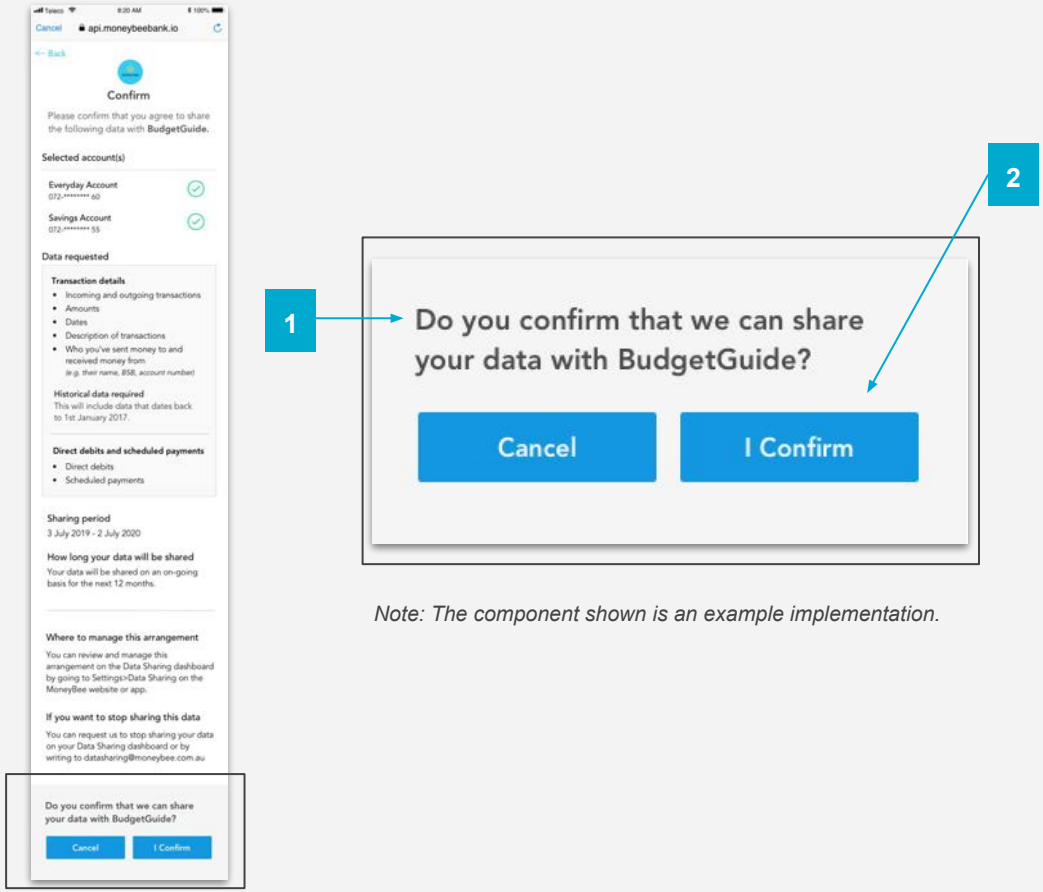
CDR Rules 4.23(f),(g) | CX Research 30, 32, 33

CDR Rule

2 Data holders **MUST** give the consumer ability to withdraw the authorisation to disclose data by communicating to the data holder in writing or via the consumer dashboard.

CDR Rules 4.25(1) | CX Research 30, 32, 33





Note: The component shown is an example implementation.

Authorise | Confirmation

Final affirmative action

CX Guideline

1 2 Data holders **SHOULD** use the term 'confirm' to communicate the final affirmative action. The term used for the final affirmative action **SHOULD** clearly communicate that it is the final step to mitigate user error.

Data holders **MAY** use alternative terms; alternatives **SHOULD** clearly communicate that this is the final affirmative action; alternatives **SHOULD** have regard to maintaining consistency and comprehension.

10 Usability Heuristics for User Interface Design: Error prevention (Nielsen)

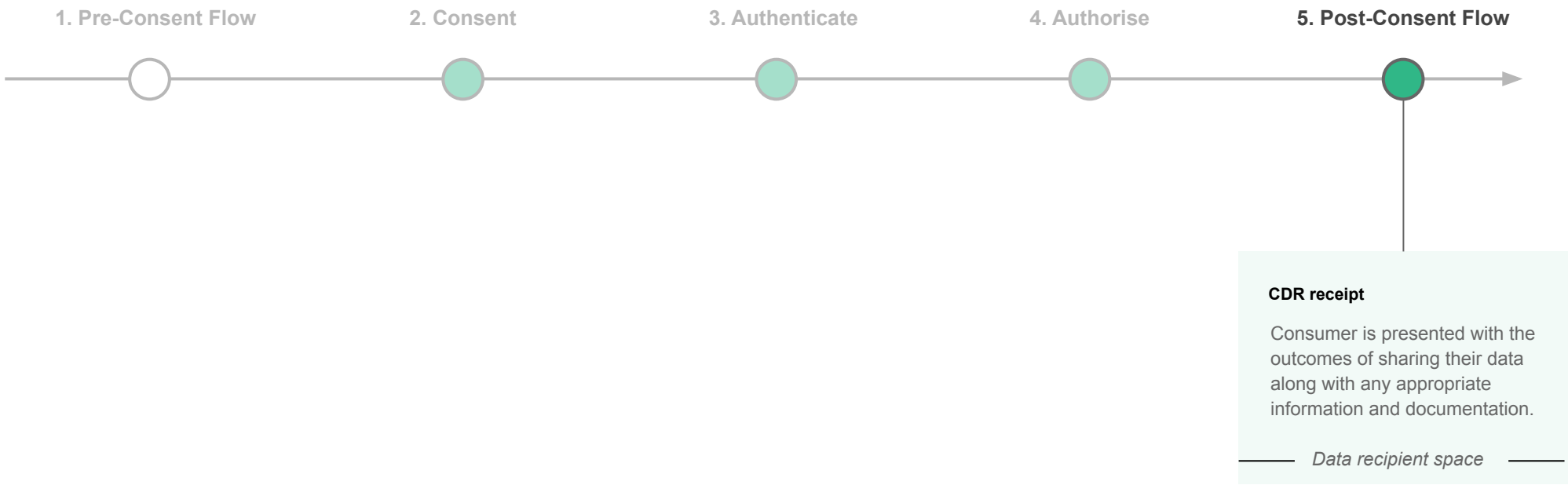
CX Guideline

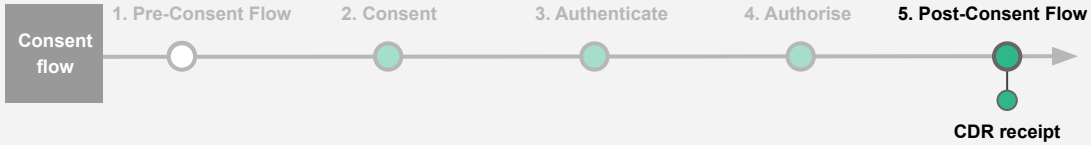
Data holders **SHOULD** redirect the consumer back to the data recipient following the final affirmative action.

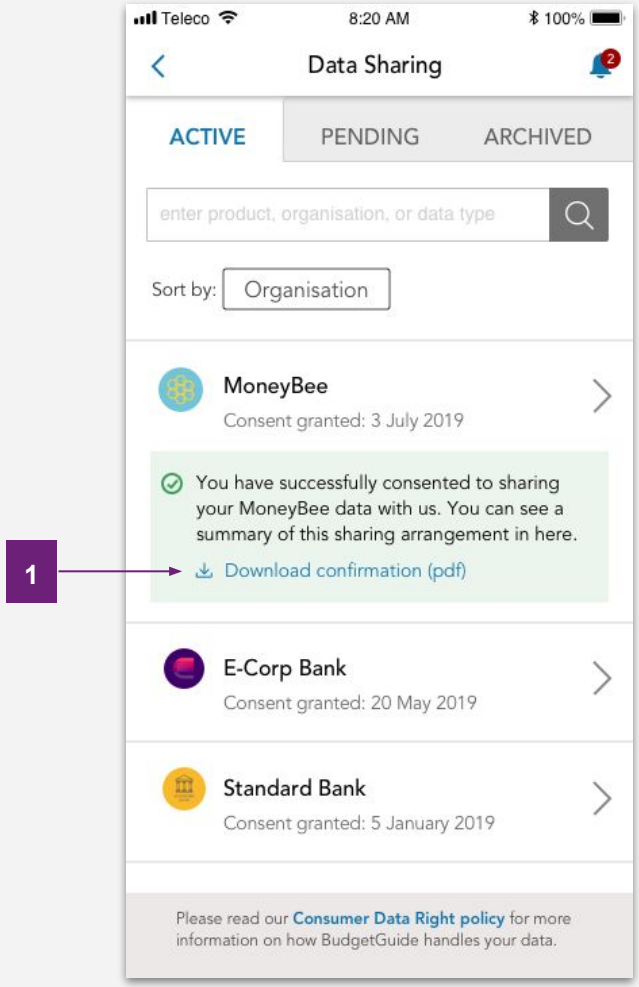
5. POST-CONSENT FLOW

Rather than a predetermined series of steps, the Post-Consent stage describes some of the actions a consumer may take after they have completed the consent flow and have a sharing arrangement in place.

The consumer will receive a record of their consent and be able to view and manage their sharing arrangements via a consumer dashboard.







Note: The screen shown is an example implementation.

In this example, the consumer is redirected back to the data recipient space.

Post-Consent | Consumer Dashboard

CDR receipt

CX Guideline

Following an authorisation the consumer **SHOULD** be directed back to the data recipient and presented with a 'confirmation' screen.

This 'confirmation' screen **MAY** be presented in the data recipient dashboard.

Data recipients and data holders **SHOULD** provide the consumer with a contextual 'walkthrough' or 'tutorial' to introduce them to the concept of the dashboard if they are not familiar with it.

CDR Rule

At the end of the consent flow, data recipients **MUST** provide a consumer with a CDR receipt that outlines:

- Details that relate to the consent
- The name of each data holder the consumer has consented to sharing their CDR data from
- Any other information the data recipient provided to the consumer when obtaining the consent

A CDR receipt **MUST** be given in writing otherwise than through the CDR consumer's consumer dashboard.

1 A copy of the CDR receipt **MAY** be included in the CDR consumer's consumer dashboard.

CDR Rule 4.18(1)(a), (2), (4), (5)

Manage and Withdraw
Data Recipient

MANAGE CONSENT

The consumer dashboard enables a consumer to manage their data sharing arrangements.

Dashboard landing page

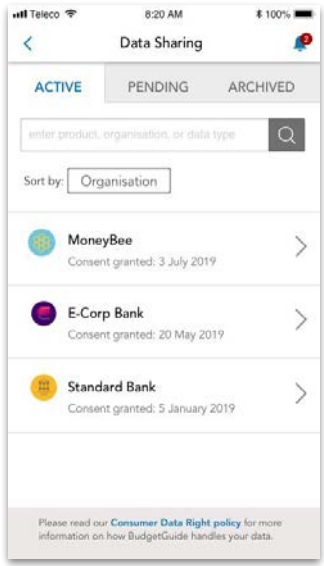
From this view, the consumer will be able to see a list of all their data sharing arrangements. The default display is at the discretion of the data recipient, but the dashboard **SHOULD** be organised in a way that helps consumers achieve a desired outcome.

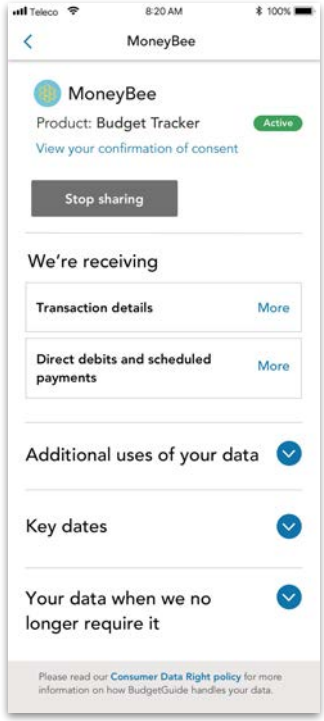
Data sharing arrangement

From this view, the consumer will be able to see a detailed breakdown of a specific data sharing arrangement.

Dashboard landing page

Data sharing arrangement

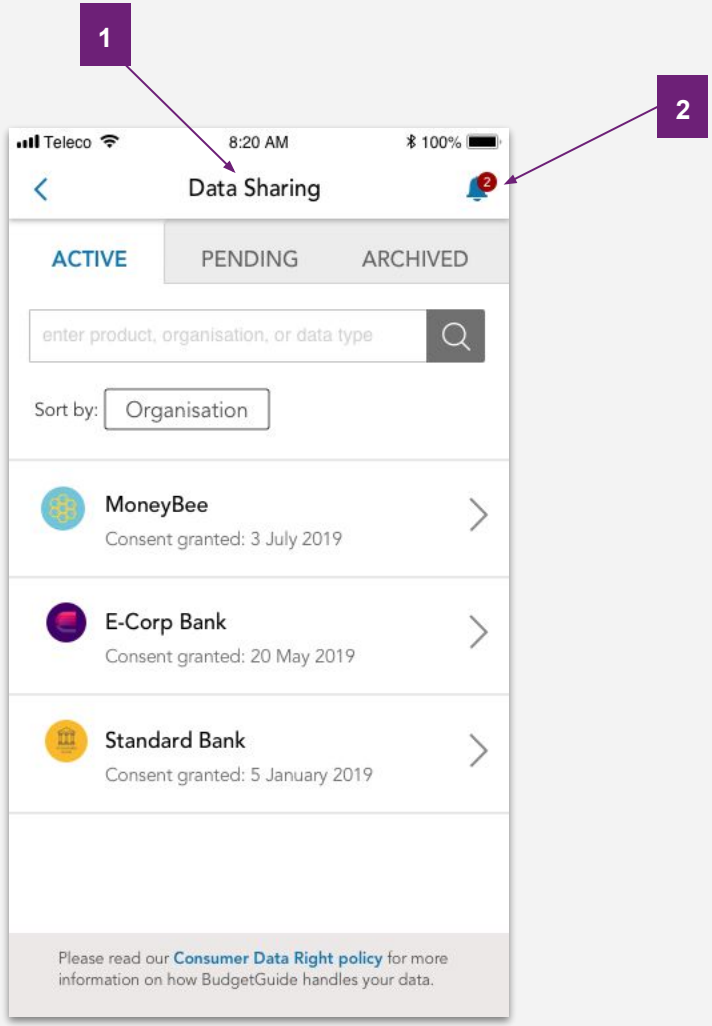




Example wireframes

Note: Refer to 'withdraw consent' section for detailed information of this screen

CONSUMER DATA STANDARDS



Note: The screen shown is an example implementation.

