CONSUMER
DATA
STANDARDS

Consumer Experience Guidelines

Version 0.9.5

17 July 2019

Contents

Contents

Contents

Document management

This document has been reviewed and endorsed by the following:

Endorsement

Version	Date	Endorsed by
v0.9.5	16.07.2019	Chair of the Data Standards Body

Change log

Version	Date	Author(s)	Description of changes
v0.9.5	15.07.2019	MP, EC, BC	Working Draft CX Guidelines

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	Endorsement
1	Consent	These guidelines allow for the provision of consent at the level of data clusters and meet the requirements of the exposure draft of the CDR rules. Consultation and research have indicated that fine-grained consent will be needed within the regime. Further consultation on how fine-grained consent will be accommodated into the CDR regime will be undertaken. This will include further rounds of customer experience research.	*Endorsed: DSB Chair*
2	Authentication	The DSB has determined that a single, consistent, authentication flow will be adopted by the CDR regime. The redirect with one-time password will be incorporated into the standards as the proposed authentication flow. Guidelines and standards for this authentication flow are contained in this document.	*Endorsed: DSB Chair*
3	Re-authorisation	The DSB has determined that for version 1 of the CDR implementation the full authorisation flow will be required for any extensions of approval. 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.	*Endorsed: DSB Chair*

Decision Proposals

The below table contains a list of decision proposals. Some of these are not currently reflected in the CDR Rules or Standards and are being reviewed by the ACCC to, as appropriate, be elevated to the level of the CDR Rules, made into binding standards, or published as guidance.

#	Area	Decision for approval	Endorsement
1	Data language standard	Proposed data cluster language to be endorsed and made into a binding standard.	*Endorsed: DSB Chair*
2	Data language standard	Proposed data permissions language to be endorsed and made into a binding standard.	*Endorsed: DSB Chair*
3	Component 2.12: De-identification within duration	If the data recipient intends to de-identify CDR data during the sharing period they **must** receive consumer consent.	*Endorsed: DSB Chair*
4	Component 2.12: De-identification within duration	If the data recipient intends to de-identify CDR data during the sharing period, they **must** provide further information on what de-identification is, how data will be de-identified, and genuine examples of how de-identified data may be put to use.	*Endorsed: DSB Chair*
5	Component 2.13: Handling of redundant data	The data recipient **must** state the specific method they will attempt to use to handle redundant CDR data.	*Endorsed: DSB Chair*
6	Component 2.13: Handling of redundant data	If the data recipient intends to de-identify CDR data after the sharing period, they **must** provide further information on what de-identification is, how data will be de-identified, and genuine examples of how de-identified data may be put to use.	*Endorsed: DSB Chair*

Decision Proposals

#	Area	Decision for approval	Endorsement
7	Component 2.14: Review and revocation	The data recipient **must** provide a clear and consistent location for the consent management dashboard via which consent can be withdrawn.	*Endorsed: DSB Chair*
8	Component 2.14: Review and revocation	The data recipient **must** state that sharing arrangements for single collection requests can be reviewed via consent management dashboards.	*Endorsed: DSB Chair*
9	Component 2.15: Data holder selection	Data recipients **must** make data holder lists searchable.	*Endorsed: DSB Chair*
10	Component 2.16: Data holder selection	Data recipients **must** list data holders in alphabetical order.	*Endorsed: DSB Chair*
11	Component 2.16: Data holder selection	Data recipients **must** allow consumers to scroll through and select data holders from a list.	*Endorsed: DSB Chair*
12	Component 2.16: Data holder selection	Data recipients **must** not allow more than one data holder to be selected at a time.	*Endorsed: DSB Chair*
13	Component 2.16: Data holder selection	The data recipient **must** request CDR data in direct connection to each time a data holder is selected to avoid compromising the quality of consent.	*Endorsed: DSB Chair*
14	Component 2.16: Data holder selection	The data recipient **must** not allow the consumer to select several data holders at once, complete authorisation for one, and then return to the session at some point in the future to connect more data holders without seeing the data request screens again.	*Endorsed: DSB Chair*

Decision Proposals

#	Area	Decision for approval	Endorsement
15	Component 2.17: Pre-authentication	Data recipients **must** notify consumers of redirection prior to doing so.	*Endorsed: DSB Chair*
16	Component 3.1: Customer ID	Data holders **must** not include a forgotten password link in redirect screens. The inclusion of links to reset password is considered to increase the likelihood of phishing attacks.	*Endorsed: DSB Chair*
17	Component 3.1: Customer ID	Data holders and data recipients **must** state in consumer-facing interactions and material that ADRs will never ask consumers for their banking password to access CDR data.	*Endorsed: DSB Chair*
18	Component 3.2: One Time Password delivery	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.	*Endorsed: DSB Chair*
19	Component 3.3: One Time Password instructions	Data holders and data recipients **must** clearly refer to the OTP as a “One Time Password” in consumer-facing interactions and material.	*Endorsed: DSB Chair*
20	Component 3.3: One Time Password instructions	Data holders and data recipients **must** state in consumer-facing interactions and material that ADRs will never ask consumers for their banking password to access CDR data.	*Endorsed: DSB Chair*
21	Component 3.3: One Time Password instructions	The provided OTP **must** be invalidated after a period of time at the discretion of the Data Holder.	*Endorsed: DSB Chair*

Decision Proposals

#	Area	Decision for approval	Endorsement
22	Component 3.3: One Time Password instructions	The expiry of the OTP **must** be communicated in the authentication flow.	*Endorsed: DSB Chair*
23	Component 4.5: Review and revocation	The data holder **must** provide a clear and consistent location for the consent management dashboard via which consent can be withdrawn.	*Endorsed: DSB Chair*
24	Component 4.5: Review and revocation	Data holders **must** state that sharing arrangements for single collection requests can be reviewed via authorisation management dashboards.	*Endorsed: DSB Chair*
25	Accessibility	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.	*Endorsed: DSB Chair*
26	Accessibility	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.	*Endorsed: DSB Chair*
27	Accessibility	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 through various inputs beyond a keyboard.	*Endorsed: DSB Chair*
28	Accessibility	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.	*Endorsed: DSB Chair*
29	Accessibility	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.	*Endorsed: DSB Chair*

Glossary

Definition of terms used within 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 be considered an accredited data recipient.*

Authenticate *When a consumer verifies themselves with a data holder prior to authorising the sharing of their CDR data.*

Authorise *Granting permission for the data holder to share the requested CDR data with a data recipient.*

CDR *Consumer Data Right*

CDR logo *Official Consumer Data Right branding to be provided by ACCC*

CDR rules *Rules defined by ACCC, specifically Exposure Draft of the Competition and Consumer (Consumer Data) Rules 2019, outlining what is expected of participants in the CDR ecosystem.*

CDS *Consumer Data Standards, technical advisor to the Data Standards Body for the Consumer Data Right. The Consumer Data Standards Program is part of CSIRO's Data61.*

Consent *A consumer agreeing to the terms of a sharing agreement for an organisation to collect and use their CDR data. Technically distinguished from the final affirmative action (i.e. 'authorise') in the Consent Flow.*

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 *Data has been grouped into categories through CX research. These groupings are referred to as 'data clusters'. 'Data cluster language' refers to the name of each group. Refer to 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

Definition of terms used in the CX Guidelines.

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.

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 that may be accessed via an endpoint is referred to as a permission. These 'permissions' are grouped by data cluster. Refer to the Data Language Standards for examples.

Purpose

The reason(s) for the data request. The purpose specifies why the data recipient needs the requested data to provide a product or service.

Reauthorise

Permission given by a consumer for a sharing arrangement to continue (for an agreed period) beyond the expiry date of the current sharing arrangement.

Revoke

Withdrawing consent or authorisation is also referred to as 'revocation'. This occurs when a consumer stops sharing or cancels a sharing arrangement.

Sharing arrangement

An instance of data sharing that a consumer has consented to and the terms that apply to this instance.

Trustmark

Official Consumer Data Right branding that may be used by an organisation to show that they are an accredited data recipient.

Value proposition

A consumer's perception of the usefulness of a product or service offered by a data recipient.

Wireframe

A two-dimensional illustration of a page's interface that specifically focuses on space allocation and prioritisation of content, functionalities available, and intended behaviors.

Overview

Overview

The Australian government is introducing a Consumer Data Right (CDR) giving consumers greater control over their data. Part of this right requires the creation of common technical standards making it easier and safer for consumers to access data held about them by businesses, and – if they choose to – share this data via application programming interfaces (APIs) with trusted, accredited third parties.

The Consumer Data Right is intended to apply sector by sector across the whole economy, beginning in the banking sector, and followed by the energy and telecommunications sectors.

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.

CSIRO's Data61 has been appointed as technical advisor for an interim standards body, designing the first iteration of open technical standards to support consumer-driven data sharing. The work is progressing through four open work streams, sharing feedback and progress with the broader Australian and international community.

One of these workstreams has been specifically focused on the Consumer Experience of the Consumer Data Right.

Alongside the technical standards, the Consumer Experience (CX) Guidelines created by the CX Workstream have been developed to help organisations provide consumers with a simple, informed, and trusted data sharing experience.

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 focus on best practice design patterns for organisations seeking consent from consumers to access their data, and cover:

- the process and decision points that a consumer steps through when consenting to share their data;
- what (and also how) information should be presented to consumers to support informed decision making; and
- particular language that should be used (where appropriate) to ensure a consistent experience for consumers across the broader CDR ecosystem.

The guidelines included here, and the supporting examples illustrating their implementation, are presented as a valid interpretation of the CDR Rules.

Outputs of the CX Workstream's consultation and research can be found here as well as a blog here. Major updates from the Consumer Data Standards program can be found here

Developing the CX Guidelines

These guidelines have been developed for the Australian context through extensive consumer research, industry consultation, and in collaboration with various government agencies.

In total, 202 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.

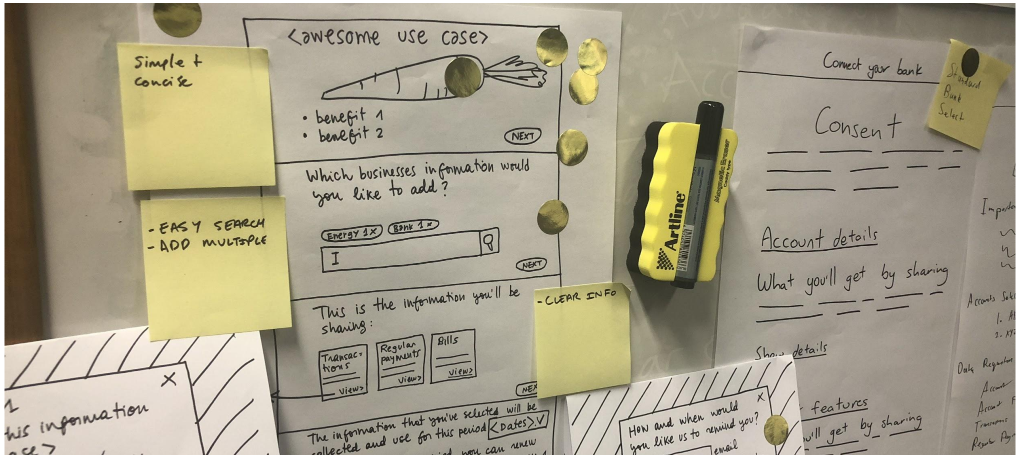
Feedback and guidance has also been provided by an Advisory Committee, spanning representatives from the financial sector, FinTechs, consumer groups, energy and telecommunications representatives and software vendors.

Outputs of this consultation and research can be found here as well as a blog here.

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 revocation
    - Stream 3: consent flow, authentication models, reauthorisation, and notifications
- 3x industry workshops involving data holders, data recipients, and consumer advocacy groups.

This version of the guidelines focuses on banking as the first designated sector. Further phases of CX research and design activities are planned to build on version 1 of the CDR standards and to facilitate the expansion of the CDR into other sectors.



How to use this document

The aim of the CX Workstream is to help organisations provide consumers with simple, informed, and trusted data sharing experiences that conform to the CDR Rules. These guidelines are a manifestation of this intent and have been developed to help organisations deploy applications for use in the CDR.

This document has been developed with data holders and data recipients in mind as the intended primary audience. The guidelines have been developed to ensure any CDR implementation use adopts an evidence-based approach and reflects best practice design patterns, facilitates informed consent, and builds consumer trust in data sharing.

Throughout the document, guidelines are presented as either **Mandatory** or **Recommended**.

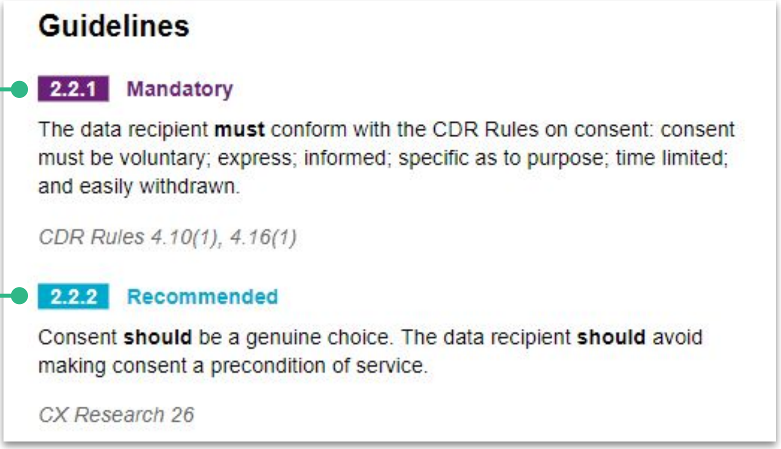
- **Mandatory**: guidelines are denoted as required where they are directly linked to a specific CDR Rules reference. In these cases the rule(s) is referenced alongside the guideline.
- **Recommended**: guidelines are denoted as recommended where they are linked to outcomes of stakeholder consultation, heuristic evaluation, and/or CX Research findings. Where appropriate, a reference is provided alongside the guideline.

The key words **must**, **must not**, **should**, **should not**, and **may** are to be interpreted as described in RFC2119

The rules referenced throughout the guidelines are detailed in the *Exposure Draft of the Competition and Consumer (Consumer Data) Rules 2019*, published on 29th March, 2019.

Breaches of the specific CDR Rules, in addition to any of the 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.

*Guidelines which are **mandatory** are accompanied by a specific CDR Rules reference. In some instances they will also be accompanied by an additional reference to the CX Research.*



Guidelines

2.2.1 Mandatory

The data recipient **must** conform with the CDR Rules on consent: consent must be voluntary; express; informed; specific as to purpose; time limited; and easily withdrawn.

CDR Rules 4.10(1), 4.16(1)

2.2.2 Recommended

Consent **should** be a genuine choice. The data recipient **should** avoid making consent a precondition of service.

CX Research 26

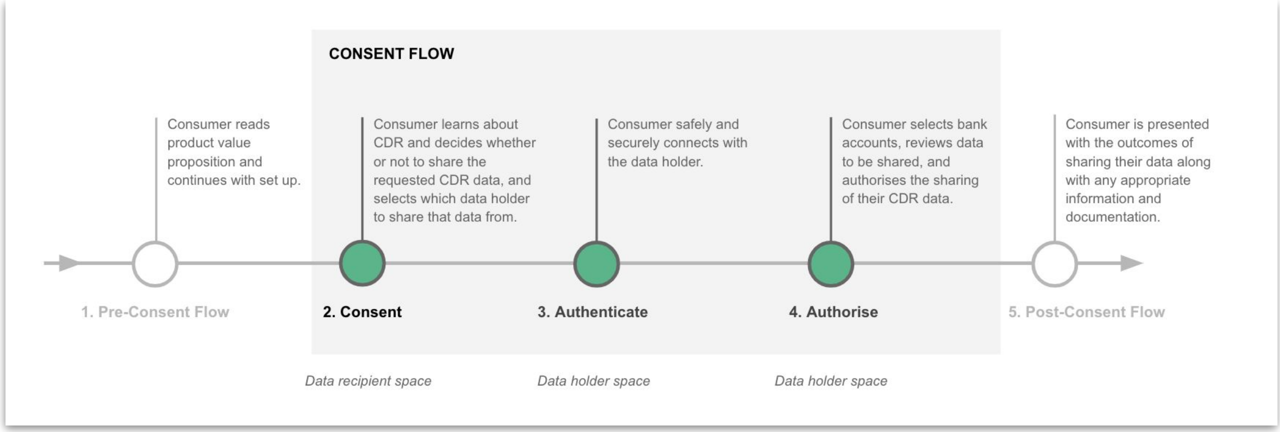
*Guidelines which are **recommended** are accompanied by a reference to the CX Research.*

How to use this document

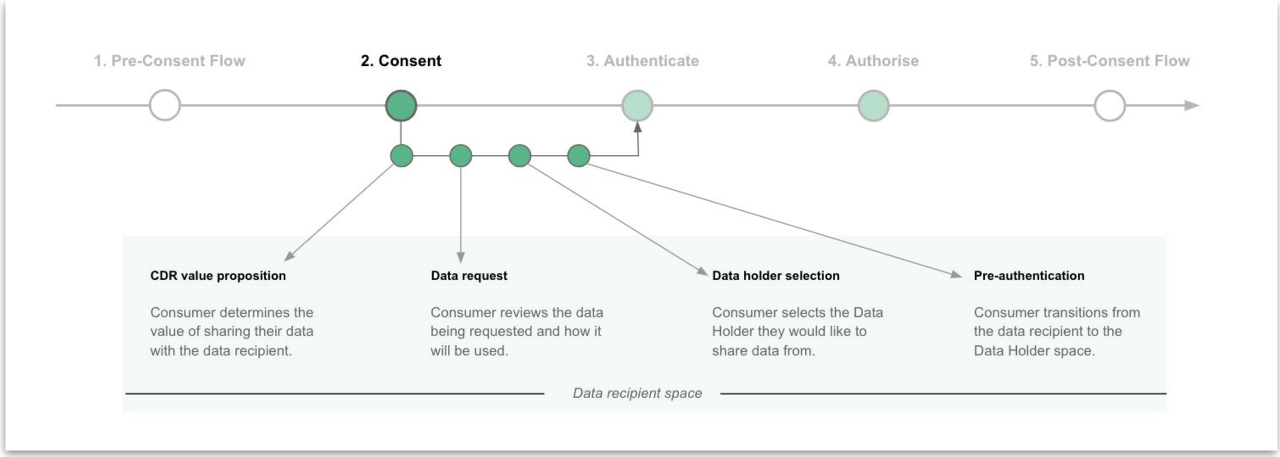
This version of the guidelines focuses on the 3 main stages of the Consent Flow (Consent, Authenticate, and Authorise).

The guidelines are presented in the form of modular components to allow each component to be combined and deployed as appropriate.

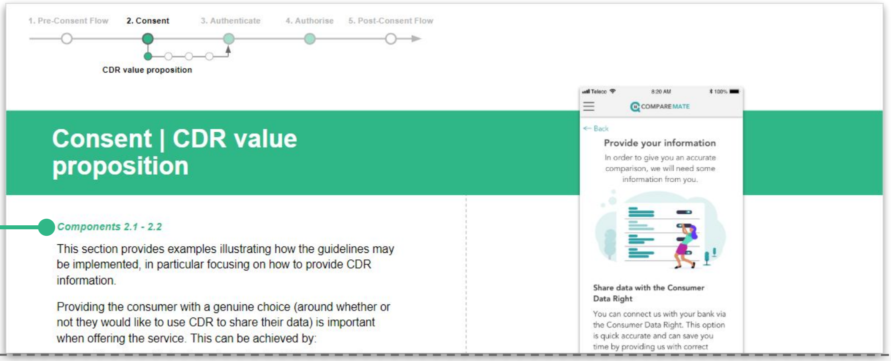
The Consent Flow is comprised of three main stages.