Data Recipient | Manage Consent

Dashboard landing page (1)

CDR Rule

1 Data recipients **MUST** provide a consumer dashboard for the consumer to manage their consents. This dashboard **MUST** contain the details of each consent.

CDR Rules 1.14(1)(a),(b), 1.14(2)

CDR Rule

Data recipients **MUST** update the consumer dashboard as soon as practicable after the information required to be contained on the dashboard changes.

Information on what CDR data was collected, when the CDR data was collected, and the data holder of the CDR data **MUST** be updated.

CDR Rule 4.19, 7.4

CDR Rule

Data recipients **MUST** show information in relation to CDR data that was collected pursuant to the consent.

CDR Rule 1.14(3)(h)

CDR Rule

Where a consent is still current, data recipients **MUST** notify CDR consumers of this fact if 90 days have elapsed since the latest of the following:

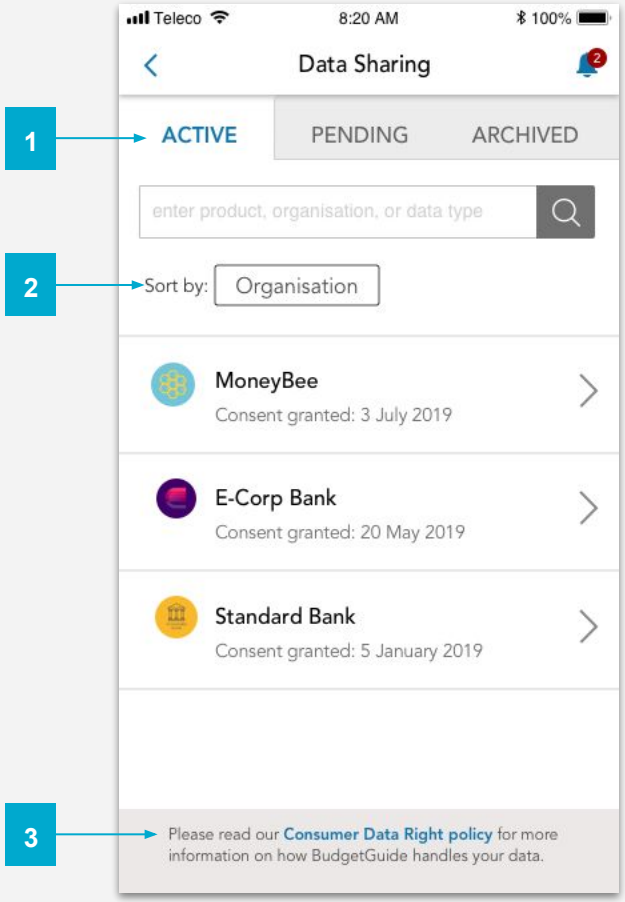
(i) the CDR consumer consented to the collection and use of the CDR data;
(ii) the CDR consumer last used their consumer dashboard;
(iii) the accredited person last sent the CDR consumer a notification in accordance with this rule.

CDR Rule 4.20

CDR Rule

2 The notification **must** be given in writing otherwise than through the CDR consumer's consumer dashboard. A copy **MAY** be included in the dashboard.

CDR Rule 4.20(3), (4)



Note: The screen shown is an example implementation.

Data Recipient | Manage Consent

Dashboard landing page (2)

CX Guideline

1 Data recipients **SHOULD** prioritise information that is important to consumers. This **MAY** include using tabs (e.g. active, pending, archived), or presenting key details up front, such as when consent was granted.

CX Workshop: Manage and withdraw

CX Guideline

Data recipients **SHOULD** allow consumers to create user-defined tags, names, and/or descriptions (e.g. home deposit) for each data sharing arrangement. This will facilitate comprehension and management in the absence of information about the purpose or use case.

CX Workshop: Manage and withdraw

CX Guideline

Data recipients **SHOULD** allow consumers to search, sort, and filter their data sharing arrangements in a way that is aligned to the outcomes consumers are seeking.

2 **Example 1:** A consumer may want to sort by data recipient, data cluster, or by a user-defined tag.

Example 2: A consumer may want to stop sharing in bulk

10 Usability Heuristics for User Interface Design: Flexibility and efficiency of use (Nielsen)

CX Guideline

3 Data recipients **SHOULD** provide a link to the CDR policy in the consumer dashboard.

WITHDRAW CONSENT: CONSUMER JOURNEY

See InVision prototype

The withdrawal journey for a consumer contains several steps, including: identifying a data sharing arrangement they wish to withdraw; reviewing the implications; confirming withdrawal; and receiving a final notification of success.

Data sharing arrangement

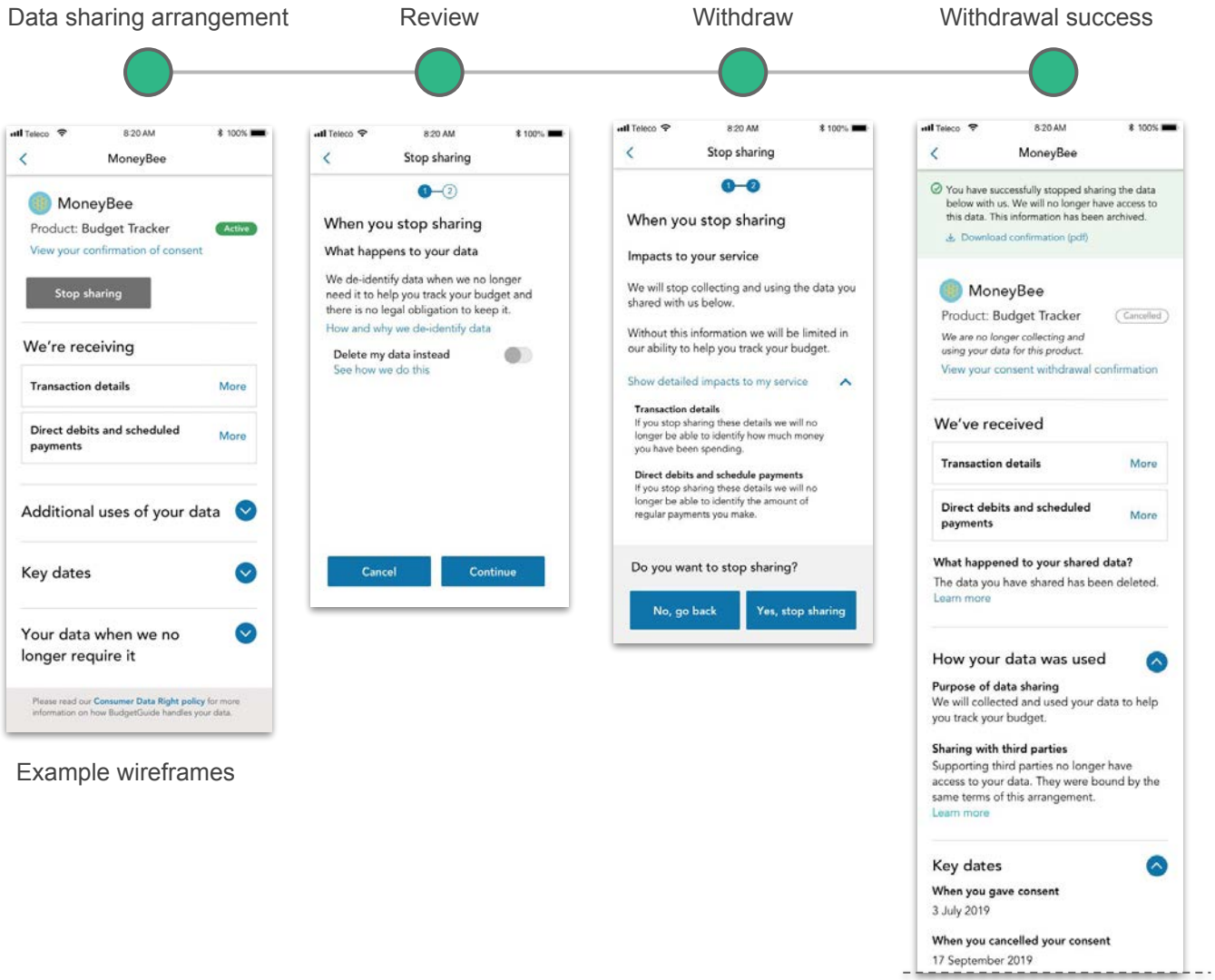
The consumer **MUST** be able to review their data sharing arrangement from the consumer dashboard.

Review and withdraw

The consumer will be advised of potential consequences of withdrawal before they stop sharing. This **SHOULD** nudge the consumer to review how withdrawal may impact their service and the handling of their data.

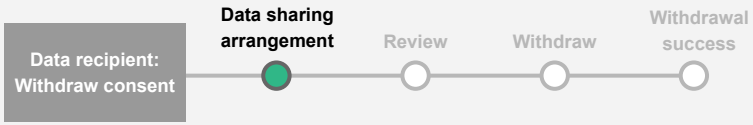
Withdrawal success

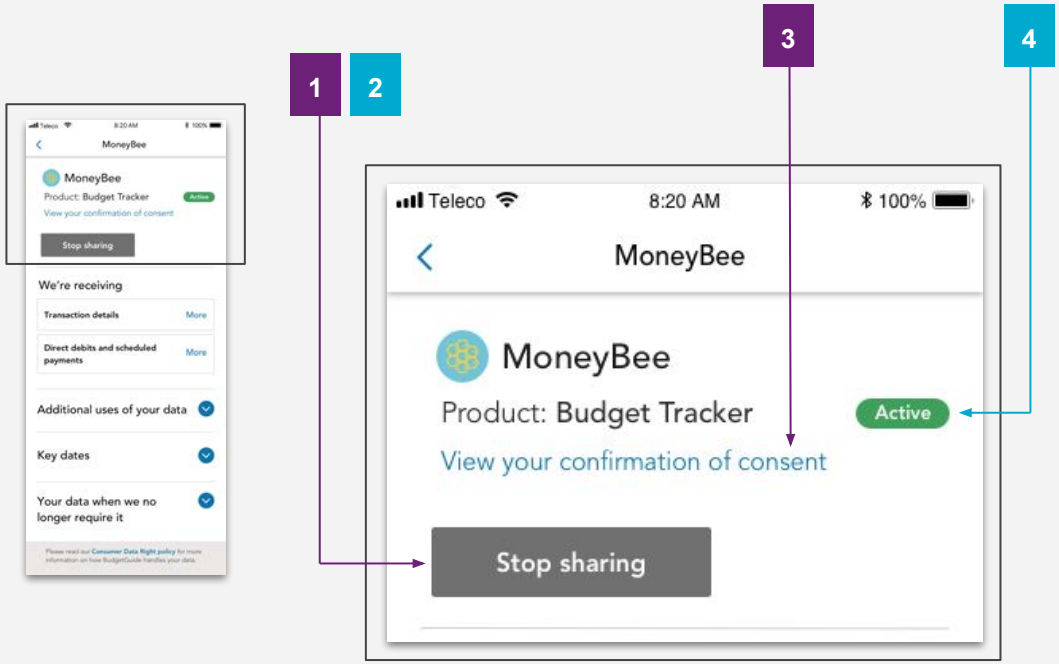
From this view, the consumer **MAY** receive confirmation that they have successfully withdrawn, and an updated view of their data sharing arrangement.



Example wireframes

CONSUMER DATA STANDARDS





Note: The component shown is an example implementation.

Data recipient | Manage Consent

Data sharing arrangement: General information

CDR Rule

1 Data recipient consumer dashboards **MUST** have functionality that allows consumers to withdraw their authorisation at anytime. This functionality **MUST** be simple and straightforward to use and prominently displayed.

CDR Rules 1.14(1)(c)(i)(A),(ii),(iii)

CDR Rule

3 A CDR receipt **MUST** be given in writing otherwise than through the CDR consumer's consumer dashboard. A copy of the CDR receipt **MAY** be included in the CDR consumer's consumer dashboard.

CDR Rules 4.18(4) and (5)

CX Guideline

2 Data recipients **SHOULD** use the phrase 'stop sharing' to refer to how a consumer can withdraw authorisation.

CX Research 29

CX Guideline

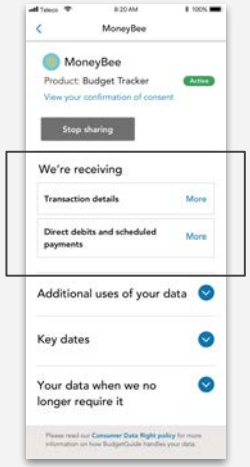
4 Data recipients **SHOULD** show the status of the data sharing arrangement e.g. active, pending, cancelled, expired.