CONSENT FLOW
Consumer reads product value proposition and continues with set up.
Consumer learns about CDR and decides whether or not to share the requested CDR data, and selects which data holder to share that data from.
Consumer safely and securely connects with the data holder.
Consumer selects bank accounts, reviews data to be shared, and authorises the sharing of their CDR data.
Consumer is presented with the outcomes of sharing their data along with any appropriate information and documentation.
1. Pre-Consent Flow
2. Consent
3. Authenticate
4. Authorise
5. Post-Consent Flow
Data recipient space
Data holder space
Data holder space

Each stage of the Consent Flow is further broken down into a series of steps.


1. Pre-Consent Flow
2. Consent
3. Authenticate
4. Authorise
5. Post-Consent Flow
CDR value proposition
Consumer determines the value of sharing their data with the data recipient.
Data request
Consumer reviews the data being requested and how it will be used.
Data holder selection
Consumer selects the Data Holder they would like to share data from.
Pre-authentication
Consumer transitions from the data recipient to the Data Holder space.
Data recipient space

How to use this document



1. Pre-Consent Flow 2. Consent 3. Authenticate 4. Authorise 5. Post-Consent Flow

CDR value proposition

Consent | CDR value proposition

Components 2.1 - 2.2

This section provides examples illustrating how the guidelines may be implemented, in particular focusing on how to provide CDR information.

Providing the consumer with a genuine choice (around whether or not they would like to use CDR to share their data) is important when offering the service. This can be achieved by:

Teleco
8:20 AM
100%
COMPAREMATE
← Back
Provide your information
In order to give you an accurate comparison, we will need some information from you.
Share data with the Consumer Data Right
You can connect us with your bank via the Consumer Data Right. This option is quick accurate and can save you time by providing us with correct

Each section includes one or more components.

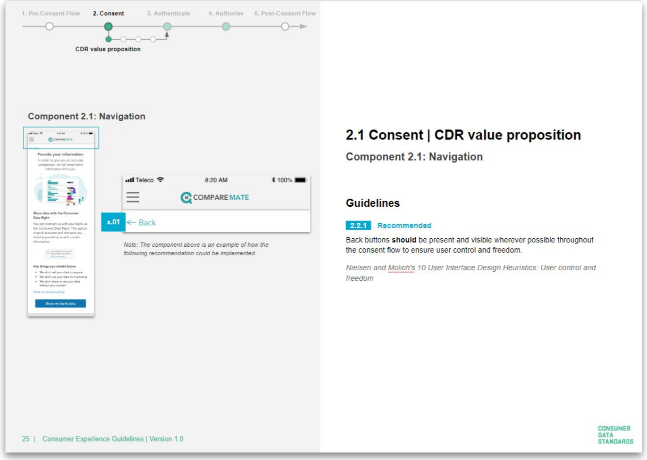
The wireframes illustrated alongside the guidelines are included to demonstrate examples of how to put the CDR Rules into effect. These interpretations are to be validated and endorsed by the ACCC.

The guidelines do not necessarily prescribe how to put the rules into effect, but aligning with these is recommended to help provide a consistent and familiar CDR ecosystem that consumers 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. CDR implementation must align to the rules and standards regardless of the consumer's device.

References to the CDR rules can be found in the Exposure draft CDR rules on the ACCC website. References to the CX research can be found in the Appendix.

Wireframes illustrate example implementations of the guidelines.



1. Pre-Consent Flow 2. Consent 3. Authenticate 4. Authorise 5. Post-Consent Flow

CDR value proposition

Component 2.1: Navigation

Note: The component above is an example of how the following recommendation could be implemented.

2.1 Consent | CDR value proposition

Component 2.1: Navigation

Guidelines

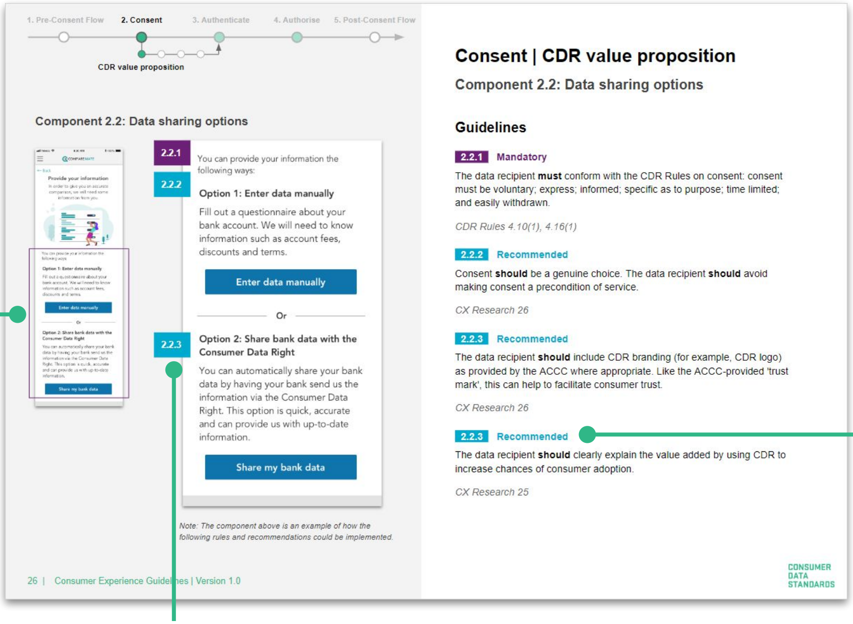
2.2.1 Recommended

Back buttons **should** be present and visible wherever possible throughout the consent flow to ensure user control and freedom.

Nielsen and Molich's 10 User Interface Design Heuristics: User control and freedom

25 | Consumer Experience Guidelines | Version 1.0

CONSUMER DATA STANDARDS



1. Pre-Consent Flow 2. Consent 3. Authenticate 4. Authorise 5. Post-Consent Flow

CDR value proposition

Component 2.2: Data sharing options

2.2.1 2.2.2 You can provide your information the following ways:

Option 1: Enter data manually

Fill out a questionnaire about your bank account. We will need to know information such as account fees, discounts and terms.

2.2.3 Option 2: Share bank data with the Consumer Data Right

You can automatically share your bank data by having your bank send us the information via the Consumer Data Right. This option is quick, accurate and can provide us with up-to-date information.

Note: The component above is an example of how the following rules and recommendations could be implemented.

Consent | CDR value proposition

Component 2.2: Data sharing options

Guidelines

2.2.1 Mandatory

The data recipient **must** conform with the CDR Rules on consent: consent must be voluntary; express; informed; specific as to purpose; time limited; and easily withdrawn.

CDR Rules 4.10(1), 4.16(1)

2.2.2 Recommended

Consent **should** be a genuine choice. The data recipient **should** avoid making consent a precondition of service.

CX Research 26

2.2.3 Recommended

The data recipient **should** include CDR branding (for example, CDR logo) as provided by the ACCC where appropriate. Like the ACCC-provided 'trust mark', this can help to facilitate consumer trust.

CX Research 26

2.2.3 Recommended

The data recipient **should** clearly explain the value added by using CDR to increase chances of consumer adoption.

CX Research 25

26 | Consumer Experience Guidelines | Version 1.0

CONSUMER DATA STANDARDS

The outlined area specifies where the component lies in the example wireframe

These numbers correspond to the rule / recommendation on the left

This is the specific component. These components are examples of how the rules/recommendations can be implemented.

CONSUMER DATA STANDARDS

Consent

Consent

A consumer's ability to offer genuine consent when deciding to share their data is central to the Consumer Data Right. Consent-driven data sharing will give consumers with more control of their data 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.

For consent to be genuine, it **must** meet the following requirements:

- Consent **must** be voluntary, express, informed, specific as to purpose, time limited and easily withdrawn.
- An accredited data recipient **must** not make consent a precondition to obtaining another unrelated product or service. The collection of CDR data **must** be reasonably necessary or required to provide the good or service the accredited data recipient is offering.
- An accredited data recipient **must** not bundle consent with other directions, permissions, consents or agreements.

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.

Factors relevant to deciding whether consent is voluntary include:

- the alternatives open to the individual if they choose not to consent
- the seriousness of any consequences to the individual if they choose not to consent
- any adverse consequences for family members or associates of the individual if the individual chooses not to consent.

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 the sharing agreement is associated with.

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 guidance for seeking and receiving consent from consumers. The Consent Model represents the current scope of the CX Workstream. 'Consent Model' refers to:

The Consent Flow

- Consent (the data recipient requesting consumer data)
- Authentication (the consumer authenticating themselves with the data holder)
- Authorisation (the consumer authorising the data holder to their share with the data recipient)

Consent Management

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

Revocation

- Withdrawing the consent/authorisation of data sharing

Reauthorisation

- Consent durations will last up to 12 months, and consumers will need to reauthorise data sharing prior to the arrangement expiring if they wish to continue sharing CDR data with a data recipient.

The CX Workstream will provide guidance and advice 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 trusted CDR ecosystem. Combining these frameworks 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 revoke sharing
- Understand the implications of revocation
- Feel confident and informed about the sharing of their data
- Understand how to navigate the Consent Model

This document provides a best view of the Consent Flow with guidelines on other items to follow in further phases of CX research where appropriate.

Accessibility

In 2015, almost one in five Australians reported living with disability, roughly 18.3% or 4.3 million people. Making consent more accessible will make consent simpler and easier for everyone. The importance of this was highlighted by participants in consumer research.

Data recipients and data holders **should** make the Consent Model as accessible and easy to comprehend as possible. This document 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 usable to people in general. WCAG address accessibility of web content on desktops, laptops, tablets, and mobile devices.

At a minimum, all CDR participants **must** seek to comply with the following accessibility guidelines to facilitate informed consent across a diverse range of users. These guidelines **must** be applied throughout the Consent Model. Special attention **must** be paid to typography and layout, and specific attention **must** be paid to the Consent Flow.

These recommendations represent the CX Workstream's best view of accessibility guidelines to be complied with. They will need to be considered by the community and should ideally be assessed and refined further by accessibility consultants.

WCAG 1.4 **Mandatory**

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.

CX Research 15, 16, 37

WCAG 2.1 **Mandatory**

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.

CX Research 15, 16, 37

WCAG 2.5 **Mandatory**

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 through various inputs beyond a keyboard.

CX Research 15, 16, 37

WCAG 3.1 **Mandatory**

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.

CX Research 15, 16, 37

WCAG 3.3 **Mandatory**

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.

CX Research 15, 16, 37

Data Language Standards

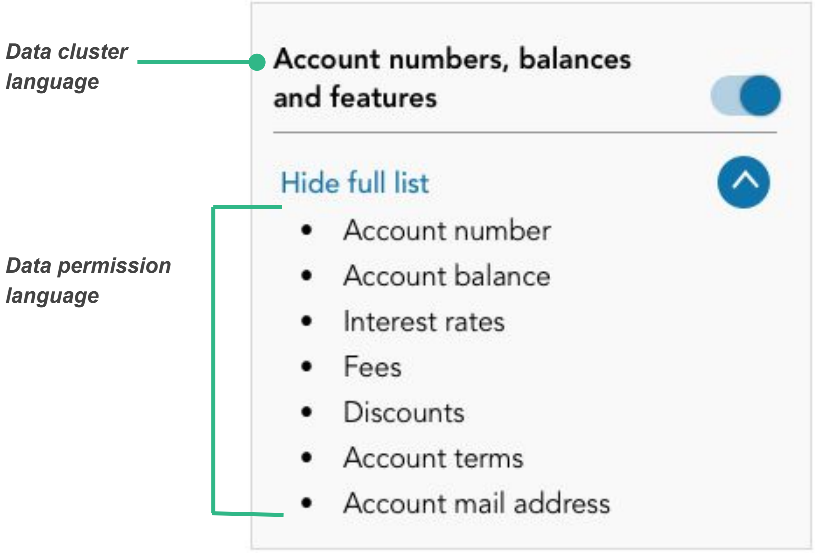
Data language standards

In accordance with the CDR Rules 8.11(1)(c), a data standard **must** be set which provides descriptions of the types of data to be used by CDR participants in making and responding to requests. These descriptions will be made into a binding data standard and use of them will be mandatory for data recipients and data holders.

The data language standards outlined on the next page have been shaped by consumer research and community consultation conducted by the CX Workstream.

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.

In addition to the guidelines found in this document, the Authorisation Scopes section in the API Standards will provide additional guidance and technical specifics on how to implement this decision.



Account numbers, balances and features

Hide full list

- Account number
- Account balance
- Interest rates
- Fees
- Discounts
- Account terms
- Account mail address

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

Mandatory

The data recipient and data holder **must** list the data clusters consented to be shared. Permission language within each data cluster **must** also be listed.

CDR Rule 4.22(2)(c)

Mandatory

Specific language **must** be used for data clusters and permissions.

CDR Rule 8.11

Recommended

The data recipient and data holder **should** include in-line help (e.g. questions marks) to provide a more detailed but plain-English (grade 7 readability) descriptions of what is included in the data cluster, including permissions.

Data language standards

Data Cluster Language	Permission language	Authorisation scopes
Name and occupation	Name; Occupation	common_basic_customer
Organisation profile*	Agent name and role; Organisation name; Organisation numbers (ABN or ACN); Charity status; Establishment date; Industry; Organisation type; Country of registration	common_basic_customer
Contact details	Phone; Email address; Mail address; Residential address	common_detailed_customer
Organisation contact details*	Organisation address; Mail address; Phone number	common_detailed_customer
Account name and type	Name of account; Type of account	bank_basic_accounts
Account numbers, balances and features	Account number; Account balance; Interest rates; Fees; Discounts; Account terms; Account mail address	bank_detailed_accounts
Transaction details	Incoming and outgoing transactions; Amounts; Dates; Description of transactions; Who you've sent money to and received money from *(e.g. names, BSB's, and account numbers)***	bank_transactions
Direct debits and scheduled payments	Direct debits; Scheduled payments	bank_regular_payments
Saved payees	Names and account details of people and organisations whose details you've saved *(e.g. BSB and Account Number, BPay CRN and Biller code or NPP PayID)***	bank_payees

***Note**: these data clusters are defined specifically for business (rather than individual) consumers.

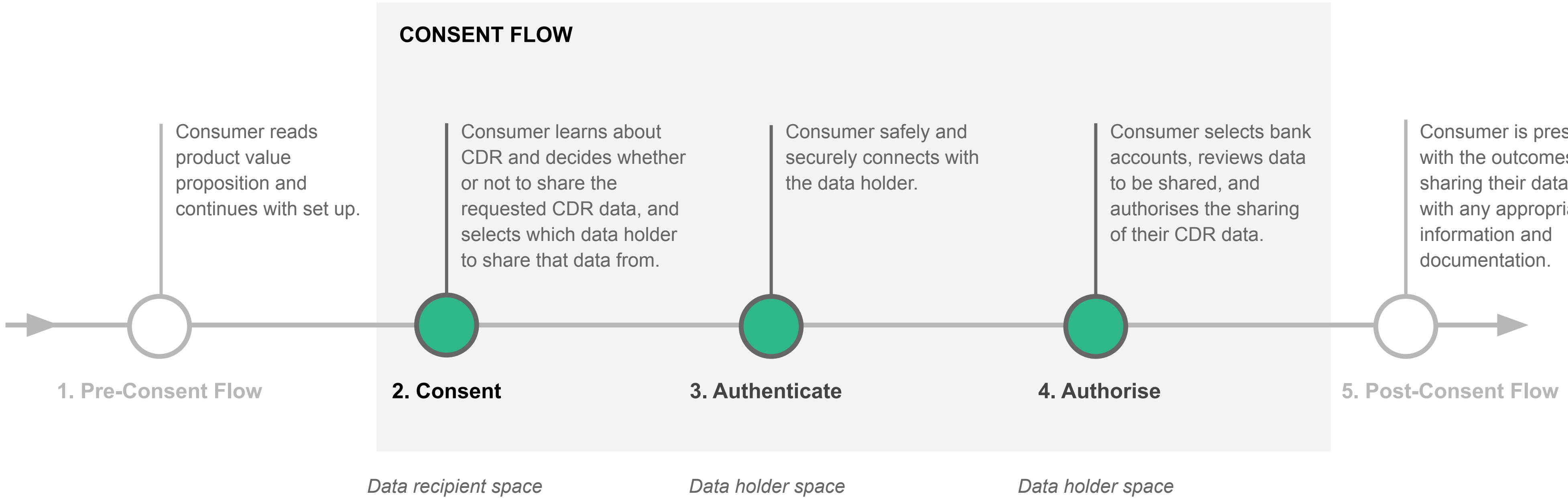
****Note**: Items in italics are provided as an example description of the permission that **may** be provided as in-line help.

Consent Flow: Consumer journey

CONSENT FLOW: CONSUMER JOURNEY OVERVIEW

The following are stages of the consumer journey of the consent flow with the inclusion of the consumer experience before and after the consent flow.

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



CONSENT FLOW

Consumer reads product value proposition and continues with set up.

Consumer learns about CDR and decides whether or not to share the requested CDR data, and selects which data holder to share that data from.

Consumer safely and securely connects with the data holder.

Consumer selects bank accounts, reviews data to be shared, and authorises the sharing of their CDR data.

Consumer is presented with the outcomes of sharing their data along with any appropriate information and documentation.

1. Pre-Consent Flow

2. Consent

3. Authenticate

4. Authorise

5. Post-Consent Flow

Data recipient space

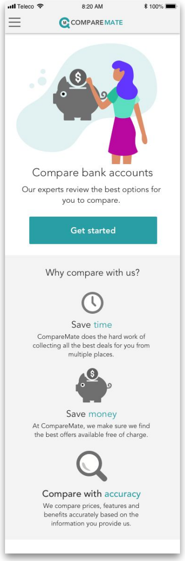
Data holder space

Data holder space

CONSENT FLOW: CONSUMER JOURNEY OVERVIEW

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

1. PRE-CONSENT



Compare bank accounts

Our experts review the best options for you to compare.

Why compare with us?

Save time

CompareMate does the hard work of collecting all the best deals for you from multiple places.

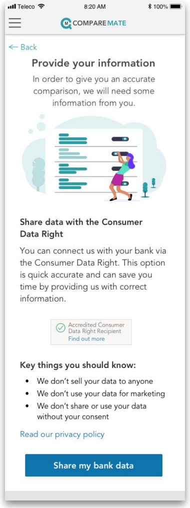
Save money

At CompareMate, we make sure we find the best offers available free of charge.

Compare with accuracy

We compare prices, features and benefits accurately based on the information you provide us.

2. CONSENT



Provide your information

In order to give you an accurate comparison, we will need some information from you.

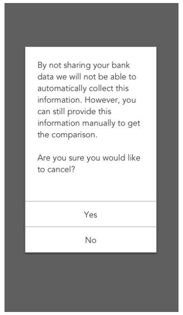
Share data with the Consumer Data Right

You can connect us with your bank via the Consumer Data Right. This option is quick accurate and can save you time by providing us with correct information.

Key things you should know:

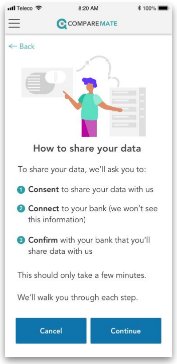
- We don't sell your data to anyone
- We don't use your data for marketing
- We don't share or use your data without your consent

Read our privacy policy



By not sharing your bank data we will not be able to automatically collect this information. However, you can still provide this information manually to get the comparison.

Are you sure you would like to cancel?