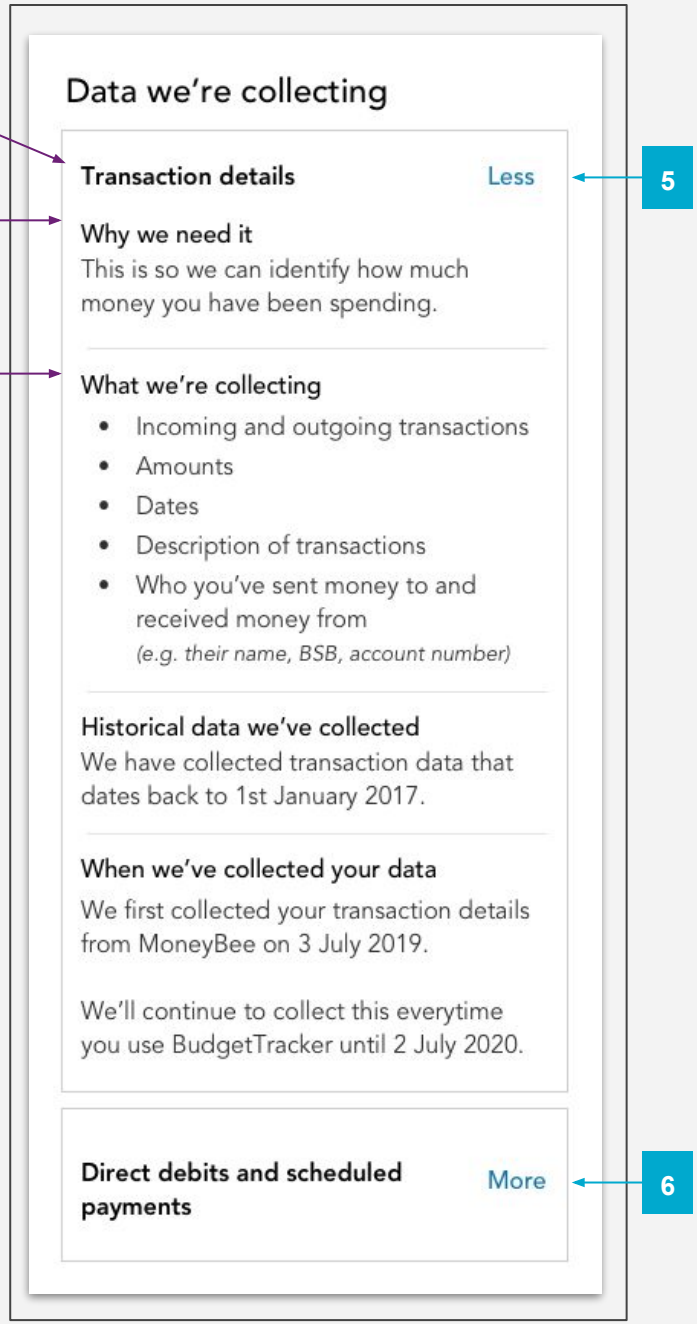
CX Workshop: Manage and withdraw

CX Guideline

Data recipients **SHOULD** allow consumers to create user-defined tags, and/or descriptions (e.g. home deposit) for each data sharing arrangement to facilitate management in the absence of information about the purpose or use case.

CX Workshop: Manage and withdraw





Note: The component shown is an example implementation.

Data recipient | Manage Consent

Data sharing arrangement: Data clusters and permissions (1)

CDR Rule

1 4 Data recipient consumer dashboards **MUST** show details of the CDR data to which the consent relates.

CDR Rules 1.14(3)(a)

CDR Rule

2 Data recipients **MUST** show the purpose of collecting this data, including the specific use(s).

CDR Rules 1.14(3)(b)

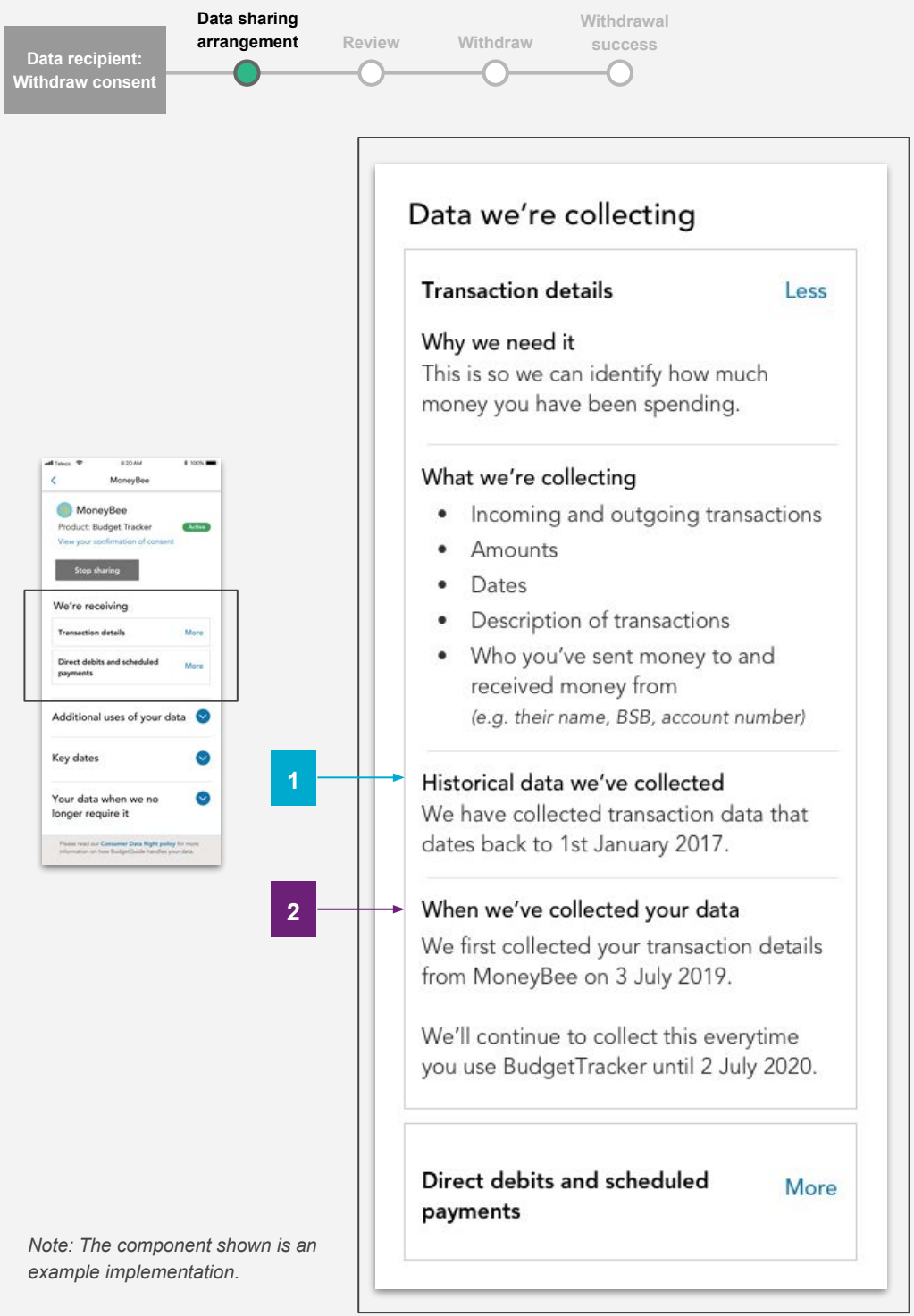
CX Guideline

3 Data recipients **SHOULD** structure the 'purpose' and 'use' statements in ways that:
1. Are specific as to purpose *(e.g. 'Why we need it' for each data cluster)*
2. Refer to the broader 'use case' or 'uses' *(e.g. 'to pre-populate your application')*
3. Relate to the product/service being provided *(e.g. 'so BudgetGuide can help you manage your budget')*

This information **SHOULD** be framed in a way that communicates the benefit of data sharing to the consumer.

CX Guideline

5 6 Data recipients **SHOULD** nudge consumers to be more privacy conscious and **SHOULD** use appropriate interventions to facilitate comprehension and consumer control. This can be done in a variety of ways, including through the use of design patterns like progressive disclosure, micro and/or descriptive copy, and with the use of microinteractions.



Note: The component shown is an example implementation.

Data recipient | Manage Consent

Data sharing arrangement: Data clusters and permissions (2)

CX Guideline

1 Data recipient consumer dashboards **SHOULD** show details of any historical CDR data that was collected and used.

CDR Rule

2 For section 56EH of the Act, an accredited person that collects CDR data in accordance with section 56EF of the Act as a result of a consent from a CDR consumer to collect CDR data must update the person's consumer dashboard as soon as practicable to indicate:

(a) what CDR data was collected; and

(b) when the CDR data was collected; and

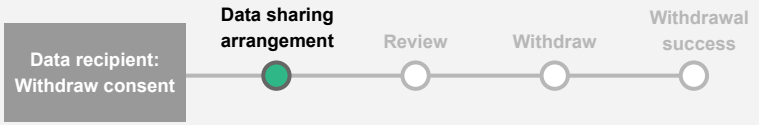
(c) the data holder of the CDR data.

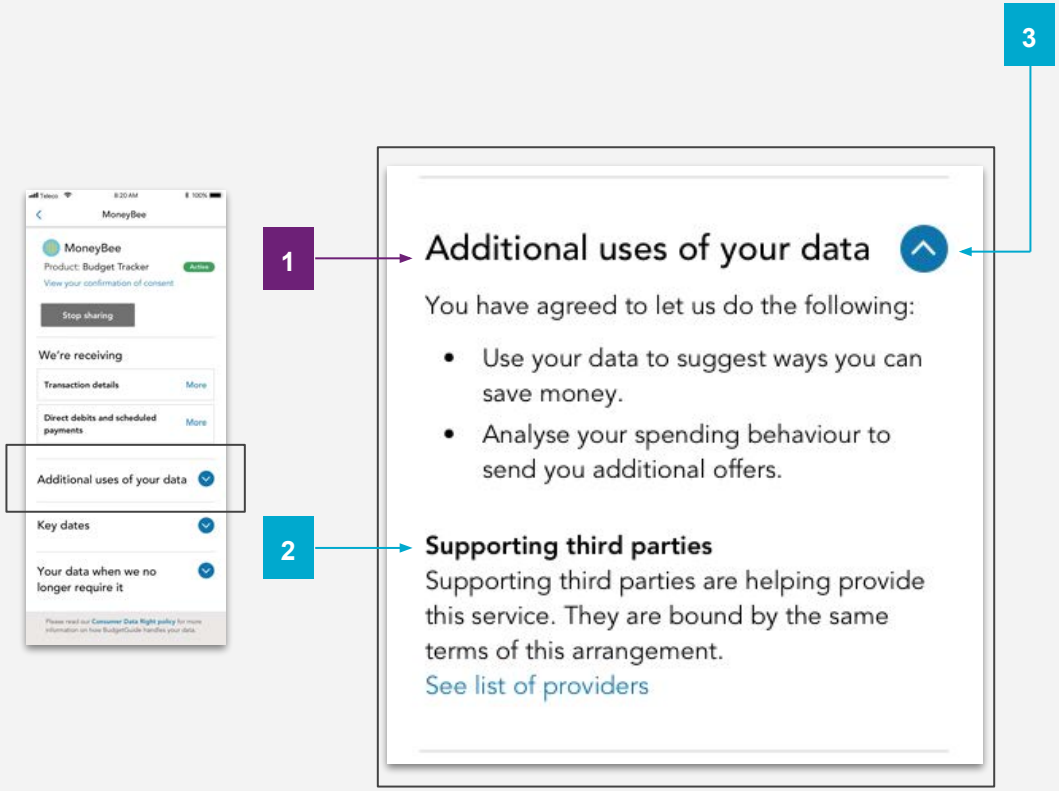
**For ongoing data sharing:* Data recipients should include the date range between which CDR data will be collected (dates of initial and final collection), as well as frequency of data collection.

For single or 'once-off' disclosure: Data recipients should include the date on which the CDR data was collected (date of initial collection).

Note: The example provide is context dependent. Please refer to Privacy Safeguard 5 for more guidance.

CDR Rules 7.4 | OAIC Draft CDR Privacy Safeguard Guidelines: Privacy Safeguard 5





Note: The component shown is an example implementation.

Data recipient | Manage Consent

Data sharing arrangement: Additional uses of data

CDR Rule

1 Data recipients **MUST** show the purpose of collecting this data, including the specific use(s).

CDR Rule 1.14(3)(b)

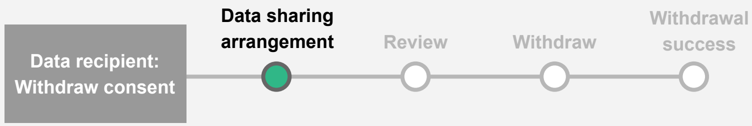
CX Guideline

2 If data is being shared with outsourced providers, data recipients **SHOULD** include this information on the dashboard. See the section on outsourced providers for more information.

CX Guideline

3 Data recipients **SHOULD** prioritise information that is important to consumers and structure the presentation in a way that reduces cognitive overload. This **MAY** include progressive disclosure design patterns (e.g. accordion menus), UX writing (e.g. microcopy), and visual aids (e.g. to display time-based qualities of consent).

CX Research 8, 19



Data recipient | Manage Consent

Data sharing arrangement: Duration

CDR Rule

1 **3** Data recipients **MUST** show the following information regarding sharing duration:

- When consent was given
- When consent is scheduled to expire
- If data sharing was a single collection or ongoing
- The time period for collection and frequency of data collection for ongoing collection

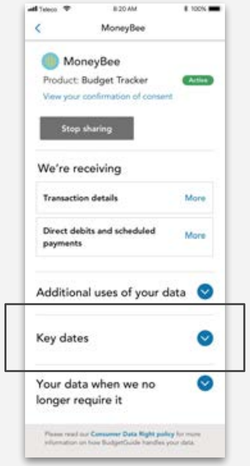
CDR Rule 1.14(3)(c)(d)(e)(f)(g), 4.14(1)(d)

CX Guideline

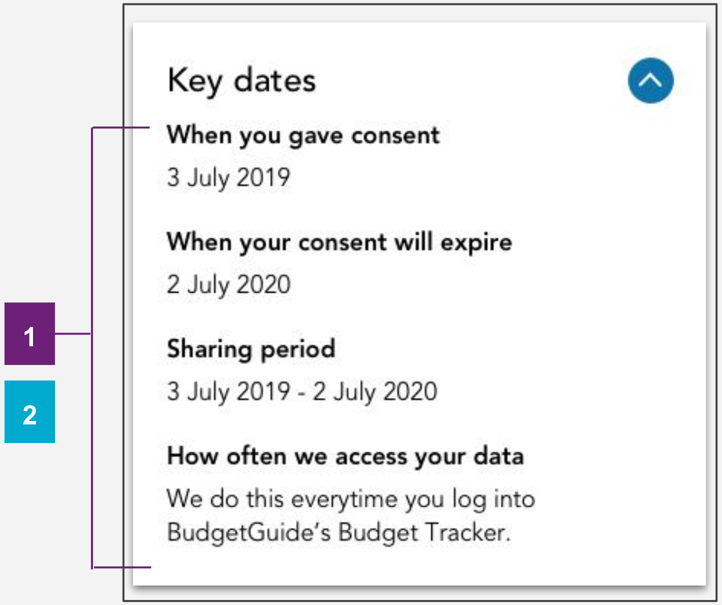
If a data recipient collects historical data that pre-dates when consent was granted, they **SHOULD** display this to the consumer in a way that is simple to understand.

CX Guideline

2 **4** Data recipients **SHOULD** use the phrases *'When you gave consent'*, *'When your consent will expire'* and *'Sharing period'* to refer to the time-based qualities of the data sharing arrangement.



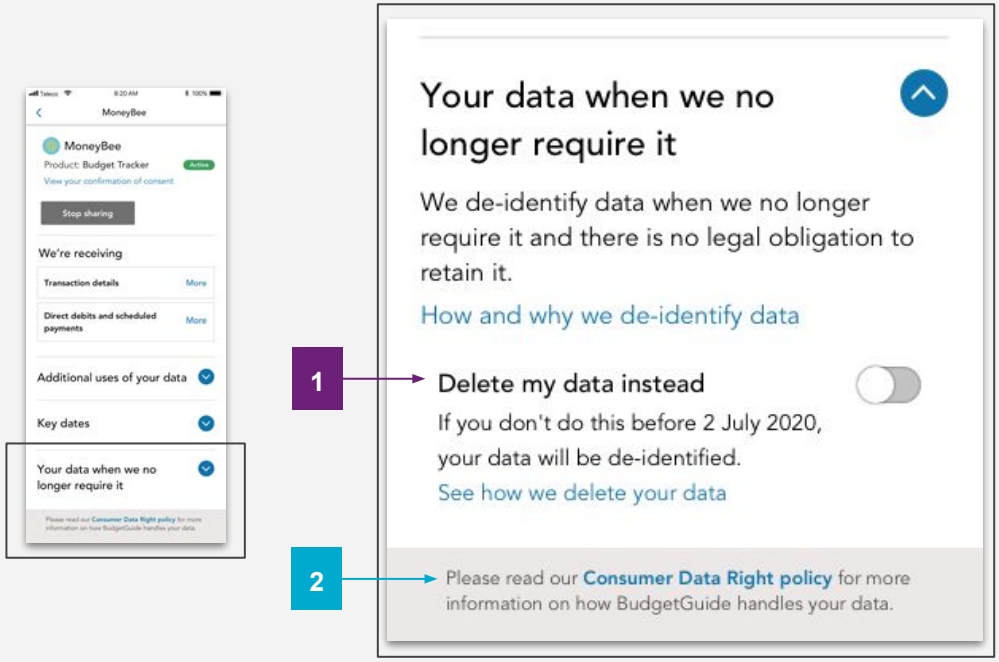
Note: The components shown are examples of implementation.



Ongoing data sharing

Single collection aka 'once-off'

CONSUMER DATA STANDARDS



Note: The component shown is an example implementation.

Data recipient | Manage Consent

Data sharing arrangement: Handling of redundant data

CDR Rule

1 Data recipient consumer dashboards **MUST** have functionality that allows consumer to choose redundant data to be deleted. It **MUST** also allow consumers to reverse this decision. This functionality must be simple and straightforward to use and prominently displayed.

The consumer **MAY** choose to communicate this this to the data recipient in writing or via the dashboard.

CDR Rules 1.14(b)(c)(ii)(iii), 4.16(2)

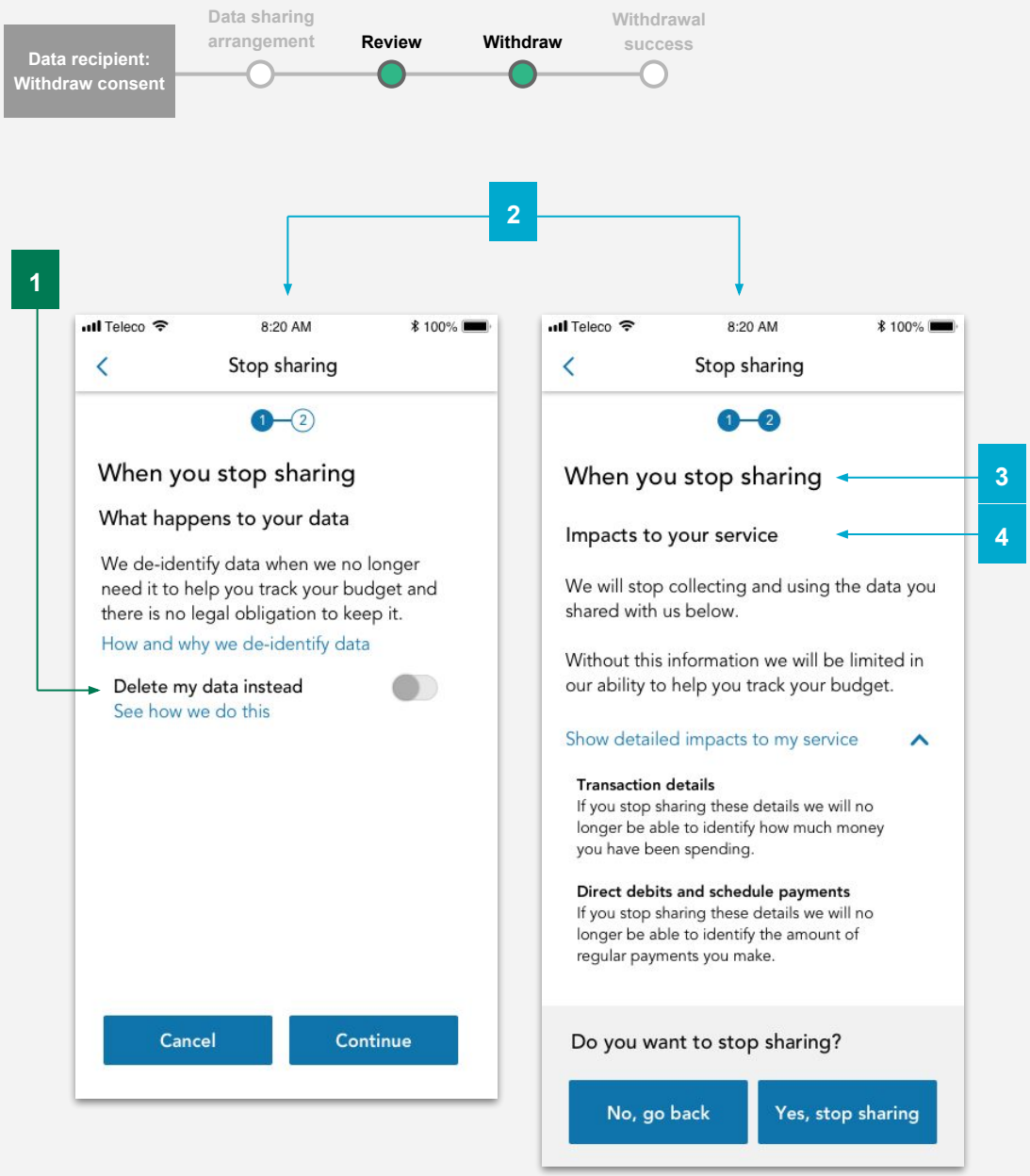
CDR Rule

1 The consumer **MAY** choose to have redundant data deleted at any time before consent expires unless the data recipient has informed the consumer that they have a general policy of deleting redundant CDR data.

CDR Rules 4.11(1)(e), 4.16(2)

CX Guideline

2 Data recipients **SHOULD** make a link to the CDR policy accessible on the dashboard.



Note: The screens shown are examples of implementation.

Data Recipient | Withdraw Consent

Review and Withdraw

CX Standard

If a Data Recipient does not have a policy to delete redundant data, and the consumer has not already requested that their redundant data be deleted:

1 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).

CX Guideline

3 Data recipients **SHOULD** use the phrase 'Stop sharing' to refer to how a consumer can withdraw consent.

CX Research 29

CX Guideline

2 Data recipients **SHOULD** introduce positive friction to the withdrawal flow to mitigate user error and unintended consequences.

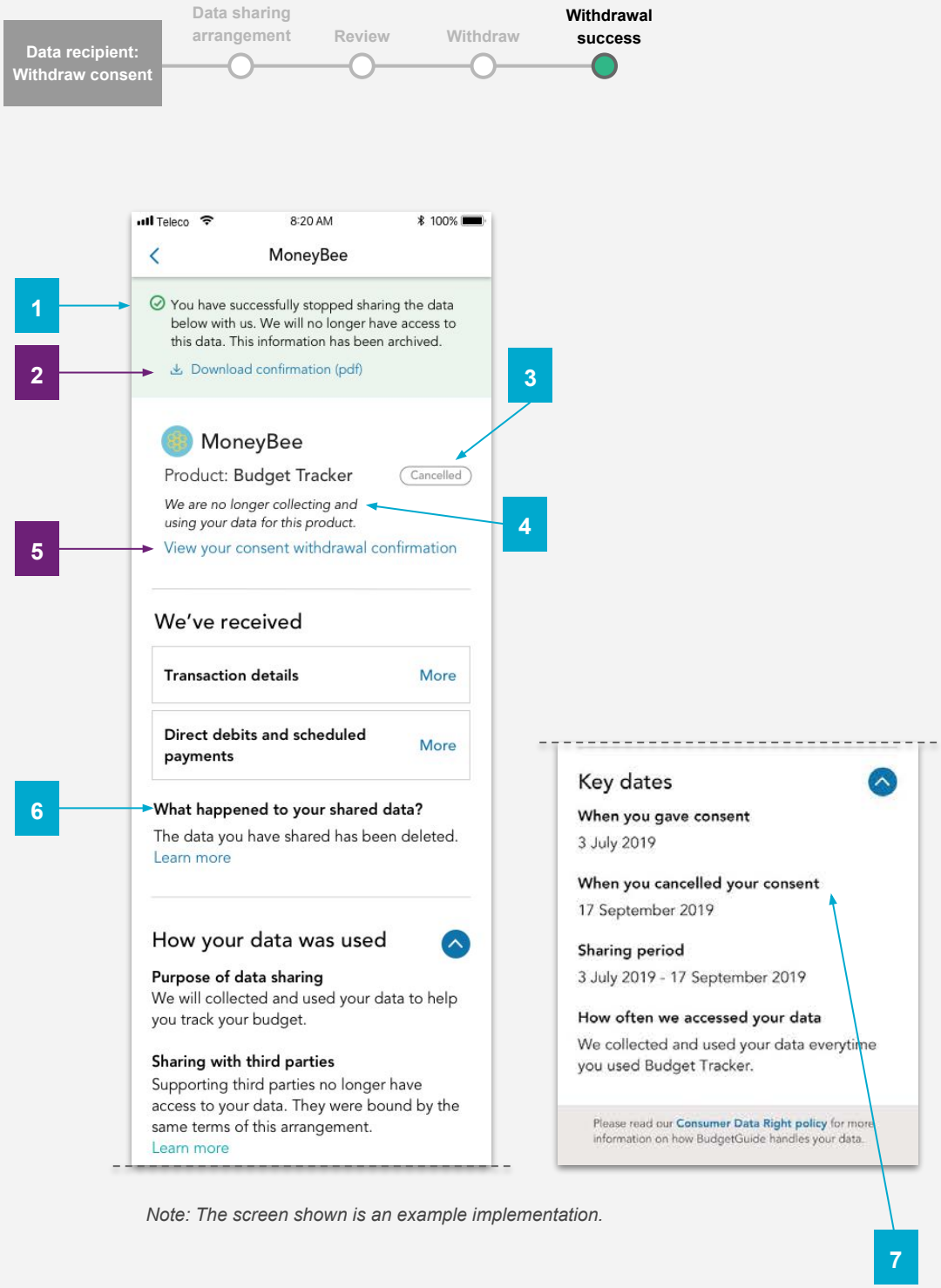
Data recipients **MAY** choose to do this via a 2-step consent withdrawal process.