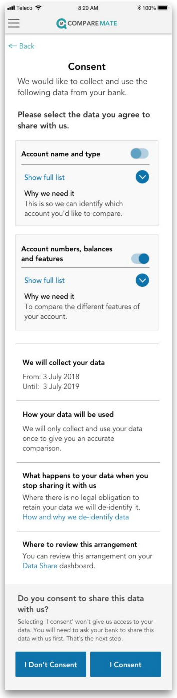
How to share your data

To share your data, we'll ask you to:

1. **Consent** to share your data with us
2. **Connect** to your bank (we won't see this information)
3. **Confirm** with your bank that you'll share data with us

This should only take a few minutes.

We'll walk you through each step.



Consent

We would like to collect and use the following data from your bank.

Please select the data you agree to share with us.

Account name and type

Show full list

Why we need it
This is so we can identify which account you'd like to compare.

Account numbers, balances and features

Show full list

Why we need it
To compare the different features of your account.

We will collect your data

From: 3 July 2018
Until: 3 July 2019

How your data will be used

We will only collect and use your data once to give you an accurate comparison.

What happens to your data when you stop sharing it with us

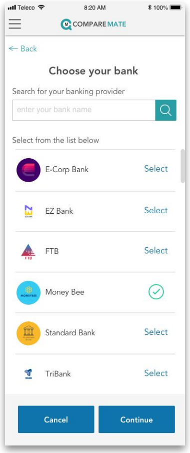
Where there is no legal obligation to retain your data we will de-identify it.
How and why we de-identify data

Where to review this arrangement

You can review this arrangement on your Data Share dashboard.

Do you consent to share this data with us?

Selecting 'I consent' won't give us access to your data. You will need to ask your bank to share this data with us first. That's the next step.

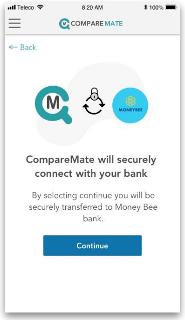


Choose your bank

Search for your banking provider

Select from the list below

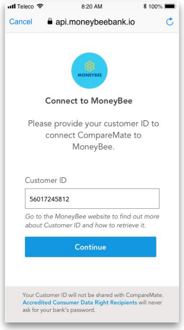
E-Corp Bank	Select
EZ Bank	Select
FTB	Select
Money Bee	✓
Standard Bank	Select
TriBank	Select



CompareMate will securely connect with your bank

By selecting continue you will be securely transferred to Money Bee bank.

3. AUTHENTICATE



Connect to MoneyBee

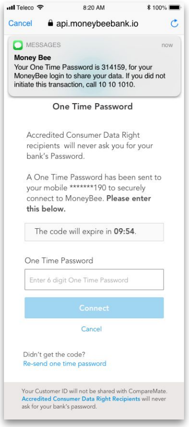
Please provide your customer ID to connect CompareMate to MoneyBee.

Customer ID

56017245812

Go to the MoneyBee website to find out more about Customer ID and how to retrieve it.

Your Customer ID will not be shared with CompareMate. Accredited Consumer Data Right Recipients will never ask for your bank's password.



Money Bee
Your One Time Password is 314159, for your MoneyBee login to share your data. If you did not initiate this transaction, call 10 10 1010.

One Time Password

Accredited Consumer Data Right recipients will never ask you for your bank's Password.

A One Time Password has been sent to your mobile *******190 to securely connect to MoneyBee. **Please enter this below.**

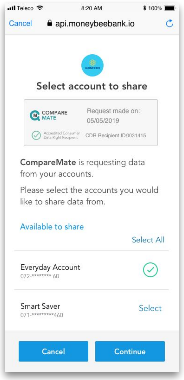
The code will expire in **09:54**.

One Time Password

Didn't get the code?
Re-send one time password

Your Customer ID will not be shared with CompareMate. Accredited Consumer Data Right Recipients will never ask for your bank's password.

4. AUTHORISE


Teleco 8:20 AM 100%
Cancel api.moneybeebank.io
MONEYBEE
COMPARE MATE
Accredited Consumer Data Right Recipient
Cancel
Continue

Select account to share

Request made on: 05/05/2019
CDR Recipient ID.0031415

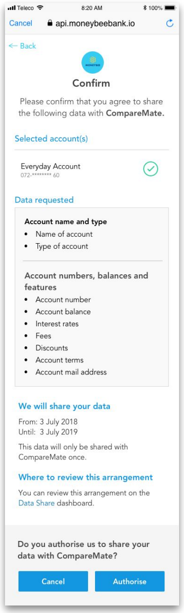
CompareMate is requesting data from your accounts.

Please select the accounts you would like to share data from.

Available to share

Select All

Everyday Account 072-******** 60	✓
Smart Saver 071-*********460	Select



Confirm

Please confirm that you agree to share the following data with **CompareMate.**

Selected account(s)

Everyday Account ✓
072-******** 60

Data requested

Account name and type

- Name of account
- Type of account

Account numbers, balances and features

- Account number
- Account balance
- Interest rates
- Fees
- Discounts
- Account terms
- Account mail address

We will share your data

From: 3 July 2018
Until: 3 July 2019

This data will only be shared with CompareMate once.

Where to review this arrangement

You can review this arrangement on the Data Share dashboard.

Do you authorise us to share your data with CompareMate?

Data recipient space

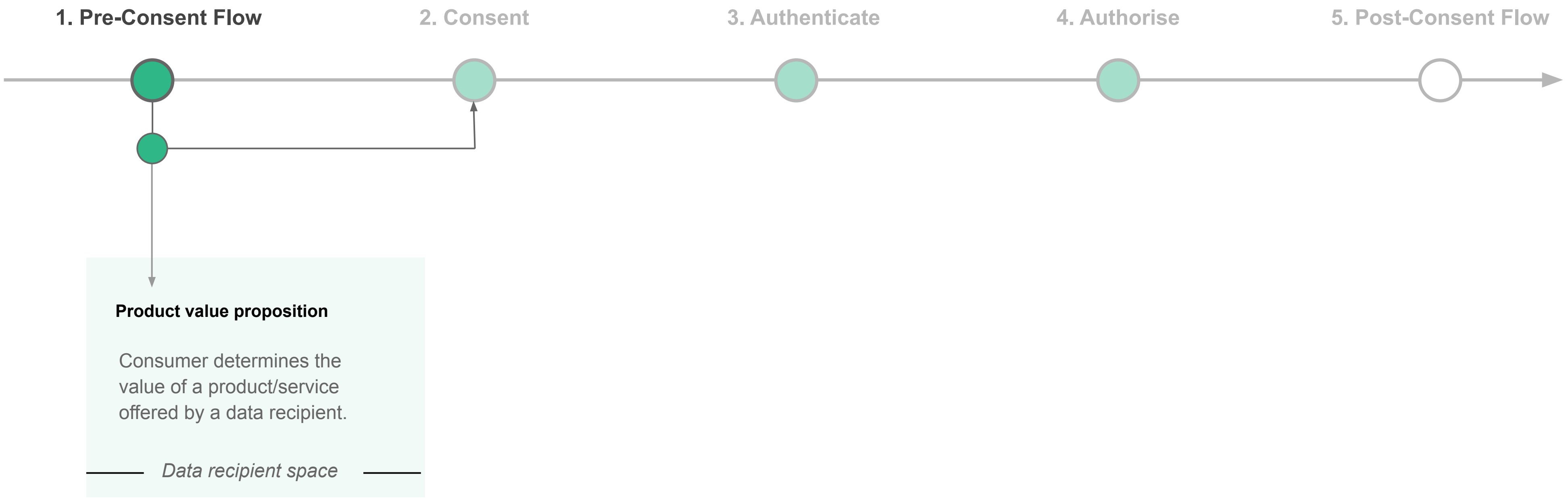
Data holder space

1. PRE-CONSENT FLOW

The Pre-Consent stage consists of a general onboarding experience and takes place prior to the Consent Flow. In order to increase consumer propensity to share and adoption to the CDR, it is critical to include product value proposition information at this stage to progressively build consumer trust. Trust **should** be built from the start of this stage and continue throughout the consent flow.

Product value proposition

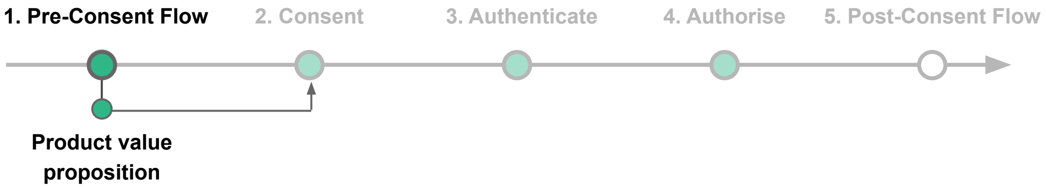
During this onboarding experience, the consumer will be presented with a product or service offered by the data recipient and determine the value and usefulness of that product/service. The propensity to share personal information at this point will correlate to the extent of expected benefits one can receive. Without a clear, compelling and timely value proposition, there is no reason to consent to data sharing.



Product value proposition

Consumer determines the value of a product/service offered by a data recipient.

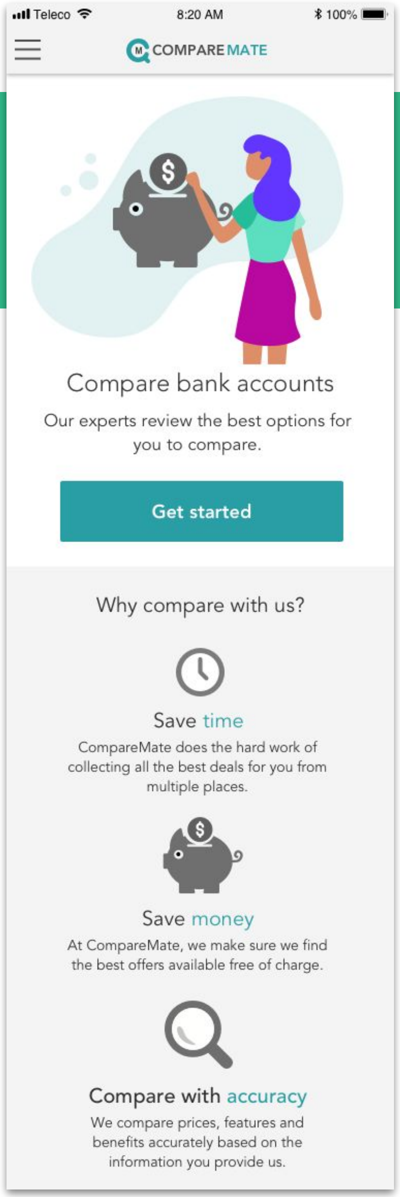
Data recipient space



Pre-consent | Product value proposition

Components 1.1

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 with unrelated purposes.



Compare bank accounts

Our experts review the best options for you to compare.

Get started

Why compare with us?

Save time

CompareMate does the hard work of collecting all the best deals for you from multiple places.

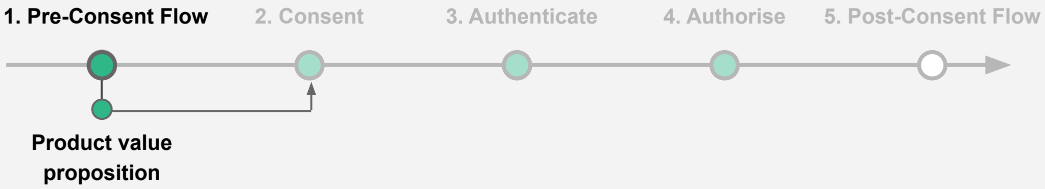
Save money

At CompareMate, we make sure we find the best offers available free of charge.

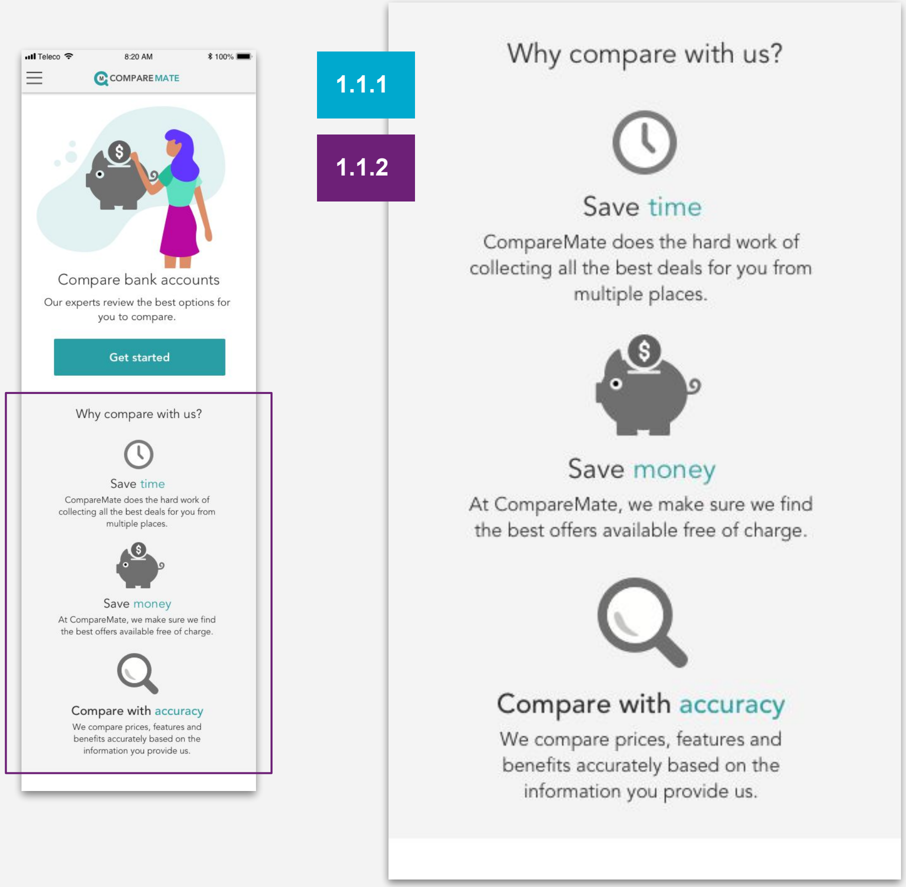
Compare with accuracy

We compare prices, features and benefits accurately based on the information you provide us.

Example wireframe 1



Component 1.1: Product value proposition



Compare bank accounts

Our experts review the best options for you to compare.

Get started

Why compare with us?

Save time

CompareMate does the hard work of collecting all the best deals for you from multiple places.

Save money

At CompareMate, we make sure we find the best offers available free of charge.

Compare with accuracy

We compare prices, features and benefits accurately based on the information you provide us.

Why compare with us?

Save time

CompareMate does the hard work of collecting all the best deals for you from multiple places.

Save money

At CompareMate, we make sure we find the best offers available free of charge.

Compare with accuracy

We compare prices, features and benefits accurately based on the information you provide us.

Note: The component above is an example of how the following recommendations could be implemented.

Pre-consent | Product value proposition

Component 1.1: Product value proposition

Guidelines

1.1.1 Recommended

The data recipient **should** build trust and onboard the consumer to the service itself before presenting a data request.

CX Research 1, 25, 28

1.1.2 Mandatory

The data recipient **must not** bundle consent with unrelated purposes.

The data recipient **must not** rely on, for example, pre-selected options to indicate the data that the consent relates to.

The data recipient **must not** infer consent or rely on an implied consent.

CDR Rules 4.10(3), 4.16(3) | *CX Research 36*

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

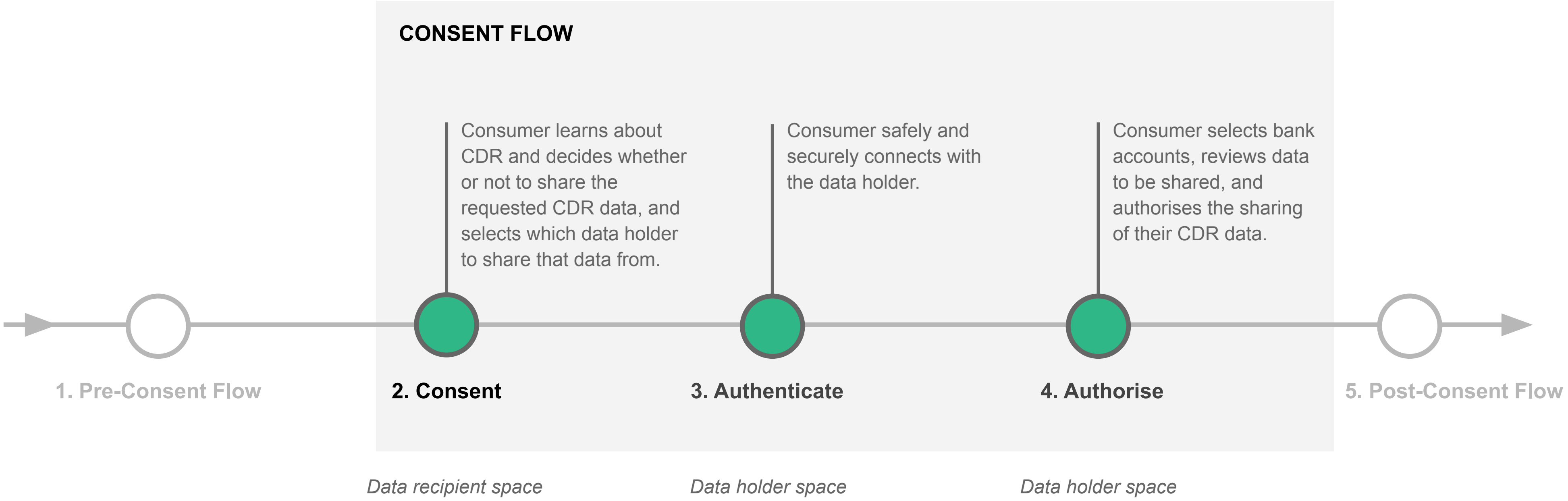
Authenticate

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.



CONSENT FLOW

Consumer learns about CDR and decides whether or not to share the requested CDR data, and selects which data holder to share that data from.

Consumer safely and securely connects with the data holder.

Consumer selects bank accounts, reviews data to be shared, and authorises the sharing of their CDR data.

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.

CDR value proposition

At this step, the data recipient should communicate the value and purpose of sharing CDR data. 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.

Data request

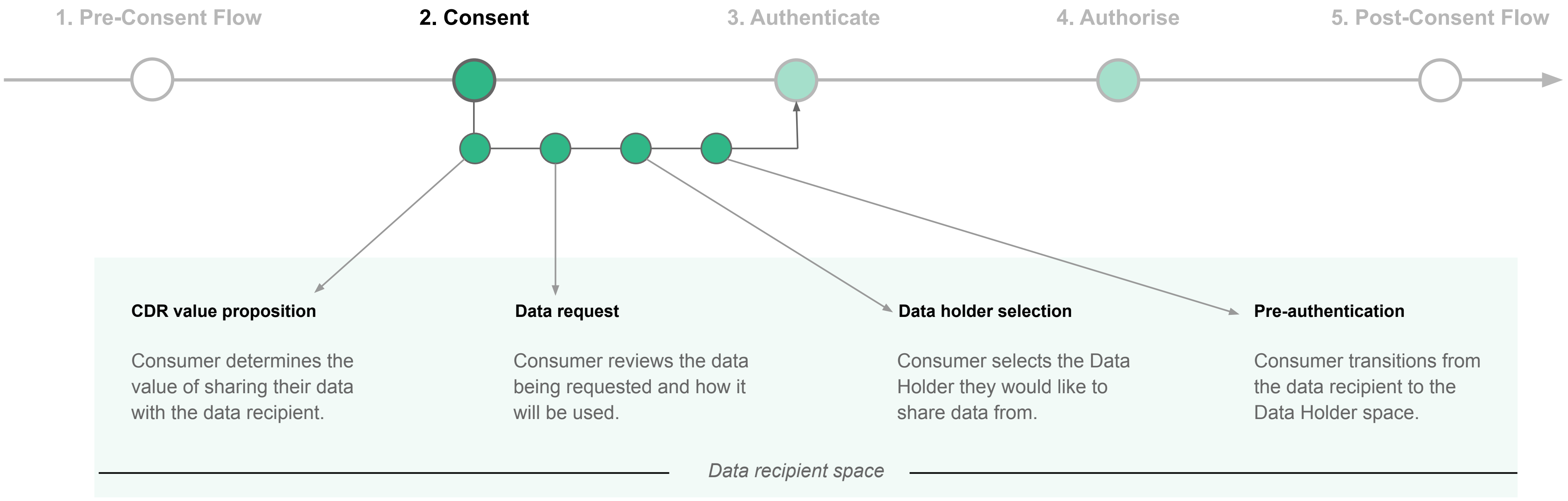
At this step, the consumer will be able to review a summary of the data that the Data Recipient is requesting.

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.



CDR value proposition

Consumer determines the value of sharing their data with the data recipient.

Data request

Consumer reviews the data being requested and how it will be used.

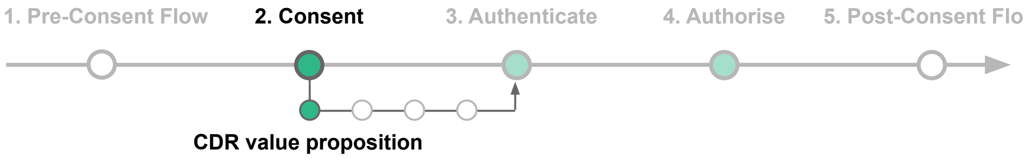
Data holder selection

Consumer selects the Data Holder they would like to share data from.

Pre-authentication

Consumer transitions from the data recipient to the Data Holder space.

Data recipient space



1. Pre-Consent Flow

2. Consent

3. Authenticate

4. Authorise

5. Post-Consent Flow

CDR value proposition

Consent | CDR value proposition

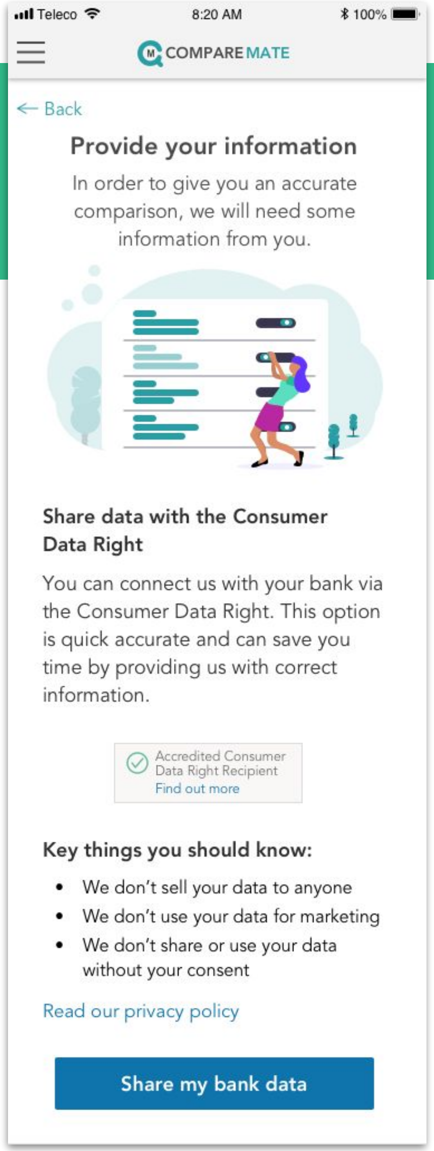
Components 2.1 - 2.2

This section provides examples illustrating how the guidelines may be implemented, in particular focusing on how to 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 using CDR to support consumer decision making
- The use of a ‘trust mark’ to show accreditation status and Consumer Data Right branding (for example, a logo) to build consumer trust.
- Information on how consumer data will be handled when data sharing is active and upon revocation/expiry.
- Clearly explaining how CDR data *won’t* be used in a way that has regime-wide consistency

This CDR educational information **should** presented upfront or on a separate page in an easy to understand and digestible manner (we recommend a simple and standardised ACCC document, infographic, comic contract, or whatever is suitable).



Provide your information

In order to give you an accurate comparison, we will need some information from you.

Share data with the Consumer Data Right

You can connect us with your bank via the Consumer Data Right. This option is quick accurate and can save you time by providing us with correct information.

Accredited Consumer Data Right Recipient
Find out more

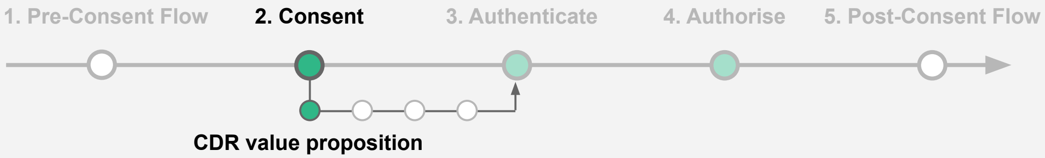
Key things you should know:

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

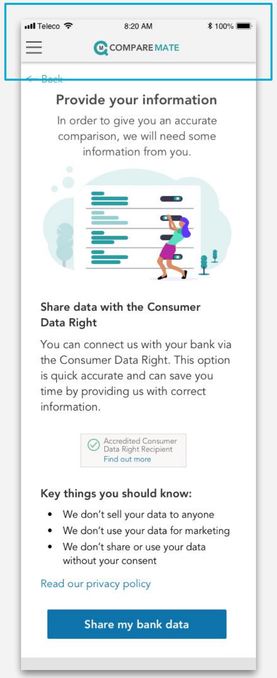
Read our privacy policy

Share my bank data

Example wireframe 2.1



Component 2.1: Navigation


Teleco 8:20 AM 100%

COMPARE MATE

← Back

Provide your information

In order to give you an accurate comparison, we will need some information from you.

Share data with the Consumer Data Right

You can connect us with your bank via the Consumer Data Right. This option is quick accurate and can save you time by providing us with correct information.

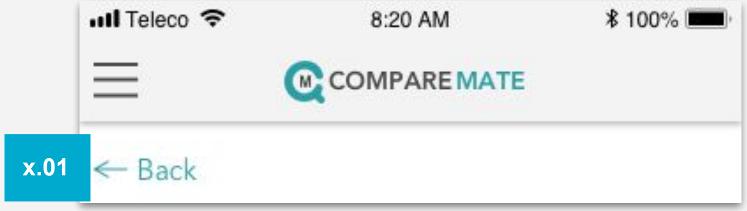
Accredited Consumer Data Right Recipient
Find out more

Key things you should know:

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

Read our privacy policy

Share my bank data


Teleco 8:20 AM 100%

COMPARE MATE

x.01 ← Back

Note: The component above is an example of how the following recommendation can be implemented.

Consent | CDR value proposition

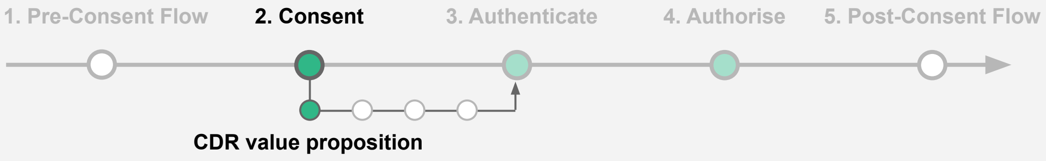
Component 2.1: Navigation

Guidelines

2.2.1 Recommended

Back buttons **should** be present and visible wherever possible throughout the consent flow to ensure user control and freedom.

Nielsen and Molich's 10 User Interface Design Heuristics: User control and freedom



1. Pre-Consent Flow

2. Consent

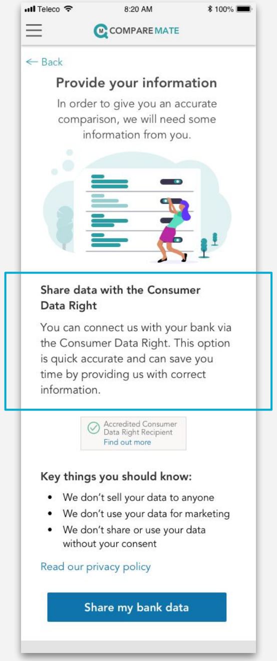
3. Authenticate

4. Authorise

5. Post-Consent Flow

CDR value proposition

Component 2.2: CDR information



Provide your information

In order to give you an accurate comparison, we will need some information from you.

Share data with the Consumer Data Right

You can connect us with your bank via the Consumer Data Right. This option is quick accurate and can save you time by providing us with correct information.

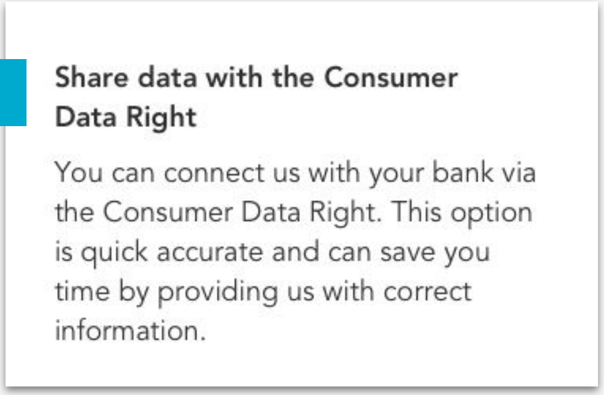
Accredited Consumer Data Right Recipient
Find out more

Key things you should know:

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

Read our privacy policy

2.2.1



Share data with the Consumer Data Right

You can connect us with your bank via the Consumer Data Right. This option is quick accurate and can save you time by providing us with correct information.

Note: The component above is an example of how the following rules and recommendations can be implemented.

Consent | CDR value proposition

Component 2.2: CDR information

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

CX Research 26

Guidelines

Mandatory

The data recipient **must** conform with the CDR Rules on consent: consent must be voluntary; express; informed; specific as to purpose; time limited; and easily withdrawn.

CDR Rules 4.10(1), 4.16(1)

Recommended

Consent **should** be a genuine choice. The data recipient **should** avoid making consent a precondition of service.

CX Research 26

2.2.1 Recommended

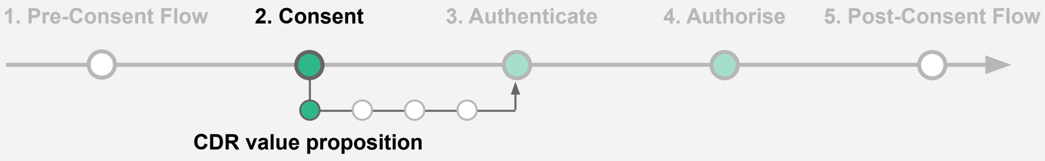
The data recipient **should** include CDR branding (for example, a CDR logo) as provided by the ACCC where appropriate.

CX Research 23

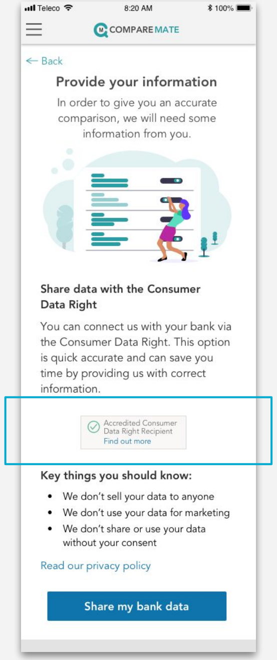
2.2.1 Recommended

The data recipient **should** clearly communicate the value of sharing data as part of the CDR.

CX Research 25



Component 2.3: Accreditation information



Teleco 8:20 AM 100%

COMPAREMATE

← Back

Provide your information

In order to give you an accurate comparison, we will need some information from you.

Share data with the Consumer Data Right

You can connect us with your bank via the Consumer Data Right. This option is quick accurate and can save you time by providing us with correct information.

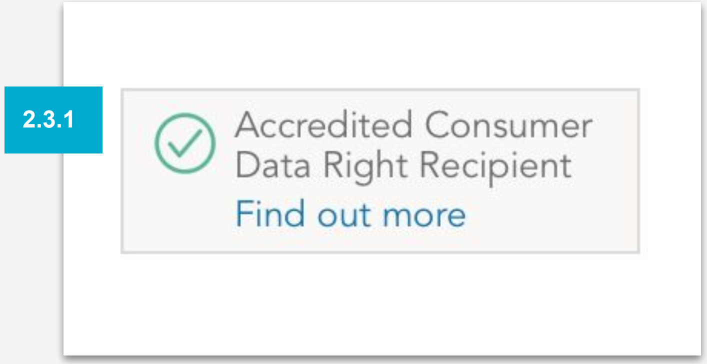
Accredited Consumer Data Right Recipient
Find out more

Key things you should know:

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

Read our privacy policy

Share my bank data



Accredited Consumer Data Right Recipient

Find out more

Note: The component above is an example of how the following recommendations can be implemented.

Consent | CDR value proposition

Component 2.3: Accreditation information

> *"I saw the little green tick box and went, 'Oh yes, they're reliable, authentic, real, honest, trustworthy people.'"*
>
> *CX Research 23*

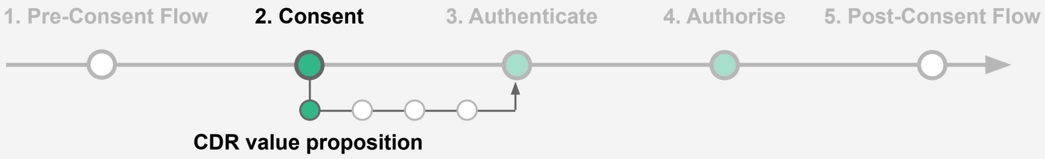
Guidelines

2.3.1 Recommended

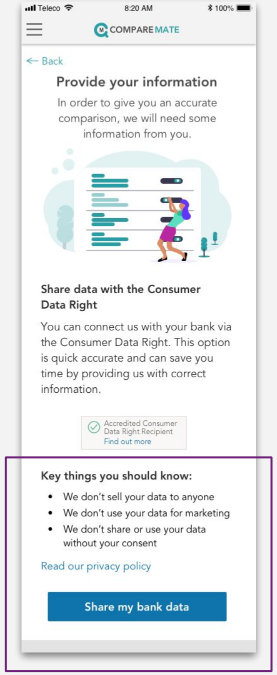
The data recipient **should** present any trust mark required by the ACCC to provide consistency and facilitate consumer trust.

The data recipient **should** provide a way for consumers to verify their accreditation via the ACCC.

CX Research 13, 23



Component 2.4: Data sharing rules



Provide your information

In order to give you an accurate comparison, we will need some information from you.

Share data with the Consumer Data Right

You can connect us with your bank via the Consumer Data Right. This option is quick accurate and can save you time by providing us with correct information.

Accredited Consumer Data Right Recipient
Find out more

Key things you should know:

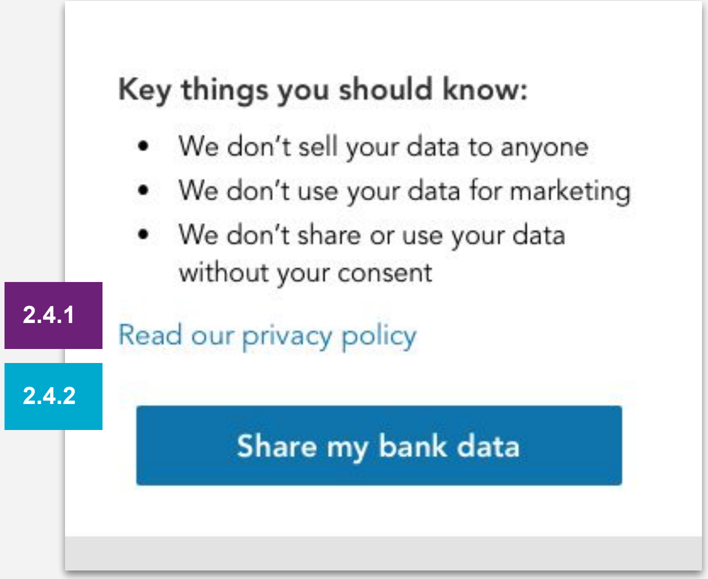
- We don't sell your data to anyone
- We don't use your data for marketing
- We don't share or use your data without your consent

Read our privacy policy

Share my bank data

2.4.1

2.4.2



Key things you should know:

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

Read our privacy policy

Share my bank data

Note: The component above is an example of how the following rules and recommendation can be implemented.

Consent | CDR value proposition

Component 2.4: Data sharing rules

Guidelines

2.4.1 Mandatory

The data recipient **must** make their CDR policy readily available on their website or mobile app. This **may** be included at this point with the data recipient's own privacy policy.

CDR Rules 7.2(4), 7.2(5)

2.4.1 Mandatory

The data recipient **must** include clear and unambiguous information on how CDR data will be handled upon consent revocation/expiry. This **should** be presented up front, and wherever applicable throughout the consent model.

CDR Rule 4.16(6) | CX Research 33

2.4.1 Mandatory

The data recipient **must not** include documents or references to other documents that reduce comprehension.

Any links to information that increase comprehension **should not** take the consumer to an external page.

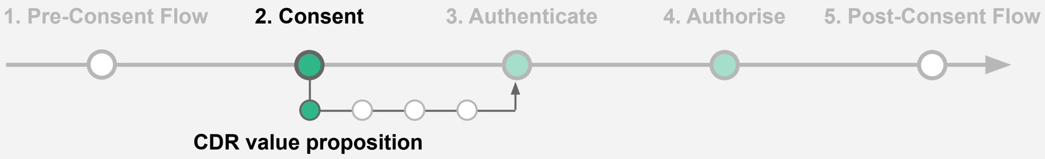
CDR Rule 4.10(2)(c), 4.16(2)(c)

2.4.2 Recommended

The data recipient **should** provide information, where applicable, about measures taken in case of security breaches.

CX Research 14

CONSUMER
DATA
STANDARDS



1. Pre-Consent Flow

2. Consent

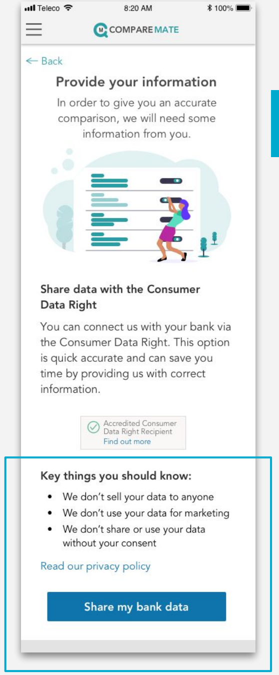
3. Authenticate

4. Authorise

5. Post-Consent Flow

CDR value proposition

Component 2.4: Data sharing rules (continued)



← Back

Provide your information

In order to give you an accurate comparison, we will need some information from you.

Share data with the Consumer Data Right

You can connect us with your bank via the Consumer Data Right. This option is quick accurate and can save you time by providing us with correct information.