CX Research 32 | 10 Usability Heuristics for User Interface Design: Error prevention (Nielsen)

CX Guideline

4 Data recipients **SHOULD** should include information on consequences of withdrawal during the consent withdrawal process. Please refer to CDR rule 7.2(4) and 4.11(3)(g)(iii).

CX Research 32



Note: The screen shown is an example implementation.

Data Recipient | Withdraw Consent

Withdrawal success

CDR Rule

Data recipients **MUST** update the consumer dashboard as soon as practicable after the information required to be contained on the dashboard changes.

CDR Rule 4.19

CX Guideline

These updates **SHOULD** include:

- 3 An updated status of the consumer's sharing arrangement.
- 4 A statement indicating to the consumer that the data recipient is no longer collecting and using their data
- 6 Information on the handling of redundant data
- 7 Updated information on sharing duration, including a consent withdrawal date

CX Guideline

1 Data recipients **SHOULD** provide a message to consumers that withdrawal was successful. This message **SHOULD** be clearly visible on the dashboard and shown as soon as withdrawal has taken place.

10 Usability Heuristics for User Interface Design: Visibility of system status (Nielsen)

CDR Rule

Data recipients **MUST** provide a CDR receipt to the consumer when consent has been withdrawn.

The receipt **MUST** provide the consumer with record of when consent has expired.

2 It **MUST** also be given in writing otherwise than through the consumer dashboard.

5 A copy **MAY** be included in the consumer dashboard.

CDR Rule 4.18(1)(b), (3), (4), (5) | CX Research 20

Manage and Withdraw
Data Holder

MANAGE AUTHORISATION

The consumer dashboard enables a consumer to manage their data sharing arrangements.

Dashboard landing page

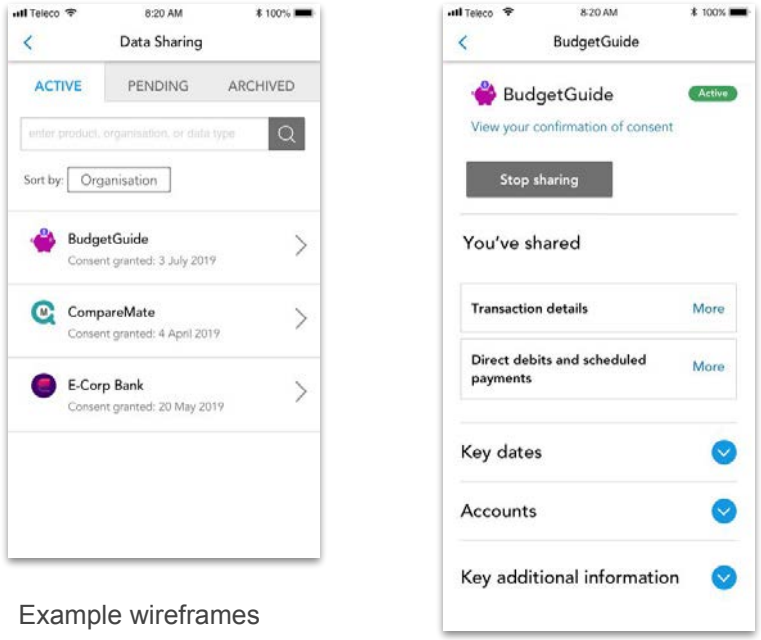
From this view, the consumer will be able to see a list of all their data sharing arrangements. The default display is at the discretion of the data holder, but the dashboard **SHOULD** be organised in a way that helps consumers achieve a desired outcome.

Data sharing arrangement

From this view, the consumer will be able to see a detailed breakdown of a specific data sharing arrangement.

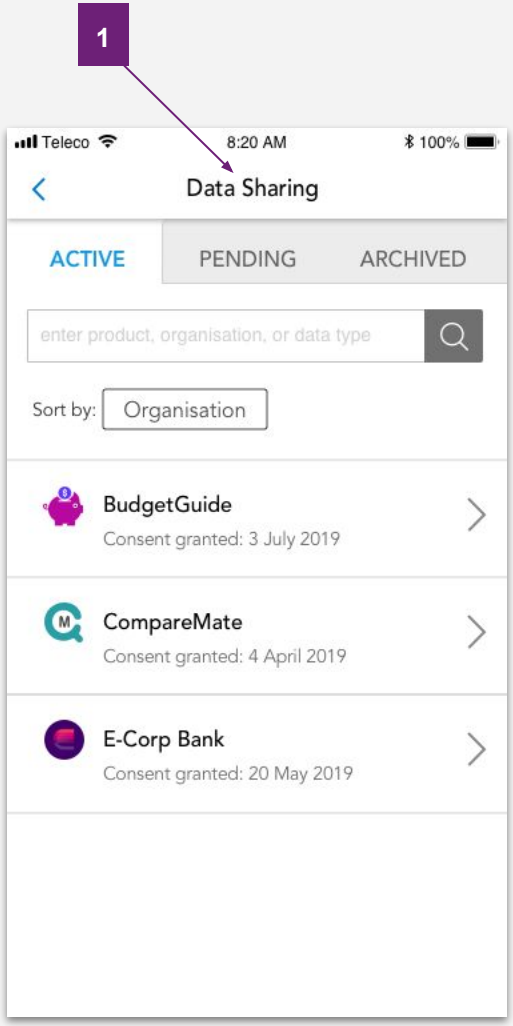
Dashboard landing page

Data sharing arrangement



Example wireframes

Note: Refer to 'withdraw consent' section for detailed information of this screen



Note: The screen shown is an example implementation.

Data Holder | Manage Authorisation

Dashboard landing page (1)

CDR Rule

1 Data holders **MUST** provide a consumer dashboard for the consumer to manage their authorisations. This dashboard must contain the details of each authorisation.

CDR Rules 1.15(1)(a),(b),(2)

CDR Rule

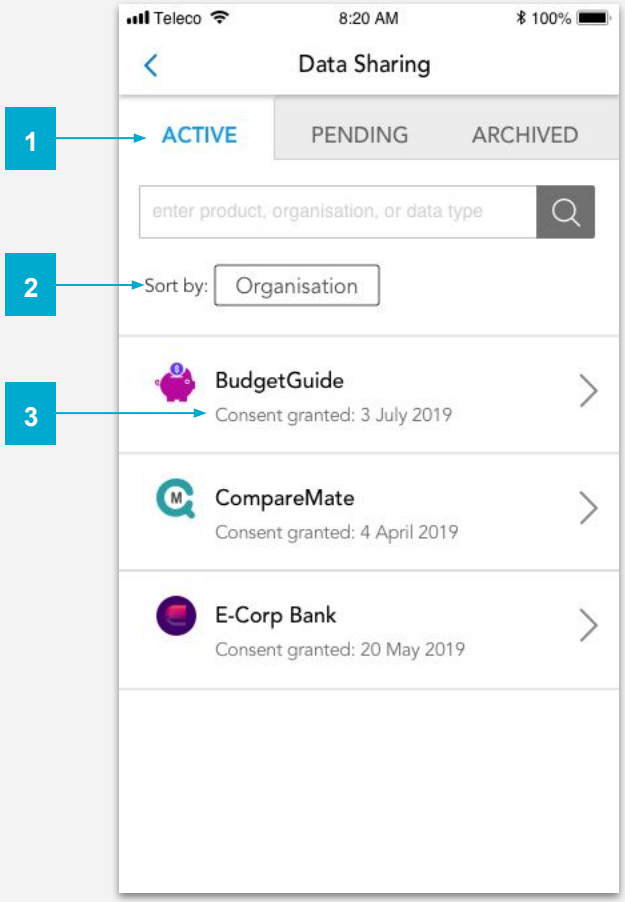
Data holders **MUST** update the consumer dashboard as soon as practicable after the information required to be contained on the dashboard changes.

CDR Rule 4.27

CDR Rule

Data holders **MUST** show information relating to CDR data that was disclosed pursuant to the authorisation.

CDR Rule 1.15(3)(f),(g)



Note: The screen shown is an example implementation.

Data Holder | Manage Authorisation

Dashboard landing page (2)

CX Guideline

1 Data holders **SHOULD** prioritise information that is important to consumers. This **MAY** include using tabs (e.g. active, pending, archived), or presenting key details up front, such as when consent was granted.

CX Workshop: Manage and withdraw

CX Guideline

Data holders **SHOULD** allow consumers to create user-defined tags, names, and/or descriptions (e.g. home deposit) for each data sharing arrangement. This will facilitate comprehension and management in the absence of information about the purpose or use case.

CX Workshop: Manage and withdraw

CX Guideline

2 Data holders **SHOULD** allow consumers to search, sort, and filter their data sharing arrangements in a way that is aligned to the outcomes consumers are seeking.
Example 1: A consumer may want to sort by data recipient, data cluster, or by a user-defined tag.
Example 2: If future capabilities enable it (e.g. fine-grained control), a consumer may want to stop sharing a particular permission in bulk with all data recipients.

10 Usability Heuristics for User Interface Design: Flexibility and efficiency of use (Nielsen)

CX Guideline

3 Data holders **SHOULD** use the term ‘consent’ instead of ‘authorisation’ to provide consistency and facilitate comprehension.

WITHDRAW AUTHORISATION: CONSUMER JOURNEY

See InVision prototype

The withdrawal journey for a consumer contains several steps, including: identifying a data sharing arrangement they wish to withdraw; reviewing the implications; confirming withdrawal; and receiving a final notification of success.

Data sharing arrangement

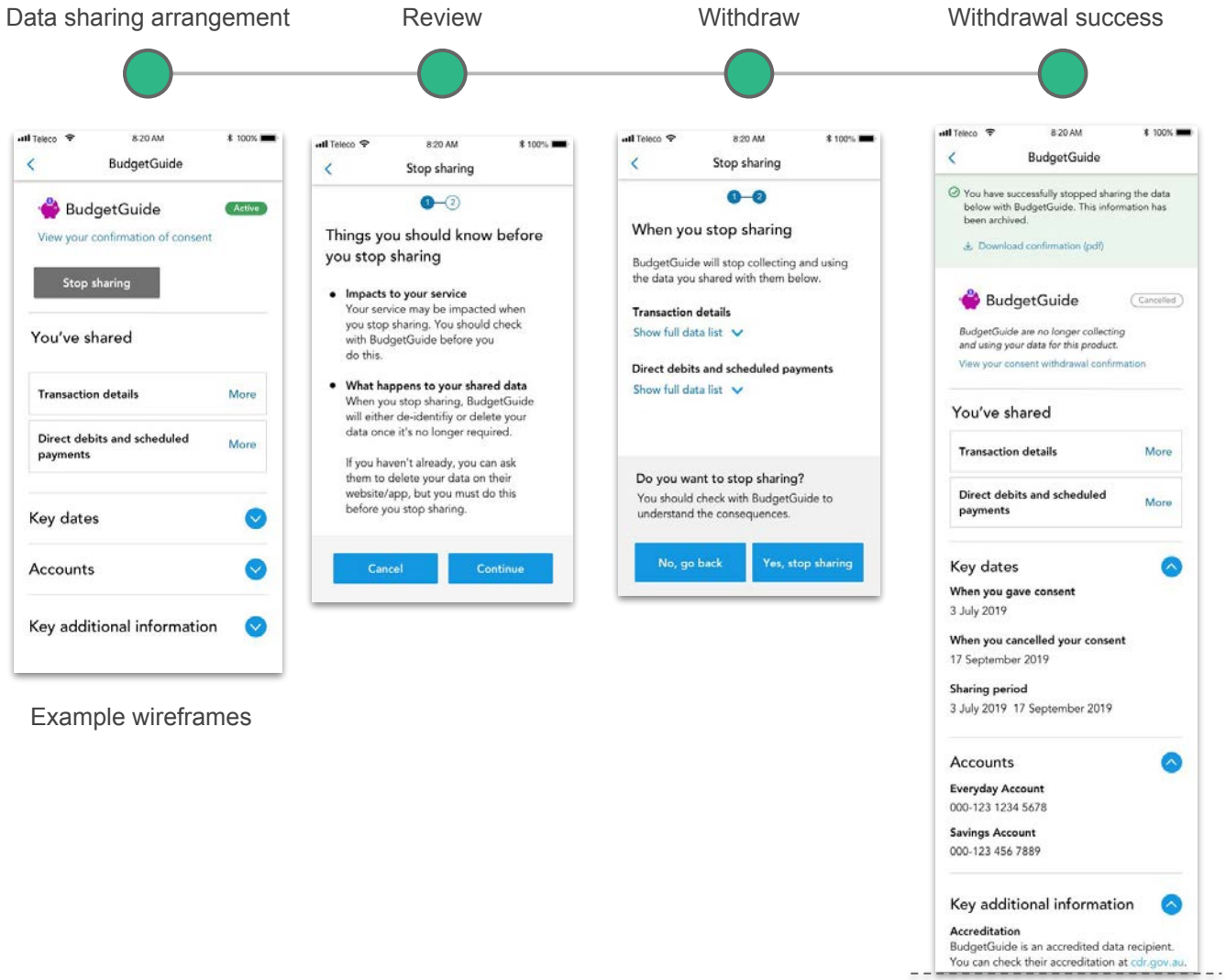
The consumer **MUST** be able to review their data sharing arrangement from the consumer dashboard.