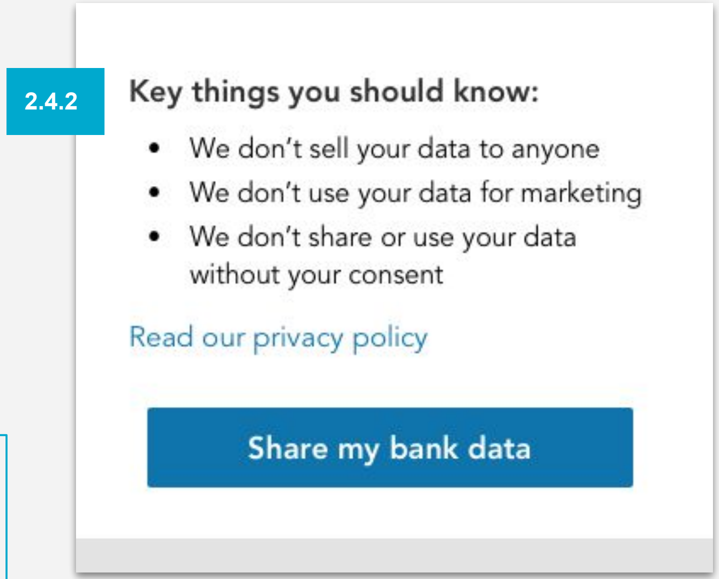
Accredited Consumer Data Right Recipient
Find out more

Key things you should know:

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

Read our privacy policy

Share my bank data



2.4.2

Key things you should know:

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

Read our privacy policy

Share my bank data

Note: The component above is an example of how the following recommendations can be implemented.

Consent | CDR value proposition

Component 2.4: Data sharing rules (continued)

Guidelines

2.4.2 Recommended

The data recipient **should** clearly state how data will *not* be used. For example:

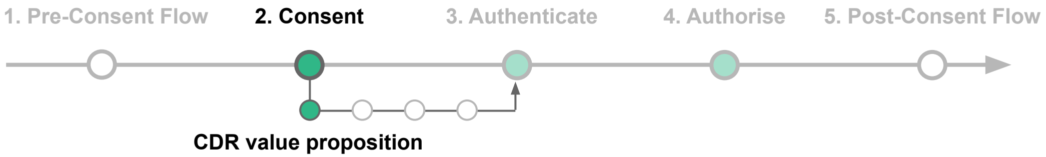
- We don't sell your data to anyone
- We don't use your data for marketing
- We don't use your data for anything other than the purpose(s) you consented to
- We don't share your data without your consent

CX Research 24

2.4.2 Recommended

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

CX Research 16



Consent | CDR value proposition

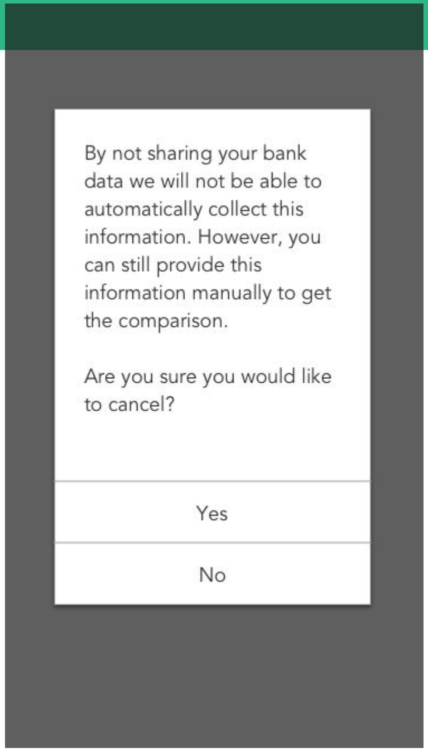
Cancellation screen

Component 2.5

This section provides examples illustrating how the guidelines may be implemented, in particular focusing on the step for cancelling a data sharing 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.

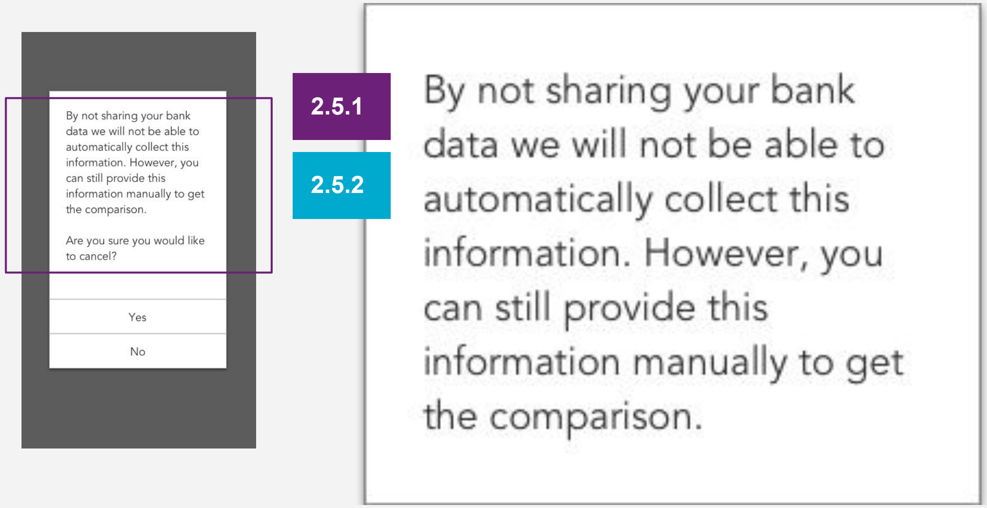
The rules and recommendations outlined on the next page **should** be implemented where possible whenever the cancel option is selected throughout the consent flow.


By not sharing your bank data we will not be able to automatically collect this information. However, you can still provide this information manually to get the comparison.

Are you sure you would like to cancel?

Example wireframe 2.2

Component 2.5: Cancellation



By not sharing your bank data we will not be able to automatically collect this information. However, you can still provide this information manually to get the comparison.

Are you sure you would like to cancel?

Note: The component above is an example of how the following rules and recommendation can be implemented.

Consent | CDR value proposition

Component 2.5: Cancellation

Guidelines

2.5.1 Required

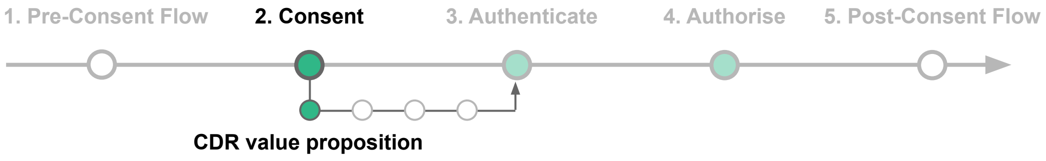
The data recipient **must** conform with the CDR Rules on consent: consent must be voluntary, express, informed, specific as to purpose, time limited and easily withdrawn.

CDR Rules 4.10(1), 4.16(1)

2.5.2 Recommended

Consent **should** be a genuine choice. The data recipient **should** avoid making consent a precondition of service.

CX Research 26



Consent | CDR value proposition

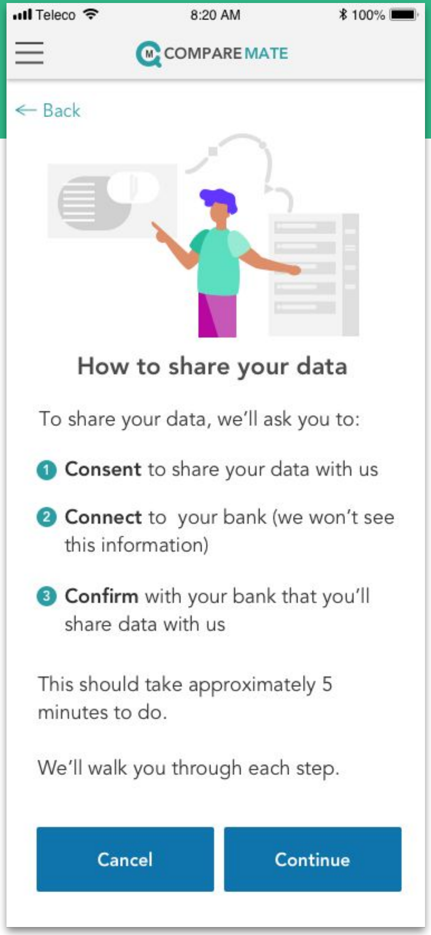
CDR data sharing instructions

Component 2.6

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.



How to share your data

To share your data, we'll ask you to:

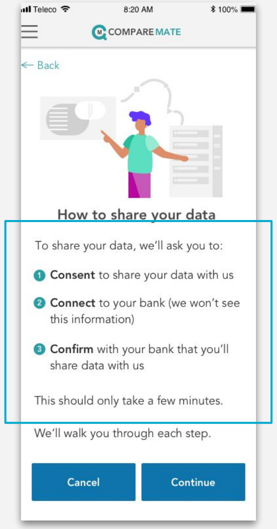
1. **Consent** to share your data with us
2. **Connect** to your bank (we won't see this information)
3. **Confirm** with your bank that you'll share data with us

This should take approximately 5 minutes to do.

We'll walk you through each step.

Example wireframe 2.3

Component 2.6: CDR data sharing instructions



Teleco 8:20 AM 100%

COMPAREMATE

← Back

How to share your data

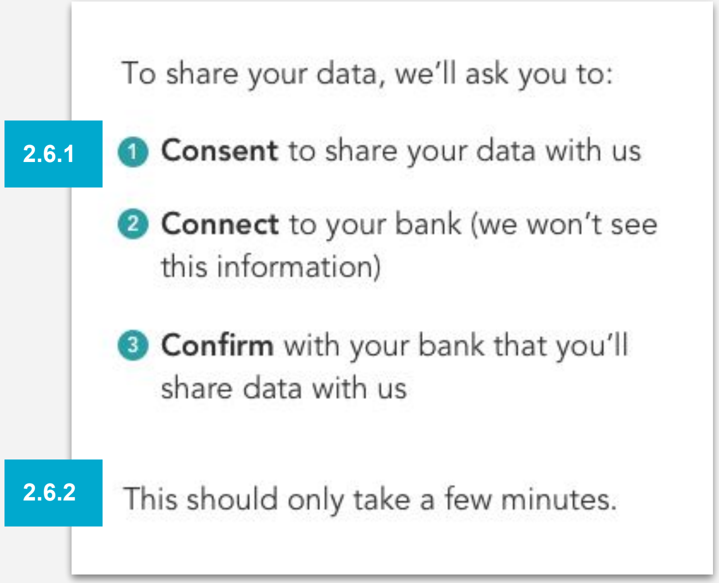
To share your data, we'll ask you to:

1. **Consent** to share your data with us
2. **Connect** to your bank (we won't see this information)
3. **Confirm** with your bank that you'll share data with us

This should only take a few minutes.

We'll walk you through each step.

Cancel | Continue



To share your data, we'll ask you to:

2.6.1

1. **Consent** to share your data with us
2. **Connect** to your bank (we won't see this information)
3. **Confirm** with your bank that you'll share data with us

2.6.2

This should only take a few minutes.

Note: The component above is an example of how the following recommendations can be implemented.

Consent | CDR value proposition

Component 2.6: CDR data sharing instructions

Guidelines

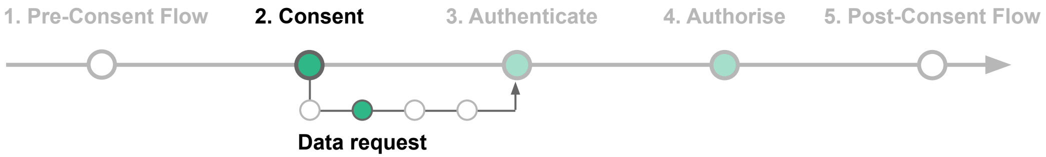
2.6.1 Recommended

The data recipient **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.

Nielsen and Molich's 10 User Interface Design Heuristics: Consistency and standards

2.6.2 Recommended

The data recipient **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 | Data request

Component 2.7 - 2.14

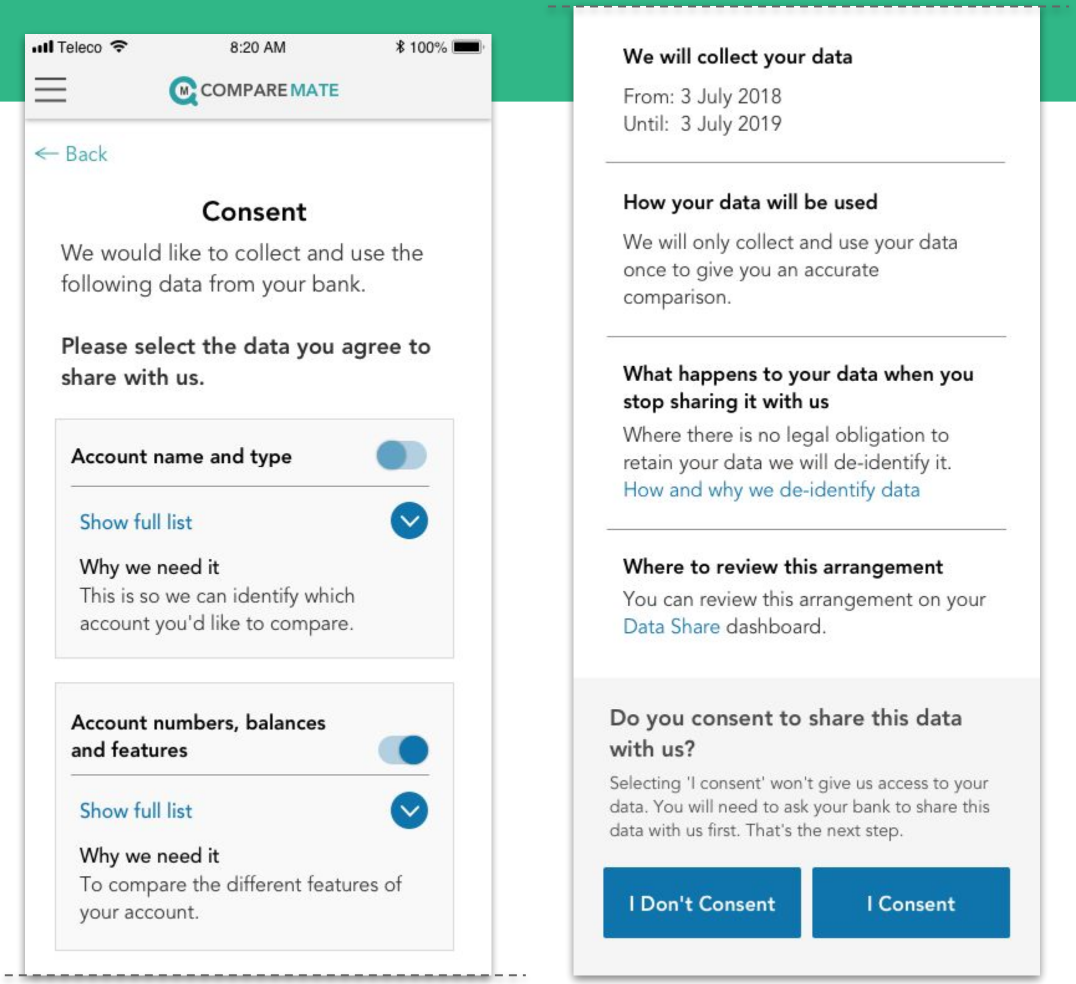
This section provides examples illustrating how the guidelines may be implemented.

Example implementation

The components contained in this section are based on the example to the left, where two data clusters are being requested: Account details and Account features. These data clusters are presented on a single screen. The consumer is required to select “I Consent” once to agree to the data sharing 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 segment information for readability and use interaction patterns. These **may** include patterns that use pagination, carousel cards, or ones similar to Typeform.



Consent

We would like to collect and use the following data from your bank.

Please select the data you agree to share with us.

Account name and type

Show full list

Why we need it

This is so we can identify which account you'd like to compare.

Account numbers, balances and features

Show full list

Why we need it

To compare the different features of your account.

We will collect your data

From: 3 July 2018
Until: 3 July 2019

How your data will be used

We will only collect and use your data once to give you an accurate comparison.

What happens to your data when you stop sharing it with us

Where there is no legal obligation to retain your data we will de-identify it.
How and why we de-identify data

Where to review this arrangement

You can review this arrangement on your Data Share dashboard.

Do you consent to share this data with us?

Selecting 'I consent' won't give us access to your data. You will need to ask your bank to share this data with us first. That's the next step.

Example wireframe 2.4

Greater consumer control for data requests

Wherever possible and appropriate, data recipients **should** provide as much consumer control as possible. This **may** include allowing consumers to choose which data clusters they do or do not want to share.

Greater consumer control **may** also include actively consenting to the specific uses or allowing consumers to amend the sharing duration both historically (in the past) and into the future.

These guidelines allow for the provision of consent at the level of data clusters and meet the requirements of the exposure draft of the CDR rules.

Consultation and research have indicated that fine-grained consent will be needed within the regime. Further consultation on how fine-grained consent will be accommodated into the CDR regime will be undertaken. This will include further rounds of customer experience research.

Guidelines

Mandatory

The data recipient **must** allow the consumer to actively select or actively specify the types of data and the uses they consent to.

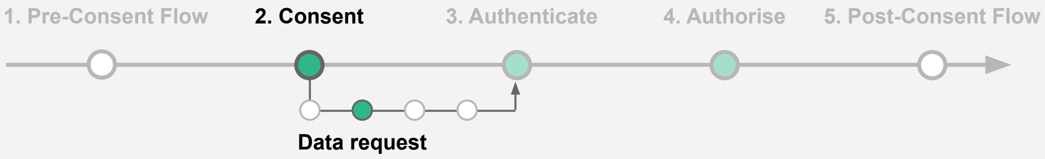
If data is being requested for multiple uses, the consumer **must** be able to specify which uses they consent to.

The data recipient **must not** rely on, for example, pre-selected options to indicate the data that the consent relates to.

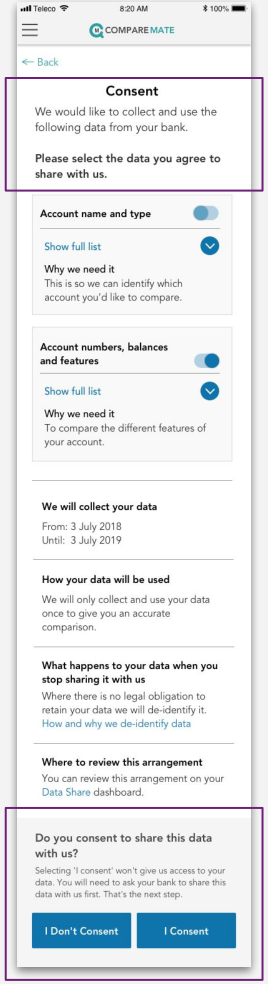
The data recipient **must not** infer consent or rely on an implied consent.

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 4.10(3), 4.16(3) | *CX Research 2, 3, 4, 5, 6*



Component 2.7: Active consent



Teleco 8:20 AM 100%

COMPARE MATE

← Back

Consent

We would like to collect and use the following data from your bank.

Please select the data you agree to share with us.

Account name and type

Show full list

Why we need it

This is so we can identify which account you'd like to compare.

Account numbers, balances and features

Show full list

Why we need it

To compare the different features of your account.

We will collect your data

From: 3 July 2018
Until: 3 July 2019

How your data will be used

We will only collect and use your data once to give you an accurate comparison.

What happens to your data when you stop sharing it with us

Where there is no legal obligation to retain your data we will de-identify it.
How and why we de-identify data

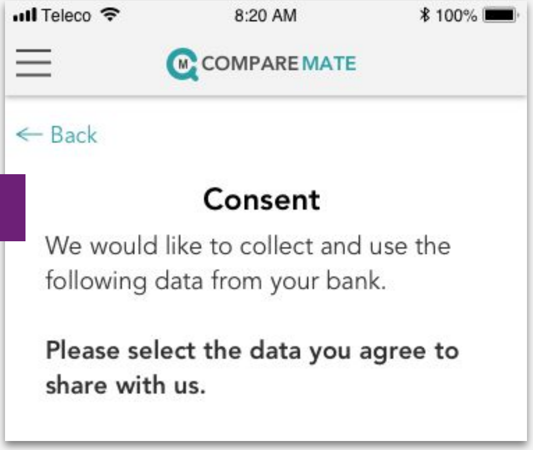
Where to review this arrangement

You can review this arrangement on your Data Share dashboard.

Do you consent to share this data with us?

Selecting 'I consent' won't give us access to your data. You will need to ask your bank to share this data with us first. That's the next step.

2.7.1



Teleco 8:20 AM 100%

COMPARE MATE

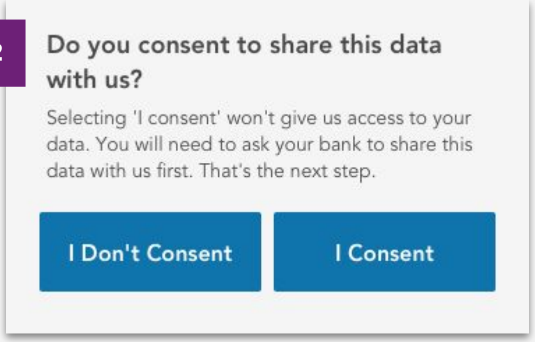
← Back

Consent

We would like to collect and use the following data from your bank.

Please select the data you agree to share with us.

2.7.2



Do you consent to share this data with us?

Selecting 'I consent' won't give us access to your data. You will need to ask your bank to share this data with us first. That's the next step.

Note: The components above are examples of how the following rules can be implemented.

Consent | Data request

Component 2.7: Active consent

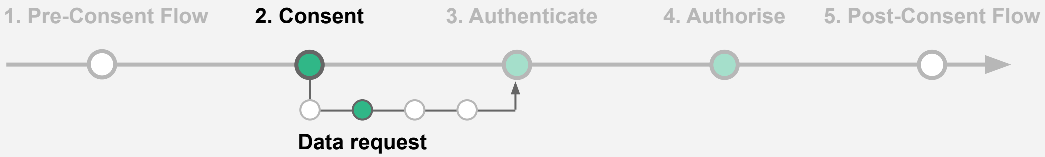
Guidelines

2.7.1 **2.7.2** **Mandatory**

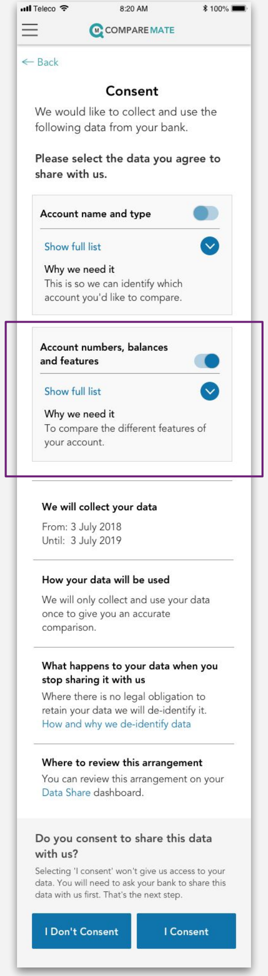
The data recipient **must** ask for the consumer's consent to collect and the selected or specified data. Consent cannot be inferred or implied.

CDR Rule 4.10(3)(c), 4.16(3)(c),

CONSUMER
DATA
STANDARDS



Component 2.8: Data clusters


Teleco 8:20 AM 100%

COMPAREMATE

← Back

Consent

We would like to collect and use the following data from your bank.

Please select the data you agree to share with us.

Account name and type

Show full list

Why we need it
This is so we can identify which account you'd like to compare.

Account numbers, balances and features

Show full list

Why we need it
To compare the different features of your account.

We will collect your data

From: 3 July 2018
Until: 3 July 2019

How your data will be used

We will only collect and use your data once to give you an accurate comparison.

What happens to your data when you stop sharing it with us

Where there is no legal obligation to retain your data we will de-identify it.
How and why we de-identify data

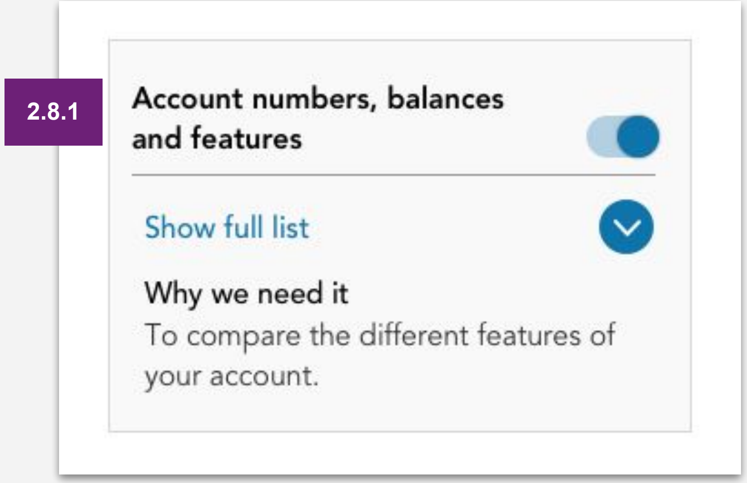
Where to review this arrangement

You can review this arrangement on your Data Share dashboard.

Do you consent to share this data with us?

Selecting 'I consent' won't give us access to your data. You will need to ask your bank to share this data with us first. That's the next step.

2.8.1


Account numbers, balances and features

Show full list

Why we need it
To compare the different features of your account.

Note: The component above is an example of how the following rules can be implemented.

Consent | Data request

Component 2.8: Data clusters

Guidelines

2.8.1 Mandatory

The data recipient **must** identify the types of CDR data for which consent is sought.

CDR Rule 4.10(3)(a)

2.8.1 Mandatory

Data language standards **must** be used for data clusters.

CDR Rule 8.11 | Data Language Standards

2.8.1 Mandatory

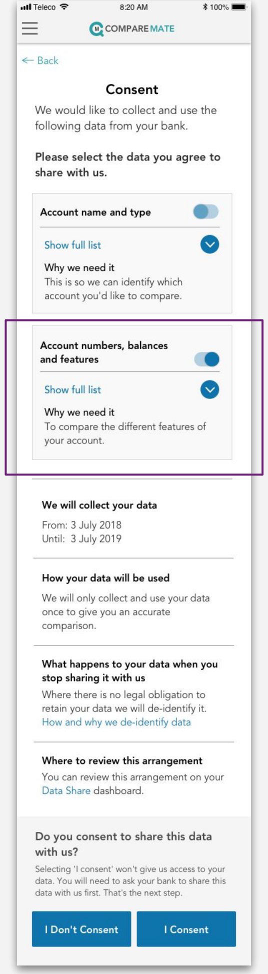
The data recipient **must** allow the consumer to actively select or actively specify the types of data and the uses they consent to.

If data is being requested for multiple uses, the consumer **must** be able to specify which uses they consent to.

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 4.10(3), 4.16(3) | *CX Research 2, 3, 4, 5, 6*

Component 2.8: Data clusters (continued)



Teleco 8:20 AM 100%

COMPAREMATE

← Back

Consent

We would like to collect and use the following data from your bank.

Please select the data you agree to share with us.

Account name and type

Show full list

Why we need it
This is so we can identify which account you'd like to compare.

Account numbers, balances and features

Show full list

Why we need it
To compare the different features of your account.

We will collect your data
From: 3 July 2018
Until: 3 July 2019

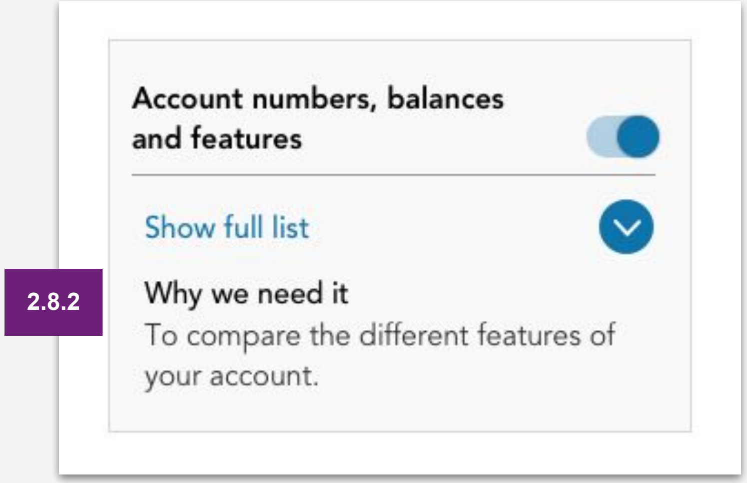
How your data will be used
We will only collect and use your data once to give you an accurate comparison.

What happens to your data when you stop sharing it with us
Where there is no legal obligation to retain your data we will de-identify it.
How and why we de-identify data

Where to review this arrangement
You can review this arrangement on your Data Share dashboard.

Do you consent to share this data with us?
Selecting 'I consent' won't give us access to your data. You will need to ask your bank to share this data with us first. That's the next step.

2.8.2



Account numbers, balances and features

Show full list

Why we need it
To compare the different features of your account.

Note: The component above is an example of how the following rules can be implemented.

> *"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

Component 2.8: Data clusters (continued)

Guidelines

2.8.2 Mandatory

The data recipient **must** state the purpose of the request in unambiguous terms. The request **must** be specific as to purpose and **must** directly refer to the specified data.

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

The data recipient **must** allow the consumer to actively select or actively specify those specific uses they are consenting to.

CDR Rule 4.10(3), 4.16(3) | *CX Research 1, 2, 3*

2.8.2 Mandatory

The data recipient **must** comply with the data minimisation principle when requesting, collecting, and using CDR data.

CDR Rules 1.7 / 4.16(4) | *CX Research 1, 2, 3*

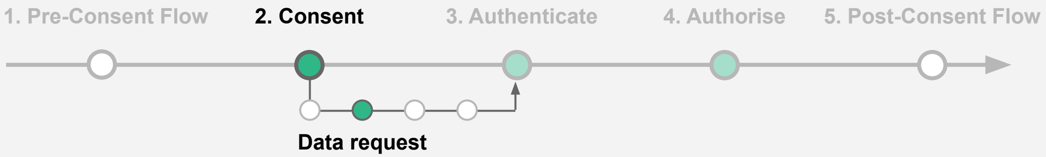
2.8.2 Mandatory

The data recipient **must** allow the consumer to actively select or actively specify the types of data and the uses they consent to.

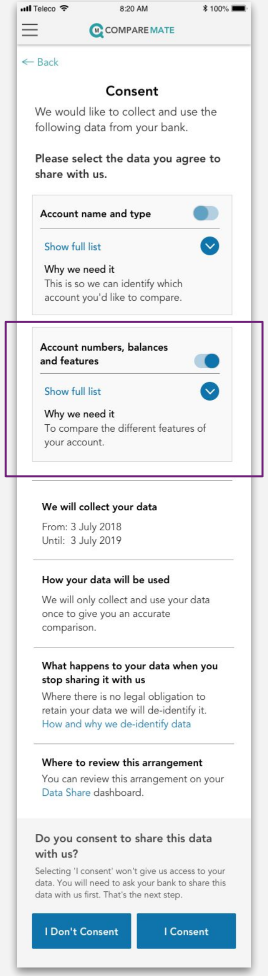
If data is being requested for multiple uses, the consumer **must** be able to specify which uses they consent to. This **may** involve using various consent capture design patterns that allow consumers to opt-in such as checkboxes, toggles, and binary yes/no choices.

CDR Rules 4.10(3), 4.16(3)

CONSUMER
DATA
STANDARDS



Component 2.9: Permission language



Consent

We would like to collect and use the following data from your bank.

Please select the data you agree to share with us.

Account name and type

Show full list

Why we need it

This is so we can identify which account you'd like to compare.

Account numbers, balances and features

Show full list

Why we need it

To compare the different features of your account.

We will collect your data

From: 3 July 2018
Until: 3 July 2019

How your data will be used

We will only collect and use your data once to give you an accurate comparison.

What happens to your data when you stop sharing it with us

Where there is no legal obligation to retain your data we will de-identify it. How and why we de-identify data

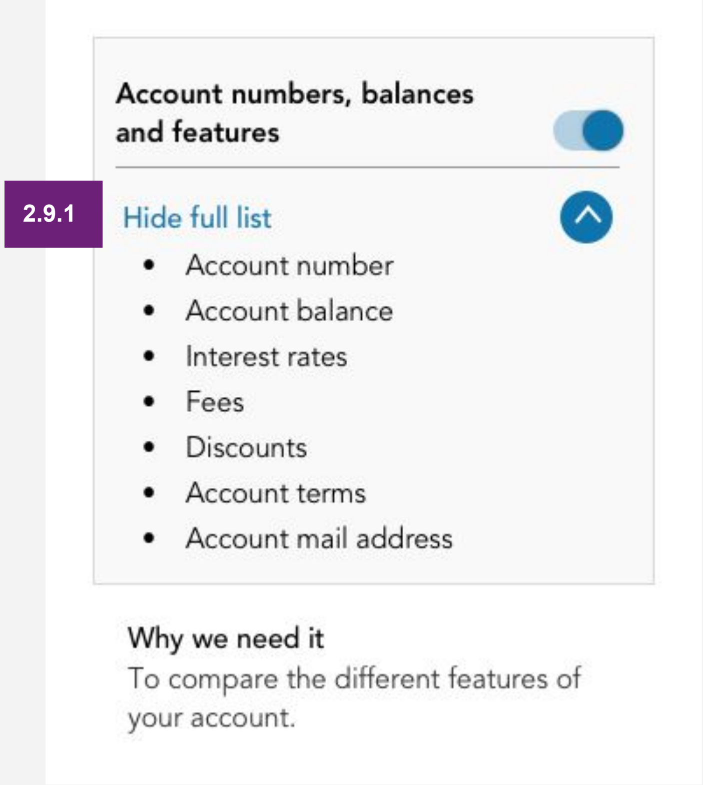
Where to review this arrangement

You can review this arrangement on your Data Share dashboard.

Do you consent to share this data with us?

Selecting 'I consent' won't give us access to your data. You will need to ask your bank to share this data with us first. That's the next step.

2.9.1



Account numbers, balances and features

Hide full list

- Account number
- Account balance
- Interest rates
- Fees
- Discounts
- Account terms
- Account mail address

Why we need it

To compare the different features of your account.

Note: The components above is an example of how the following rules can be implemented.

Consent | Data request

Component 2.9: Permission language

Guidelines

2.9.1 Mandatory

The data recipient **must** identify the types of CDR data for which consent is sought.

CDR Rules 4.10(3)(a)

2.9.1 Mandatory

The data recipient **must** comply with the data minimisation principle when requesting, collecting, and using CDR data.

CDR Rules 1.7 / 4.16(4) | CX Research 1, 2, 3

2.9.1 Mandatory

Data language standards **must** be used for permissions.

CDR Rule 8.11 | Data Language Standards

2.9.1 Mandatory

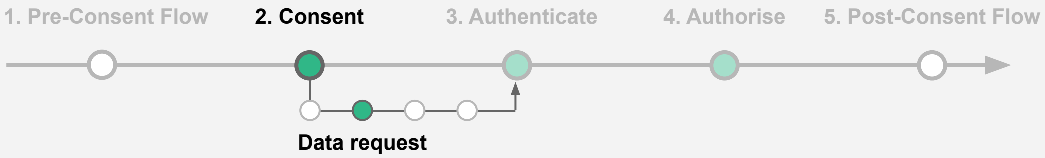
Data recipients **must** seek to make the consent process as easy to understand as is practicable. This **may** involve using progressive disclosure design patterns such as an accordion (shown in example).

4.16(2)(a) | CX Research 8, 19

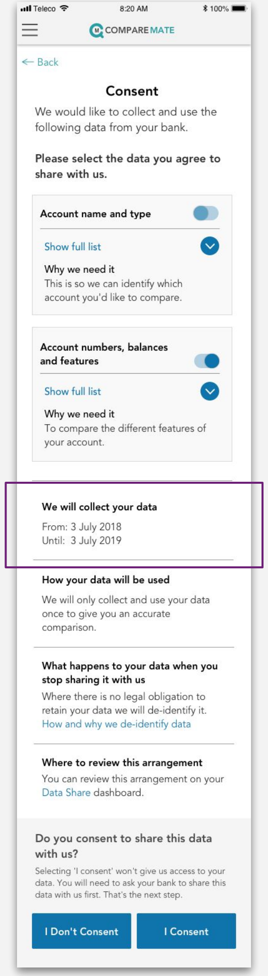
Recommended

The data recipient **should** include in-line help (e.g. questions marks) to provide a more detailed but plain-English (grade 7 readability) descriptions of what is included in the data cluster, including permissions.

Nielsen and Molich's 10 User Interface Design Heuristics: Help and documentation; Match between system and the real world



Component 2.10: Duration



Teleco 8:20 AM 100%

COMPARE MATE

← Back

Consent

We would like to collect and use the following data from your bank.

Please select the data you agree to share with us.

Account name and type

Show full list

Why we need it
This is so we can identify which account you'd like to compare.

Account numbers, balances and features

Show full list

Why we need it
To compare the different features of your account.

We will collect your data

From: 3 July 2018
Until: 3 July 2019

How your data will be used

We will only collect and use your data once to give you an accurate comparison.

What happens to your data when you stop sharing it with us

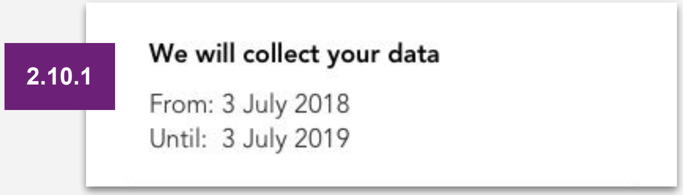
Where there is no legal obligation to retain your data we will de-identify it.
How and why we de-identify data

Where to review this arrangement

You can review this arrangement on your Data Share dashboard.

Do you consent to share this data with us?

Selecting 'I consent' won't give us access to your data. You will need to ask your bank to share this data with us first. That's the next step.

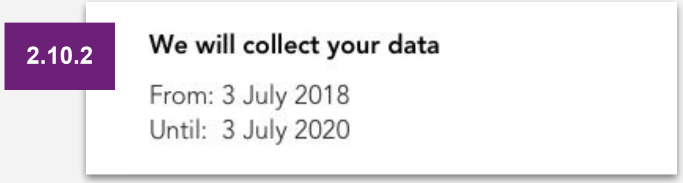


2.10.1

We will collect your data

From: 3 July 2018
Until: 3 July 2019

Single collection aka 'once-off' [Rule 4.10(4)(b)(i)]



2.10.2

We will collect your data

From: 3 July 2018
Until: 3 July 2020

On-going data sharing [Rule 4.10(4)(b)(ii)]

Note: The components above are examples of how the following rules and the recommendation can be implemented.

Consent | Data request

Component 2.10: Duration

Guidelines

2.10.1 **2.10.2** **Mandatory**

The data recipient **must** state the sharing duration, including how far back in time data will be collected.

The data recipient **must** 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 on-going).

The data recipient **should** allow the consumer to specify the sharing duration, including how far back in time data will be accessed.

The data recipient **should** present the range of collection and use in a way that is easy to understand and appropriate for the use case.

CDR Rule 4.10(4)(b), (c) and (d), 4.16(6)(b), 4.12(1)(c), 4.18 | CX Research 4, 5, 6

2.10.1 **2.10.2** **Mandatory**

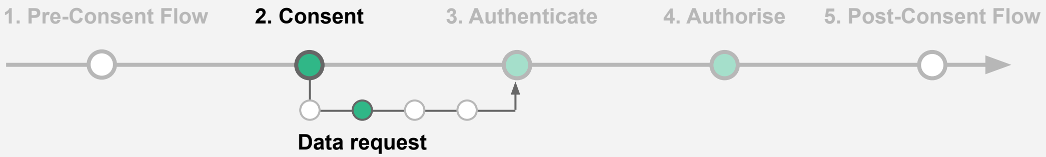
The data recipient **must** apply the data minimisation principle to the collection of historical data as well as the sharing duration into the future.