Review and Withdraw

The consumer will be advised of potential consequences of withdrawal before they stop sharing. This **MUST** nudge the consumer to review how withdrawal may impact their service and the handling of their data.

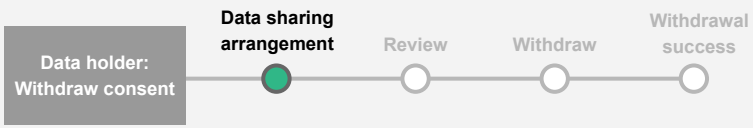
Withdrawal success

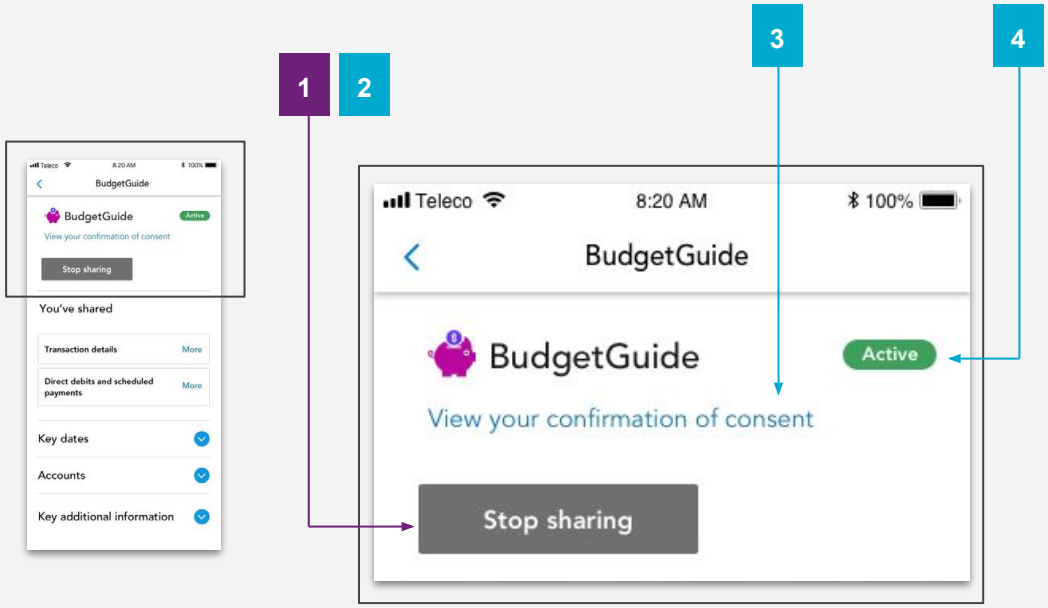
From this view, the consumer **MAY** receive confirmation that they have successfully withdrawn, and an updated view of their data sharing arrangement.



Example wireframes

CONSUMER DATA STANDARDS





Note: The component shown is an example implementation.

Data Holder | Manage Authorisation

Data sharing arrangement: General information

CDR Rule

1 Data holder dashboards **MUST** have functionality that allows consumers to withdraw their authorisation at anytime. This functionality **MUST** be simple and straightforward to use and prominently displayed.

CDR Rule 1.15(1)(c)(i)(ii)(iv)

CX Guideline

1 Data holders **SHOULD** use the phrase 'Stop sharing' to refer to how a consumer can withdraw authorisation.

CX Research 29

CX Guideline

2 Data holders **SHOULD** provide a CDR receipt detailing the consumer's authorisation. The receipt **SHOULD** provide the consumer with record of their sharing arrangement as well as details on complaint handling and resolution processes.

This information should also be made available on the dashboard.

CX Research 20

CX Guideline

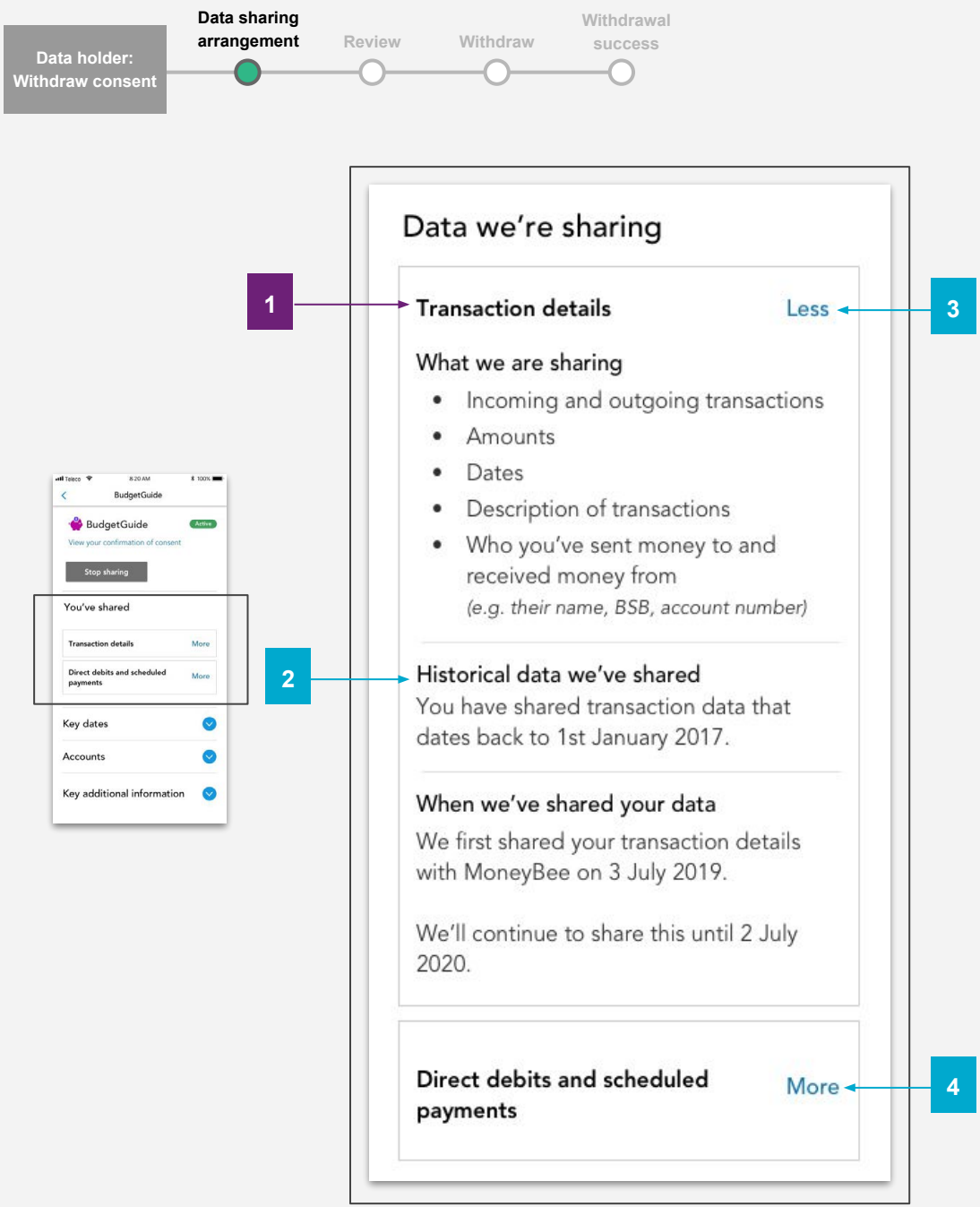
3 Data holders **SHOULD** show the status of the data sharing arrangement e.g. active, pending, cancelled, expired.

CX Workshop: Manage and withdraw

CX Guideline

Data holders **SHOULD** allow consumers to create user-defined tags, and/or descriptions (e.g. home deposit) for each data sharing arrangement to facilitate management in the absence of information about the purpose or use case.

CX Workshop: Manage and withdraw



Note: The component above is an expanded view that shows permissions. This is only an example implementation of the CDR Rules outlined.

Data Holder | Manage Authorisation

Data sharing arrangement: Data clusters and permissions (1)

CDR Rule

1 The consumer dashboard **MUST** show details of the CDR data that has been authorised to be disclosed.

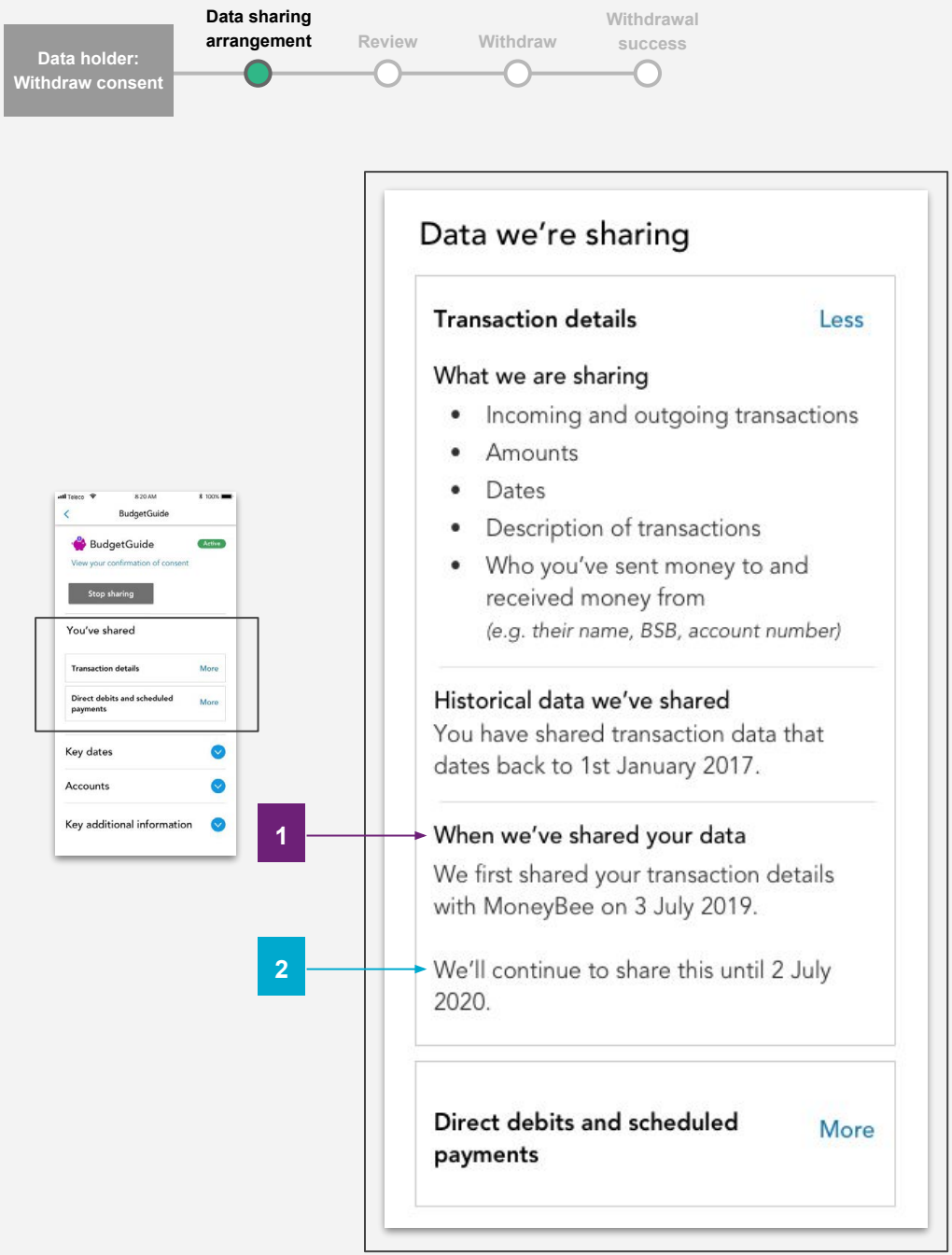
CDR Rule 1.15(3)(a)

CX Guideline

2 Data holder consumer dashboards **SHOULD** show details of any historical CDR data that was disclosed.

CX Guideline

3 4 Data recipients **SHOULD** nudge consumers to be more privacy conscious and **SHOULD** use appropriate interventions to facilitate comprehension and consumer control. This can be done in a variety of ways, including through the use of design patterns like progressive disclosure, micro and/or descriptive copy, and with the use of microinteractions.



Note: The component above is an expanded view that shows permissions. This is only an example implementation of the CDR Rules outlined.

Data Holder | Manage Authorisation

Data sharing arrangement: Data clusters and permissions (2)

CDR Rule

1 For subsection 56EM(1) of the Act, a data holder that discloses CDR data to an accredited person as a result of a consumer data request must, as soon as practicable, update each consumer dashboard that relates to the request to indicate:

(a) what CDR data was disclosed; and

(b) when the CDR data was disclosed*; and

(c) the accredited data recipient.

**For ongoing data sharing:* Data holders should include the date range between which CDR data will be disclosed (dates of initial and final disclosure).

For single or 'once-off' disclosure: Data holders should include the date on which the CDR data was disclosed (date of initial disclosure).

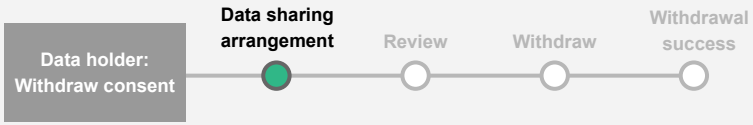
Note: The example provide is context dependent. Please refer to Privacy Safeguard 10 for more guidance.