CDR Rule 1.7 | CX Research 3, 4, 5, 6

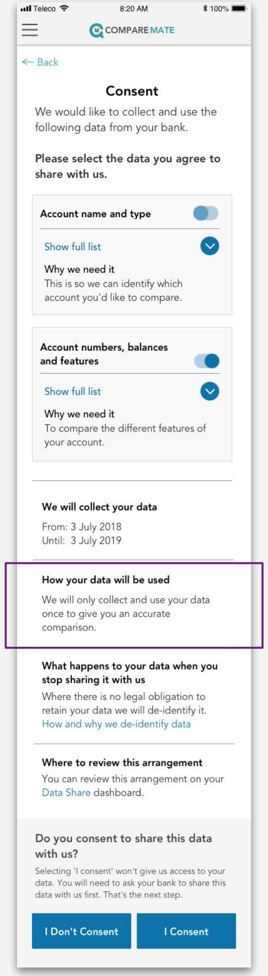
Recommended

The data recipient **should** state why this historical range is required.

CX Research 3, 4, 5, 6



Component 2.11: Data use



Teleco 8:20 AM 100%

COMPAREMATE

← Back

Consent

We would like to collect and use the following data from your bank.

Please select the data you agree to share with us.

Account name and type

Show full list

Why we need it

This is so we can identify which account you'd like to compare.

Account numbers, balances and features

Show full list

Why we need it

To compare the different features of your account.

We will collect your data

From: 3 July 2018
Until: 3 July 2019

How your data will be used

We will only collect and use your data once to give you an accurate comparison.

What happens to your data when you stop sharing it with us

Where there is no legal obligation to retain your data we will de-identify it.
How and why we de-identify data

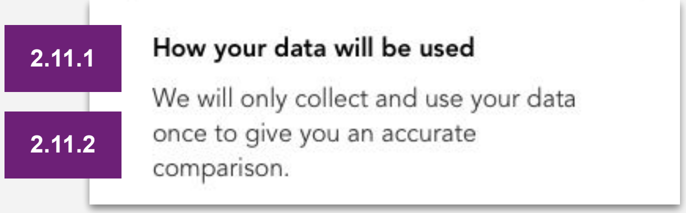
Where to review this arrangement

You can review this arrangement on your Data Share dashboard.

Do you consent to share this data with us?

Selecting 'I consent' won't give us access to your data. You will need to ask your bank to share this data with us first. That's the next step.

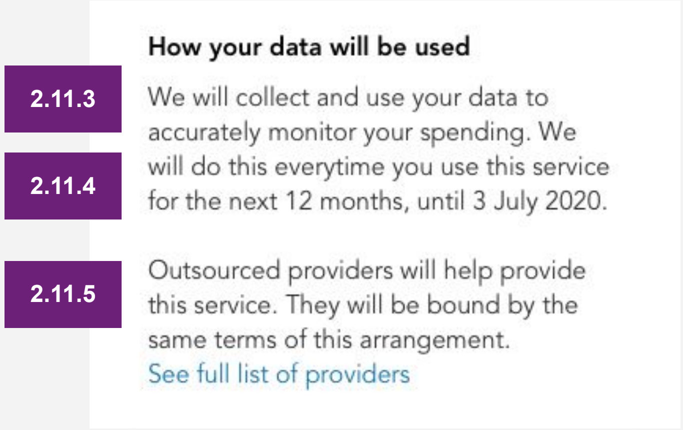
I Don't Consent | I Consent



How your data will be used

We will only collect and use your data once to give you an accurate comparison.

Single collection aka 'once-off' [Rule 4.10(4)(b)(i)]



How your data will be used

We will collect and use your data to accurately monitor your spending. We will do this everytime you use this service for the next 12 months, until 3 July 2020.

Outsourced providers will help provide this service. They will be bound by the same terms of this arrangement.
See full list of providers

On-going data sharing [Rule 4.10(4)(b)(ii)]
Outsourced provider [Rule 4.16(6)(c)]

Note: The components above are examples of how the following rules can be implemented.

Consent | Data request

Component 2.11: Data use

Guidelines

2.11.1 2.11.3 Mandatory

The data recipient **must** outline how often data is expected to be collected over that period.

The data recipient **must** state the purpose of the request. This may encompass the use case, the product or service, and the specific purpose associated with the specified data.

CDR Rule 4.10(4)(b) and (c)(ii), 4.16(3)

2.11.2 2.11.4 Mandatory

The data recipient **must** disclose all uses of CDR data.

The data recipient **must** identify the specific uses of the CDR data from which the consumer will be able to select or specify. The data recipient **must** allow the consumer to actively select or actively specify those specific uses they are consenting to.

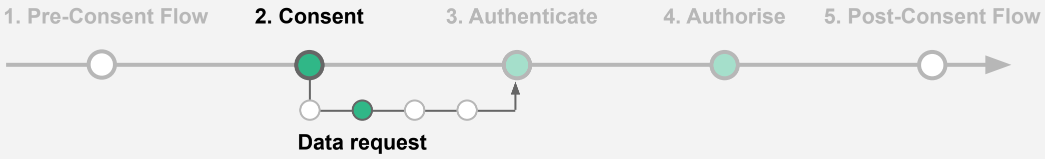
This **may** involve using various consent capture design patterns that allow consumers to opt-in such as checkboxes, toggles, and binary yes/no choices.

CDR Rules 1.7, 4.16(3)

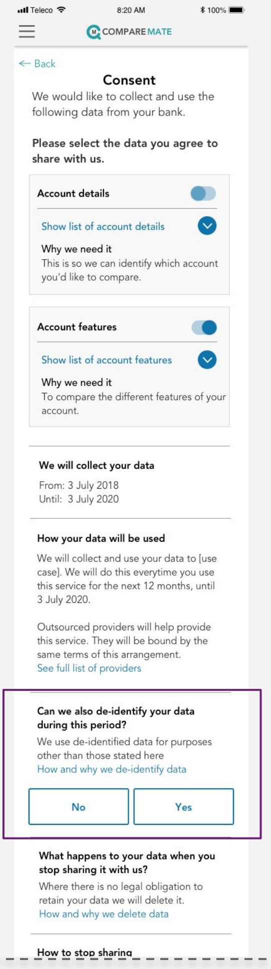
2.11.5 Mandatory

The data recipient **must** inform the consumer if data may be disclosed to an outsourced service provider and provide information on how to obtain further details about possible disclosures to outsourced service providers.

CDR Rules 4.16(6)(c), 7.2(2)



Component 2.12: De-identification within duration



Consent

We would like to collect and use the following data from your bank.

Please select the data you agree to share with us.

Account details

Show list of account details

Why we need it

This is so we can identify which account you'd like to compare.

Account features

Show list of account features

Why we need it

To compare the different features of your account.

We will collect your data

From: 3 July 2018
Until: 3 July 2020

How your data will be used

We will collect and use your data to [use case]. We will do this everytime you use this service for the next 12 months, until 3 July 2020.

Outsourced providers will help provide this service. They will be bound by the same terms of this arrangement.
See full list of providers

Can we also de-identify your data during this period?

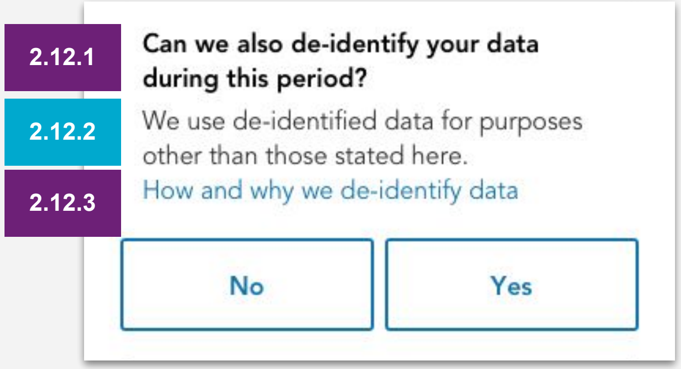
We use de-identified data for purposes other than those stated here
How and why we de-identify data

No | Yes

What happens to your data when you stop sharing it with us?

Where there is no legal obligation to retain your data we will delete it.
How and why we delete data

How to stop sharing



Can we also de-identify your data during this period?

We use de-identified data for purposes other than those stated here.
How and why we de-identify data

On-going data sharing [Rule 4.10(4)(b)(ii)]

Note: The component above is an example of how the following rules and the recommendation can be implemented.

Consent | Data request

Component 2.12: De-identification within duration

Guidelines

2.12.1 Mandatory

Consumers **must** consent to all uses of CDR data.

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

The data recipient **must** allow the consumer to actively select or actively specify those specific uses they are consenting to.

The data recipient **must not** use CDR data in ways that the consumer did not consent to. If the data recipient intends to de-identify CDR data during the sharing period they **must** receive consumer consent.

CDR Rule 4.1, 4.16(3) | CX Research 1

2.12.2 Recommended

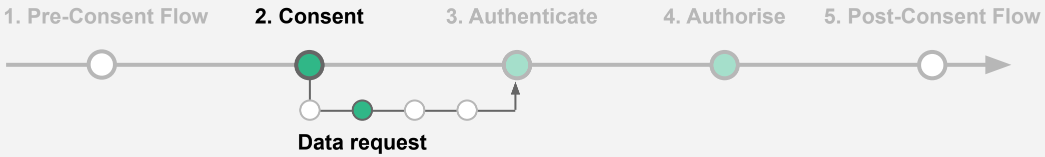
The data recipient **should** state the intended purpose(s) of de-identifying CDR data when requesting this consent.

CX Research 1

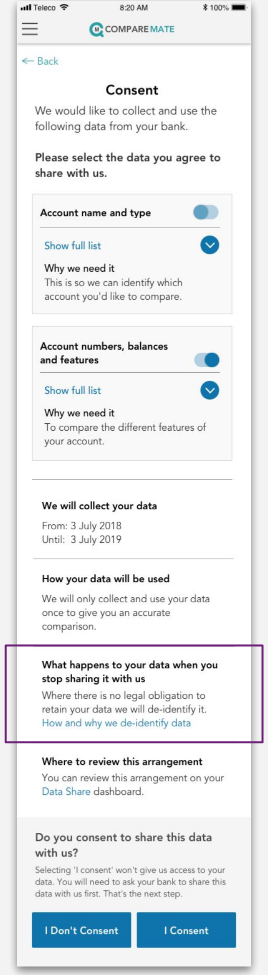
2.12.3 Mandatory

If the data recipient intends to de-identify CDR data during the sharing period, they **must** provide further information on what de-identification is, how data will be de-identified, and genuine examples of how de-identified data may be put to use. This **may** be presented as in-line help, a link to further information, or additional on-screen clarifiers.

CX Research 1, 18, 34



Component 2.13: Handling of redundant data



Consent

We would like to collect and use the following data from your bank.

Please select the data you agree to share with us.

Account name and type

Show full list

Why we need it
This is so we can identify which account you'd like to compare.

Account numbers, balances and features

Show full list

Why we need it
To compare the different features of your account.

We will collect your data
From: 3 July 2018
Until: 3 July 2019

How your data will be used
We will only collect and use your data once to give you an accurate comparison.

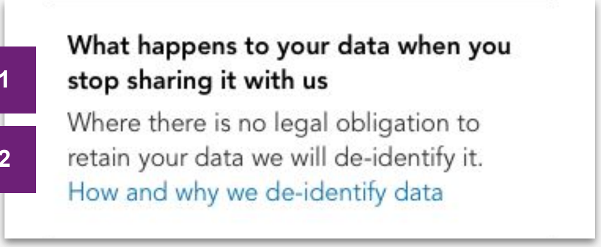
What happens to your data when you stop sharing it with us
Where there is no legal obligation to retain your data we will de-identify it.
How and why we de-identify data

Where to review this arrangement
You can review this arrangement on your Data Share dashboard.

Do you consent to share this data with us?
Selecting 'I consent' won't give us access to your data. You will need to ask your bank to share this data with us first. That's the next step.

2.13.1

2.13.2



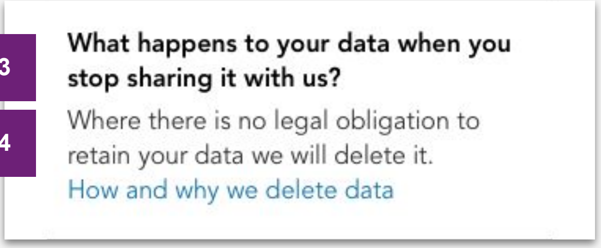
What happens to your data when you stop sharing it with us

Where there is no legal obligation to retain your data we will de-identify it.
How and why we de-identify data

When data is de-identified after consent expires

2.13.3

2.13.4



What happens to your data when you stop sharing it with us?

Where there is no legal obligation to retain your data we will delete it.
How and why we delete data

When data is deleted after consent expires

Note: The components above are examples of how the following rules can be implemented.

Consent | Data request

Component 2.13: Handling of redundant data

Guidelines

2.13.1 **2.13.3** **Mandatory**

If the data recipient intends to de-identify CDR data after the sharing period, they **must** provide further information on what de-identification is, how data will be de-identified, and genuine examples of how de-identified data may be put to use. This **may** be presented as in-line help, a link to further information, or additional on-screen clarifiers.

CX Research 18, 34

2.13.2 **2.13.4** **Mandatory**

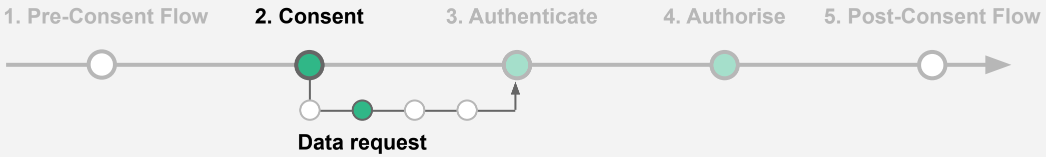
The data recipient **must** state the specific method they will attempt to use to handle redundant CDR data.

Example 1: if the data recipient intends to de-identify some or all of the CDR data, they **must** clearly state this intention. They **may** specify the types of data they intend to delete and the types of data they intend to de-identify.

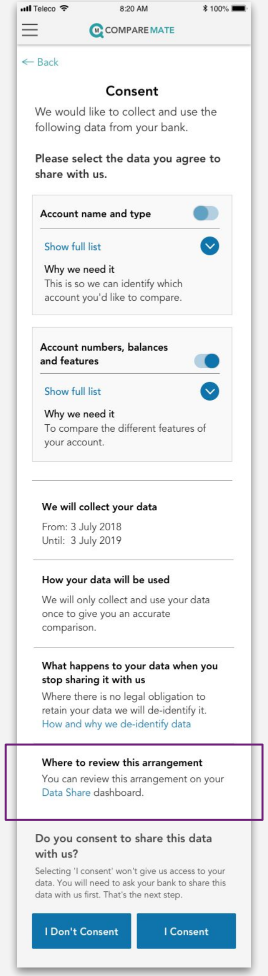
Example 2: If the data recipient intends to delete the CDR data, they **must** clearly state this intention.

Most consumer research participants expected data to be completely destroyed once sharing had stopped. De-identification made participants uncomfortable, led to distrust, and reduced willingness to share.

CX Research 18



Component 2.14: Review and revocation



Consent

We would like to collect and use the following data from your bank.

Please select the data you agree to share with us.

Account name and type

Show full list

Why we need it
This is so we can identify which account you'd like to compare.

Account numbers, balances and features

Show full list

Why we need it
To compare the different features of your account.

We will collect your data

From: 3 July 2018
Until: 3 July 2019

How your data will be used

We will only collect and use your data once to give you an accurate comparison.

What happens to your data when you stop sharing it with us

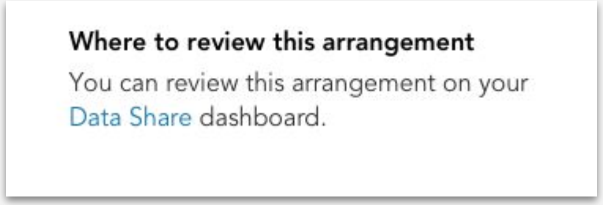
Where there is no legal obligation to retain your data we will de-identify it.
How and why we de-identify data

Where to review this arrangement

You can review this arrangement on your Data Share dashboard.

Do you consent to share this data with us?

Selecting 'I consent' won't give us access to your data. You will need to ask your bank to share this data with us first. That's the next step.



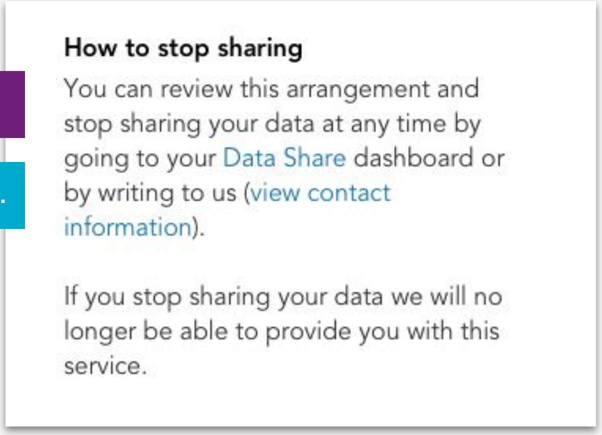
Where to review this arrangement

You can review this arrangement on your Data Share dashboard.

Single collection aka 'once-off' [Rule 4.10(4)(b)(i)]

2.14.1

2.14.2.



How to stop sharing

You can review this arrangement and stop sharing your data at any time by going to your Data Share dashboard or by writing to us (view contact information).

If you stop sharing your data we will no longer be able to provide you with this service.

On-going data sharing [Rule 4.10(4)(b)(ii)]

Note: The components above are examples of how the following rules and the recommendation can be implemented.

Consent | Data request

Component 2.14: Review and revocation

Guidelines

2.14.1 Mandatory

The data recipient **must** state that consent can be withdrawn at any time and provide instructions for withdrawing consent.

The data recipient **must** provide a clear and consistent location for the consent management dashboard via which consent can be withdrawn.

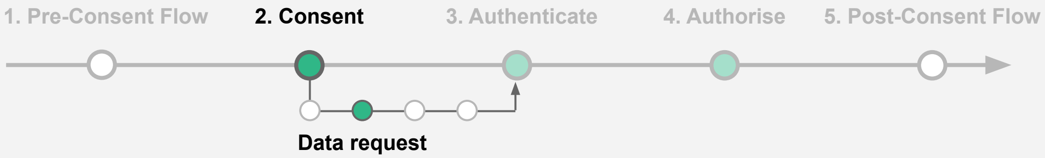
Information **should** be clearly displayed and the data recipient **should** state the future consequences of revocation. For example: The data recipient will no longer be able to provide this service and/or a tailored plan.

CDR Rules 4.10(4)(e) and (f), 4.16(6)(d) and (e), 4.10(11)(1), 4.17 | CX Research 7, 30, 32, 33

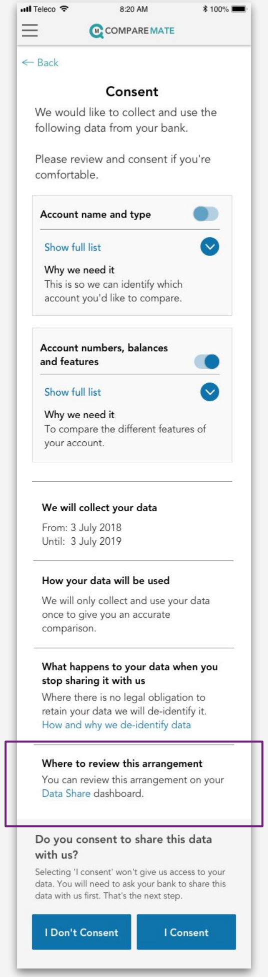
2.14.2 Recommended

The data recipient **should** also allow the consumer to initiate revocation via existing and preferred channels. These channels **should** be used as contact points to then guide consumers towards the appropriate revocation pathway (i.e. revocation via dashboard).