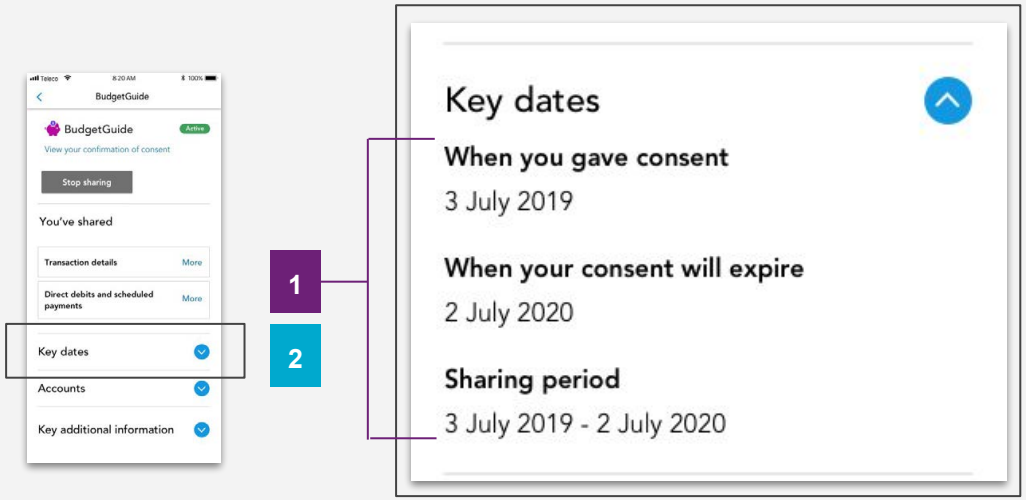
CDR Rule 7.9 | OAIC Draft CDR Privacy Safeguard Guidelines: Privacy Safeguard 10

CX Guideline

2 If a data holder is unsure of the date of final disclosure they **MAY** put the date consent expires. This date of final disclosure **SHOULD** be updated as soon as practicable after it becomes known.

OAIC Draft CDR Privacy Safeguard Guidelines: Privacy Safeguard 10





Note: The component shown is an example implementation.

Data Holder | Manage Authorisation

Data sharing arrangement: Duration

CDR Rule

1 Data holders **MUST** show the following information regarding sharing duration:

- When authorisation was given
- When authorisation is scheduled to expire
- The period in which authorisation was given

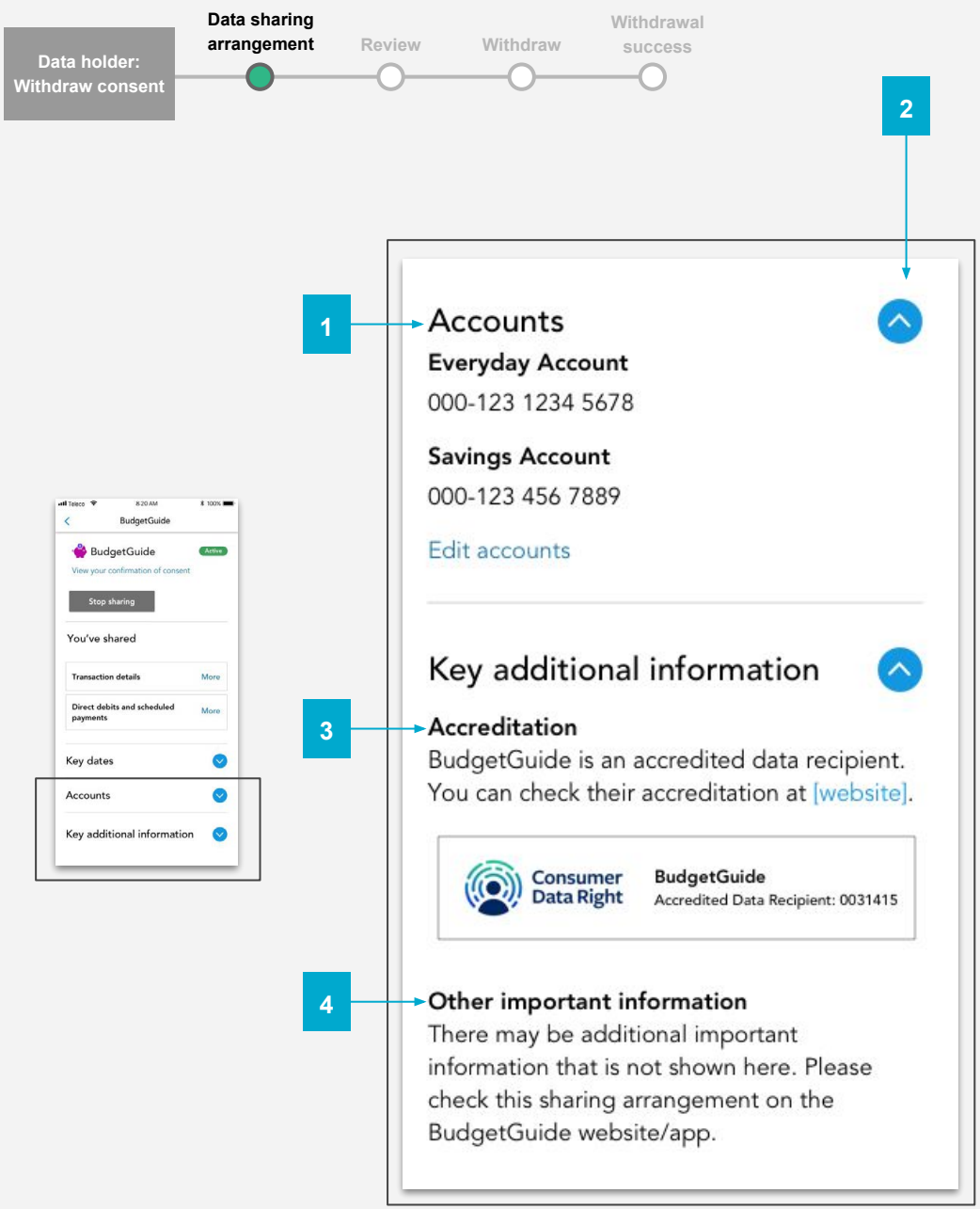
CDR Rule 1.15(3)(b),(c),(d),(e)

CX Guideline

2 Data holders **SHOULD** use the term 'consent' instead of 'authorisation' to provide consistency and facilitate comprehension.

CX Guideline

2 Data holders **SHOULD** use the phrases *'When you gave consent'*, *'When your consent will expire'* and *'Sharing period'* to refer to the time-based qualities of the data sharing arrangement.



Note: The component shown is an example implementation.

Data Holder | Manage Authorisation

Data sharing arrangement: Account and additional information

CX Guideline

1 Data holders **SHOULD** show the account(s) shared as part of the data sharing arrangement. It is at the discretion of data holders to provide functionality to add/remove additional accounts from the data sharing arrangement.

CX Workshop: Manage and withdraw

CX Guideline

2 Data holders **SHOULD** prioritise information that is important to consumers and structure the presentation in a way that reduces cognitive overload.

This **MAY** include progressive disclosure design patterns (e.g. accordion menus), UX writing (e.g. microcopy), and visual aids (e.g. to display time-based qualities of consent).

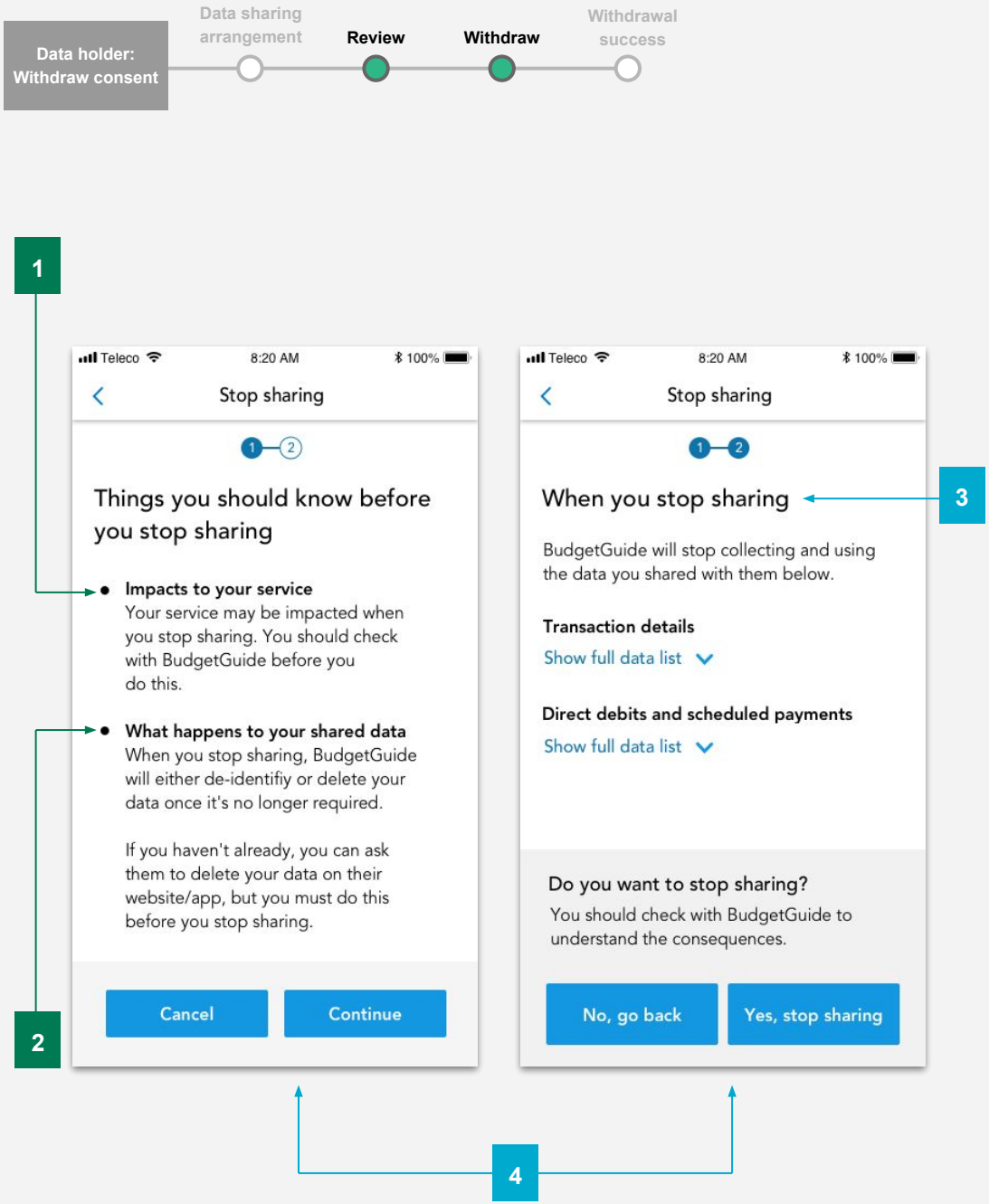
CX Research 8

CX Guideline

3 Data holders **SHOULD** provide instructions for how consumers can verify a data recipient's accreditation via an ACCC-provided URL once the ACCC makes this functionality available.

CX Guideline

4 Data holders **SHOULD** communicate that certain information may not be available on data holder dashboards and **SHOULD** advise consumers to check with the data recipient for additional information.



Note: The screens shown are examples of implementation.

Data Holder | Withdraw Authorisation

Review and Withdraw

CX Standard

In accordance with CDR Rule 1.15(1)(c)(v), data holders **MUST** display a message relating to the consequences of the withdrawal in accordance with the data standards.

1 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.'

2 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.'

CX Research 32

CX Guideline

3 Data holders **SHOULD** use the phrase 'Stop sharing' to refer to how a consumer can withdraw authorisation.

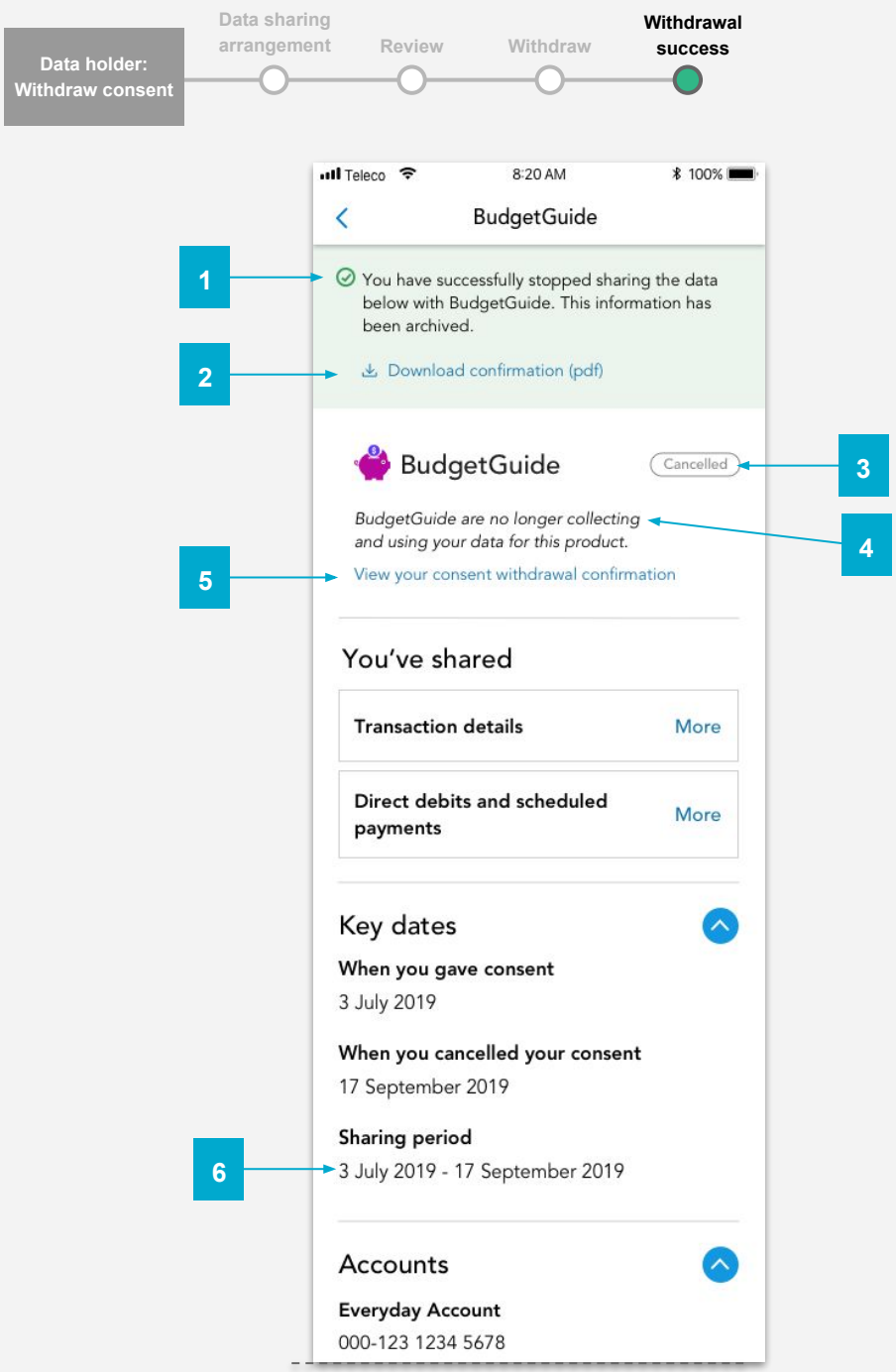
CX Research 29

CX Guideline

4 Data holders **SHOULD** introduce positive friction to the withdrawal flow to mitigate user error and unintended consequences.

Data holders **MAY** choose to do this via a 2-step consent withdrawal process.

CX Research 32 | 10 Usability Heuristics for User Interface Design: Error prevention (Nielsen)



Note: The screen shown is an example implementation.

Data Holder | Withdraw Authorisation

Withdrawal success

CDR Rule

Data holders **MUST** update the consumer dashboard as soon as practicable after the information required to be contained on the dashboard changes.

CDR Rule 4.27

CX Guideline

These updates **SHOULD** include:

- 3 An updated status of the consumer's sharing arrangement.
- 4 A statement indicating to the consumer that the data recipient is no longer collecting and using their data
- 6 Updated information on sharing duration, including a consent withdrawal date

CX Guideline

1 Data holders **SHOULD** provide a message to consumers that withdrawal was successful. This message **SHOULD** be clearly visible on the dashboard and shown as soon as withdrawal has taken place.

10 Usability Heuristics for User Interface Design: Visibility of system status (Nielsen)

CX Guideline

2 5 Data holders **SHOULD** provide a CDR receipt to the consumer when consent has expired or when the consumer has withdrawn consent.

The receipt **SHOULD** provide the consumer with a record of their sharing arrangement, details of expiry or consent withdrawal as well as details on complaint handling and resolution processes.

This information **SHOULD** also be made available on the dashboard.

CX Research 20

Appendix

CX Research references

Ref #	Research findings	Source
1	**Communicate motives for data requests** Participants needed clarity around the value proposition of sharing their data as well as data recipient motivations for wanting access to that data. Participants were suspicious of data recipient motives, and wanted assurance that their purpose for gaining access to that data was not just to advertise their services or sell their data to advertisers.	Phase 2, Stream 1 Research report, page 63
2	**Clearly explain the purposes of data requests** Data recipients should clearly explain why data is being requested. They should be relevant to the features/product that consumers are using. Most participants commented that having this detailed information throughout the consent flow was helpful. Details of how their data was going to be used, and why this was needed in the data cluster components was particularly helpful and reassuring.	Phase 2, Stream 3 Research report, page 38 Phase 2, Stream 1 Research report, page 36
3	**Data minimisation principle; consumer control** Follow the data minimisation principle to only ask for what is required. Research has shown that participants did not want to share personal data (e.g contact details or mailing address) that was perceived to have no relevance to receiving the product/service they are sharing their data for.	Phase 2, Stream 3 Research report, page 38
4	**Consent duration** Having the ability to choose the duration of consent is ideal. However participants were comfortable with the 12 months period, knowing that they can withdraw consent at anytime.	Phase 2, Stream 3 Research report, page 39
5	**Data sharing duration** Participants preferred to share enough data to enable them to find useful insights, but not their full transaction history. This generally aligned with the duration of billing cycles, or duration of seasonal changes in behaviour.	Phase 2, Stream 1 Research report, page 64
6	**Provide a clear purpose of accessing the data history** Participants needed to understand the purpose of sharing their data history. Adding this purpose can help clarify the difference between the request for historical data vs consent durations, as this was a point of confusion to participants in Phase 2 research.	Phase 2, Stream 3 Research report, page 40

CX Research references

Ref #	Research findings	Source
7	**Consent withdrawal** Add withdrawal information and clearly explain the consequences of what happens to their data when they stop sharing. Many participants in research were not able to confidently articulate the consequences of withdrawal when this information was not present.	Phase 2, Stream 3 Research report, page 41
8	**Accordion menus** Accordion menus reduce cognitive overload while also allowing more information to be revealed if desired.	Phase 1, Research report, page 55
9	**Account selection** Account(s) selection is appreciated. Many participants showed strong appreciation for this step as there were certain accounts that they did not want to share data from.	Phase 1, Research report, page 69
10	**One Time Password language** Clearly explain the use of verification code as a One Time Password. Some participants during research expected to enter their banking password following the Customer ID. Emphasising the difference can aid in a smoother authentication process.	Phase 2, Stream 3 Research report, page 53
11	**One Time Password security measure** Apply a time limit to the code for additional security measure.	Phase 2, Stream 3 Research report, page 53
12	**One Time Password delivery** The code should also be delivered by other methods such as email as alternative to SMS via mobile number.	Phase 2, Stream 3 Research report, page 53
13	**A trust mark should be strengthened by linking it to accreditation information** A 'trust mark' accreditation should be easily verifiable by linking it to the data recipient's specific accreditation data on a government website.	Phase 2, Stream 1 Research report, page 4
14	**Data recipients should provide information about measures taken in case of security breaches** Data recipients should clearly state, in an accessible and highly visible section of the app, the security measures that are being taken in order to secure any data being shared with them. They should also outline what will occur in the event of a data breach, including any notification protocols for consumers and steps taken to re-secure their data. These consequences should take into account the sensitivity of the data being stored, and the scope and consequences of the breach.	Phase 2, Stream 1 Research report, page 4

CX Research references

Ref #	Research findings	Source
15	**CDR Help** CDR helpline or contact information should be available in multiple languages.	Phase 2, Stream 1 Research report, page 4
16	**Accessibility of CDR information** CDR information site should have full translation functionality and be fully screen-reader accessible.	Phase 2, Stream 1 Research report, page 4
17	**The use of a One Time Password was perceived as secure** Authentication with One Time Password was seen as a smooth and more seamless process. The use of a verification code in this authentication method provided a sense of security for participants as they were used to receiving verification codes from their bank as an extra layer of security measure (i.e. 2-Factor authentication). *"Log in to the bank inside the app and with verification code as well. Feels more secure" - Phase 2, Round 2, Participant 12*	Phase 2, Stream 3 Research report, page 52
18	**Expectations of data once consent is expired/withdrawn** Phase 1: Most participants expected data to be deleted upon revocation, including 54% of surveyed participants. Phase 2: All participants expected that their data will be completely deleted/destroyed once data sharing had stopped. However, when stated that their data would be de-identified, participants feel uncomfortable which led to distrust, as it was perceived that their data would still be accessible.	Phase 1 CX report, p.48 Phase 2, Stream 3 Research report, page 66
19	**Presentation of data request information** Having all information available on one page but segmented for readability made participants feel the process of data sharing was more transparent and easier to understand.	Phase 2, Stream 1 Research report, page 49
20	**Provide a record of consent** The participants found it helpful to have a record of the consent process they had just completed and several participants noted that the confirmation email sent to them reinforced the trustworthiness of the overall process. *"That's good to know because I'm guessing… If I had a problem I could ring them and quote that number and then yeah. Okay. So that's reassuring."* - MH *"Cool, there's another consent receipt. I think these are really great, I love these."* - SK	Phase 2, Stream 1 Research report, page 35

CX Research references

Ref #	Research findings	Source
21	**Concerns about banking login information** Participants were not comfortable with putting sensitive information into the app such as passwords and customer IDs, particularly during redirection. Some stating that it could potentially lead to phishing scams.	Phase 2, Stream 3 Research report, page 23
22	**Clearly explain the redirection steps to the data holder space** Some participants correlated 'redirected' to being redirected to a 3rd party as the intermediary service to securely connect the app to the bank. While this wasn't causing any issues or concerns of drop out, it might be something to watch out for.	Phase 2, Stream 3 Research report, page 54
23	**The 'trust mark' helps facilitate consumer trust.** The majority of participants found the 'trust mark' to be helpful in identifying the data recipient as trustworthy. For some participants, the 'trust mark' drew their attention to the data holder's Consumer Data Right Accreditation details; for others,the simple check mark symbol in itself created a positive association with trust and security.	Phase 2, Stream 1 Research report, page 33 Phase 2, Stream 3 Research report, page 37
24	**Key and persistent concerns and anxieties about data sharing** Participants often imagined that the worst would happen to their data. To anticipate and assuage these concerns, data recipients should clearly state what data will not be used for. The following are key and persistent concerns and anxieties about data use. **These include:** - Selling data for marketing purposes - Unauthorised access by other parties, including government - CDR data being used to discriminate - Data use is unclear - Lack of trust in CDR participants to honour terms	Phase 1 and Phase 2 research
25	**Clearly articulate the sharing data value proposition** Data recipients should clearly explain the value added by sharing data to increase the chances of consumer adoption. Introducing the concept of data sharing without a clear value proposition will not be conducive to adoption. *"Without not knowing much more about it I'll probably not proceed... I'll just close it" -Phase 1, 5.3 Participant 20*	Phase 1 Research report, page 52

CX Research references

Ref #	Research findings	Source
26	**Consent should be a genuine choice and not a precondition of service** This consent flow model should not make consumers feel that access to their data and the security risks therein is the 'cost' of receiving services or benefits. Participants felt in general that they have little control over how their personal information is shared currently. This continual disempowerment has led to a state of apathy and indifference about how their personal data is used. *"I probably would like to have a little bit more to feel like you're not being spied on all the time, it would be nice. But, I guess, that's, once again, just gonna happen. You can't stop it." - Phase 2, Stream 2* Vulnerable users have more concerns about data misuse and were particularly concerned that their data would continue to exist in the system after withdrawing consent. Thus data recipients should be required to explain how consumer data will be handled during sharing and opt-out.	Phase 2, Stream 2 Research report, page 16 Phase 2, Stream 1 Research report, page 4
27	**Data recipients should use authenticators that are familiar to consumers** Participants from research noted that receiving verification codes from their bank as an extra layer of security measure is familiar to them. The verification code provides a sense of security and prevents consumers from having to change known behaviour.	Phase 2, Stream 3 Research report, pages 52, 53
28	**Product value proposition** Propensity to willingly share (consent) data is largely the result of expected value. Without a clear, compelling and timely value proposition, there is no reason to consent.	Phase 2, Stream 2 Research report, page 9
29	**Withdrawal language** Participants were not always clear what 'revoke' meant. Plain language phrase such as 'stop sharing' is recommended to replace this.	Phase 2, Stream 3 Research report, page 30
30	**Critical information should be up-front and on-screen** Critical information such as consequences of not consenting and ability to withdraw consent should be highlighted on-screen and should not require additional clicks to access. Where including additional information is not feasible, it should be clearly hyperlinked and easy to find.	Phase 2, Stream 1 Research report, page 70
31	**Importance of value proposition:** Participants' willingness to actively share information was tied directly to the value they expected to receive in return.	Phase 2, Stream 2 Report, pg 36

CX Research references

Ref #	Research findings	Source
32	**Comprehension of the consequences of consent withdrawal** It is imperative that consumers understand the consequence of sharing prior to withdrawal of consent. Research has shown that consumers tend to take a rushed approach to stop sharing which resulted in participants backtracking to better understand consequence. This is known as '“inattentional blindness'	Phase 2, Stream 2 Research report, page 19

Other references

Nielsen Norman Group. (2019). *10 Heuristics for User Interface Design: Article by Jakob Nielsen*. [online] Available at: https://www.nngroup.com/articles/ten-usability-heuristics/ [Accessed 1 Nov. 2019].

CONSUMER
DATA
STANDARDS

Consumer Data Standards | Consumer Experience Workstream

t +61 2 9490 5722
e cdr-data61-cx@csiro.au
w consumerdatastandards.org.au

www.consumerdatastandards.org.au