CX Research 15, 31, 32



Component 2.14: Review and revocation (continued)



Teleco 8:20 AM 100%

COMPARE MATE

← Back

Consent

We would like to collect and use the following data from your bank.

Please review and consent if you're comfortable.

Account name and type

Show full list

Why we need it
This is so we can identify which account you'd like to compare.

Account numbers, balances and features

Show full list

Why we need it
To compare the different features of your account.

We will collect your data

From: 3 July 2018
Until: 3 July 2019

How your data will be used

We will only collect and use your data once to give you an accurate comparison.

What happens to your data when you stop sharing it with us

Where there is no legal obligation to retain your data we will de-identify it.
How and why we de-identify data

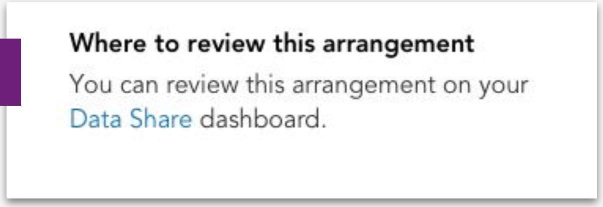
Where to review this arrangement

You can review this arrangement on your Data Share dashboard.

Do you consent to share this data with us?

Selecting 'I consent' won't give us access to your data. You will need to ask your bank to share this data with us first. That's the next step.

2.14.2

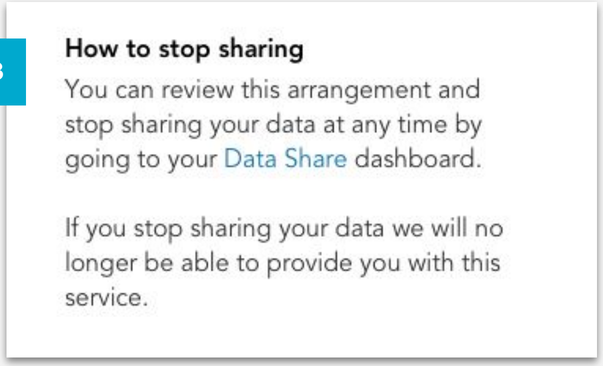


Where to review this arrangement

You can review this arrangement on your Data Share dashboard.

Single collection aka 'once-off' [Rule 4.10(4)(b)(i)]

2.14.3



How to stop sharing

You can review this arrangement and stop sharing your data at any time by going to your Data Share dashboard.

If you stop sharing your data we will no longer be able to provide you with this service.

On-going data sharing [Rule 4.10(4)(b)(ii)]

Note: The components above are examples of how the following rule and recommendation can be implemented.

Consent | Data request

Component 2.14: Review and revocation (continued)

Guidelines

2.14.2 Mandatory

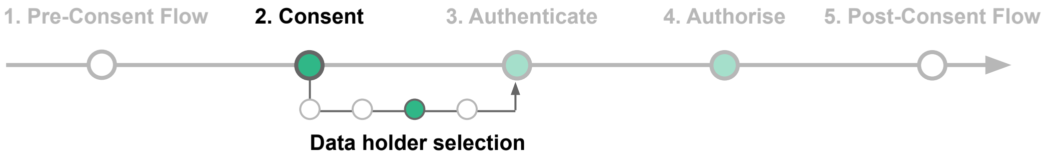
The data recipient **must** state that sharing arrangements for single collection requests can be reviewed via consent management dashboards.

CX Research 20

2.14.3 Recommended

The data recipient **should** use the phrase 'Stop Sharing' to refer to how a consumer can withdraw or revoke authorisation.

CX Research 29



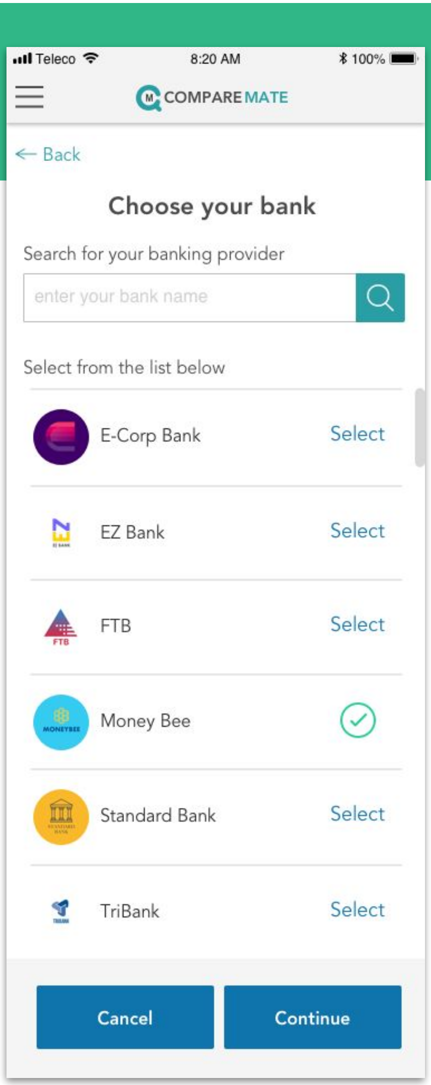
Consent | Data holder selection

Component 2.15 - 2.16

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. There are broader implications to be considered associated with the selection of multiple data holders. This includes the increased likelihood of a consumer completing part of a consent flow related to one data holder and then returning at a later date to share data from additional data holders without reviewing the terms of the sharing arrangement. This method of reducing friction would compromise the quality of consent.



Choose your bank

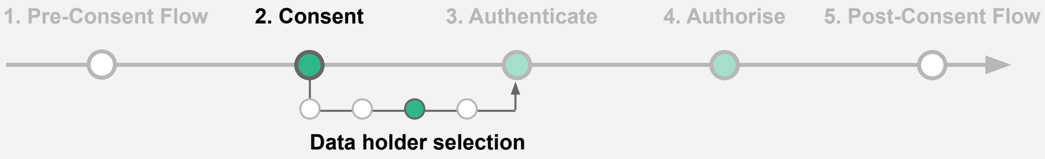
Search for your banking provider

enter your bank name

Select from the list below

E-Corp Bank	Select
EZ Bank	Select
FTB	Select
Money Bee	✓
Standard Bank	Select
TriBank	Select

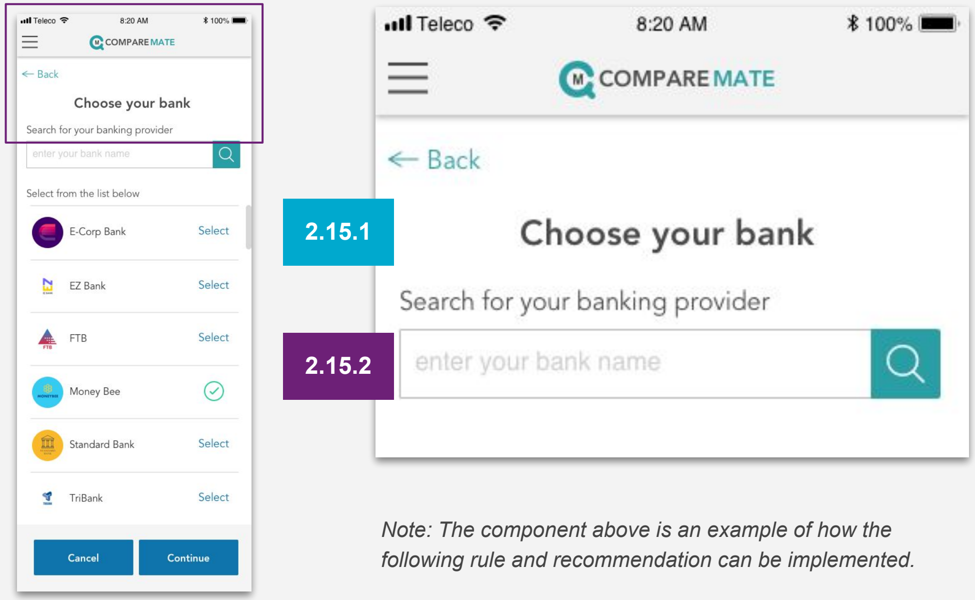
Example wireframe 2.5



1. Pre-Consent Flow
2. Consent
3. Authenticate
4. Authorise
5. Post-Consent Flow

Data holder selection

Component 2.15: Data holder selection 1



Teleco 8:20 AM 100%

COMPAREMATE

← Back

Choose your bank

Search for your banking provider

enter your bank name

Select from the list below

E-Corp Bank	Select
EZ Bank	Select
FTB	Select
Money Bee	✓
Standard Bank	Select
TriBank	Select

Cancel Continue

2.15.1

2.15.2

Note: The component above is an example of how the following rule and recommendation can be implemented.

Consent | Data holder selection

Component 2.15: Data holder selection 1

Guidelines

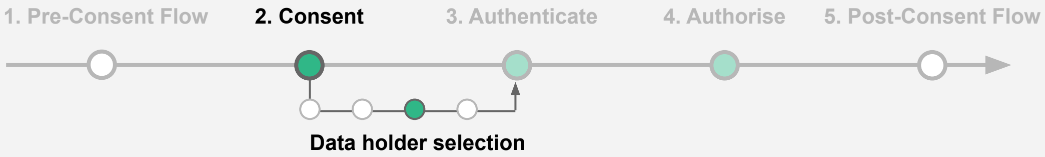
2.15.1 Recommended

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

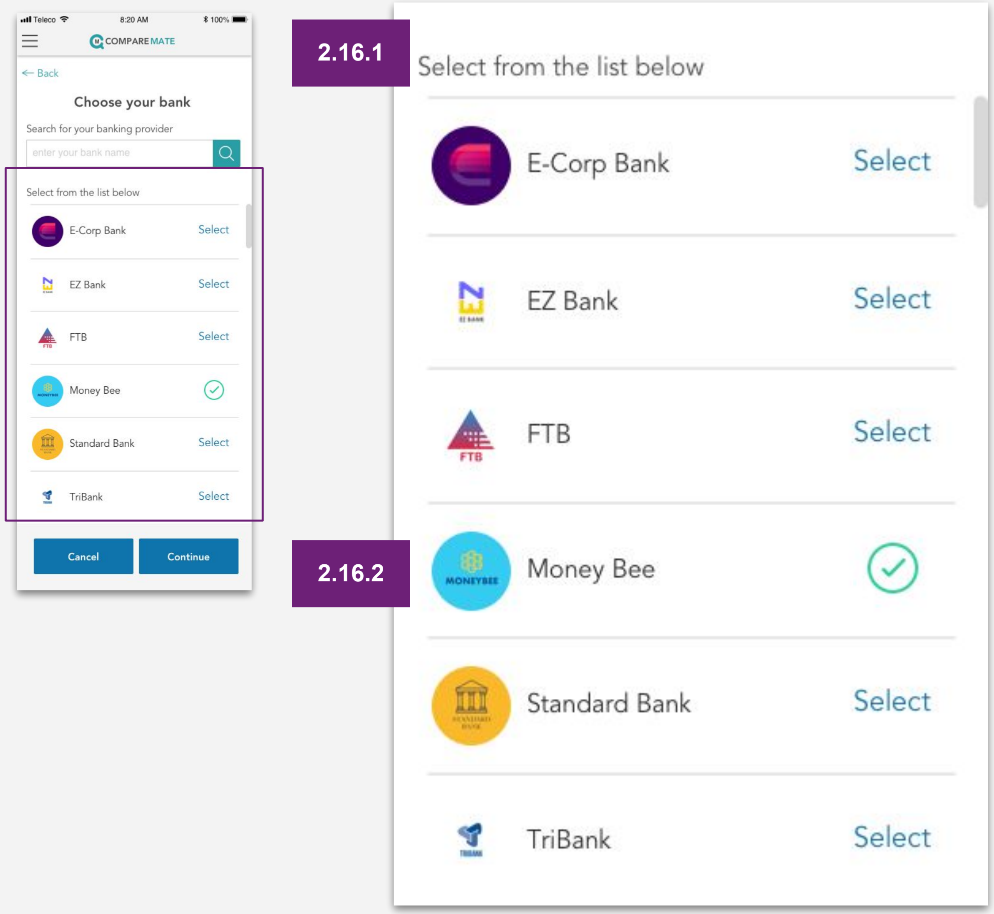
2.15.2 Mandatory

Data recipients **must** make data holder list searchable.

Nielsen and Molich's 10 User Interface Design Heuristics: Flexibility and efficiency of use



Component 2.16: Data holder selection 2



← Back

Choose your bank

Search for your banking provider

enter your bank name

Select from the list below

E-Corp Bank	Select
EZ Bank	Select
FTB	Select
Money Bee	✓
Standard Bank	Select
TriBank	Select

Cancel | Continue

Note: The component above is an example of how the following rules can be implemented.

Consent | Data holder selection

Component 2.16: Data holder selection 2

Guidelines

2.16.1 **Mandatory**

Data recipients **must** list data holders in alphabetical order.

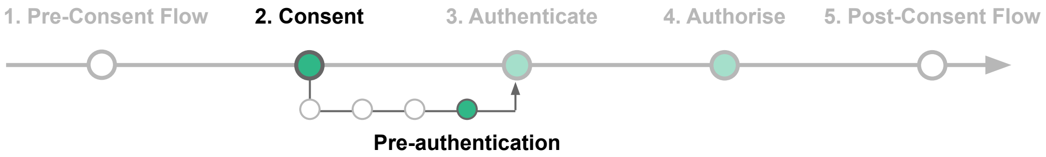
Data recipients **must** allow consumers to scroll through and select data holders from a list.

Nielsen and Molich's 10 User Interface Design Heuristics: Flexibility and efficiency of use

2.16.2 **Mandatory**

Data recipients **must not** allow more than one data holder to be selected at a time. The data recipient **must** present data requests in direct connection to each time a data holder is selected to avoid compromising the quality of consent.

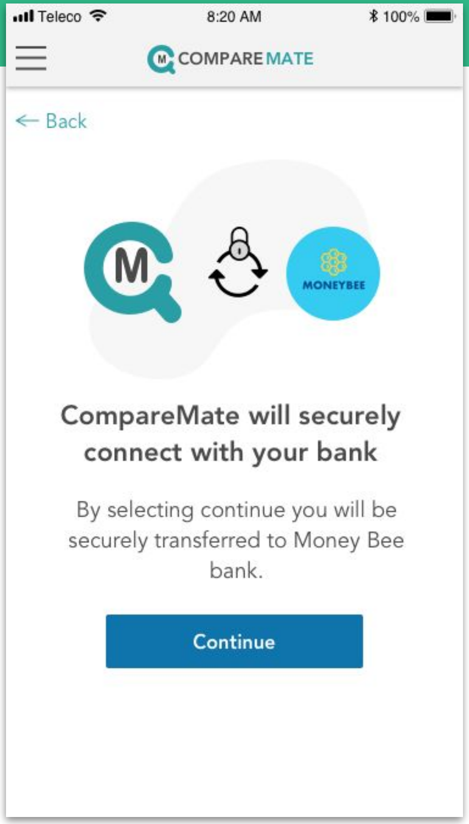
Example: The data recipient **must not** allow the consumer to select several data holders at once, complete authorisation for one, and then return to the session at some point in the future to connect more data holders without seeing the data request screens again.



Consent | Pre-authentication

Component 2.17

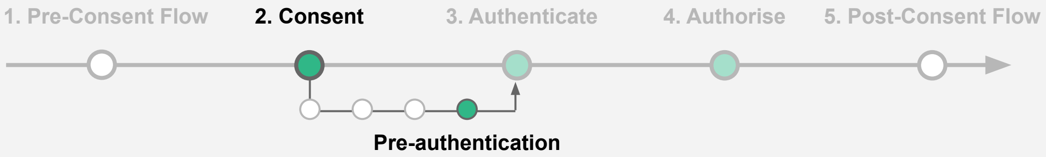
This section provides examples illustrating how the guidelines may be implemented, in particular focusing on how a consumer is redirected from the data recipient to securely connect with a data holder.



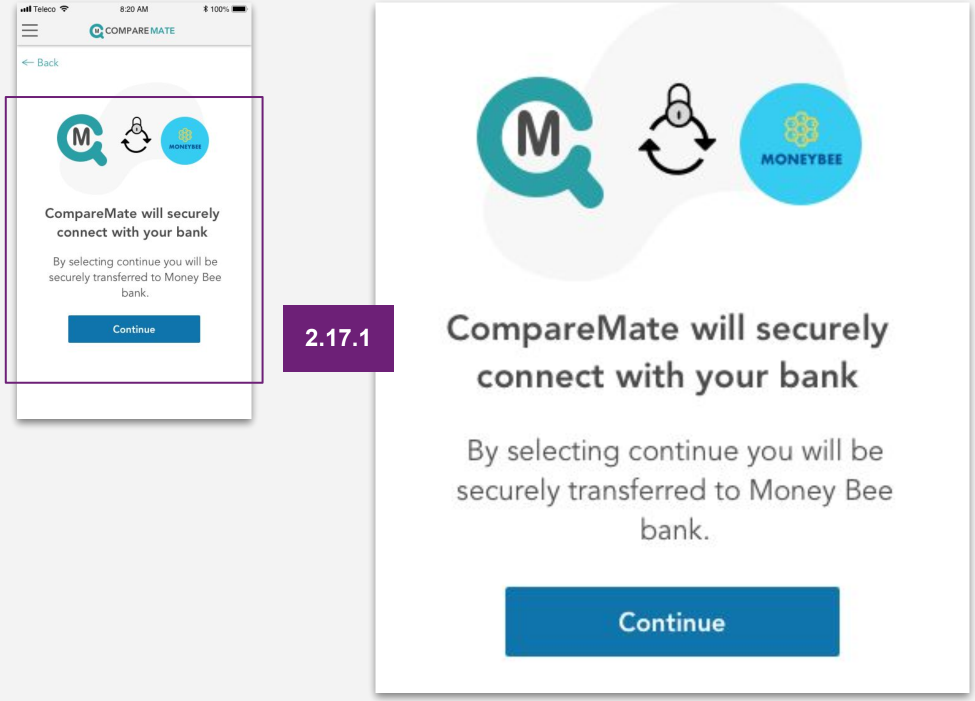
CompareMate will securely connect with your bank

By selecting continue you will be securely transferred to Money Bee bank.

Example wireframe



Component 2.17: Pre-authentication



CompareMate will securely connect with your bank

By selecting continue you will be securely transferred to Money Bee bank.

Continue

CompareMate will securely connect with your bank

By selecting continue you will be securely transferred to Money Bee bank.

Continue

Note: The component above is an example of how the following rule can be implemented.

Consent | Pre-authentication

Component 2.17: Pre-authentication

Guidelines

2.17.1 Mandatory

Data recipients **must** notify consumers of redirection prior to doing so.

CX Research 21, 22

3. AUTHENTICATE

The Authenticate stage for version 1 provides for the Redirect with One Time Password authentication method. In addition to the guidelines found in this document, the Authentication Flow section in the Security Profile will provide additional guidance and technical specifics on how to implement this decision.

Authentication flows must also reflect the information security controls set out in Part 2, 2.2 of the CDR Rules.

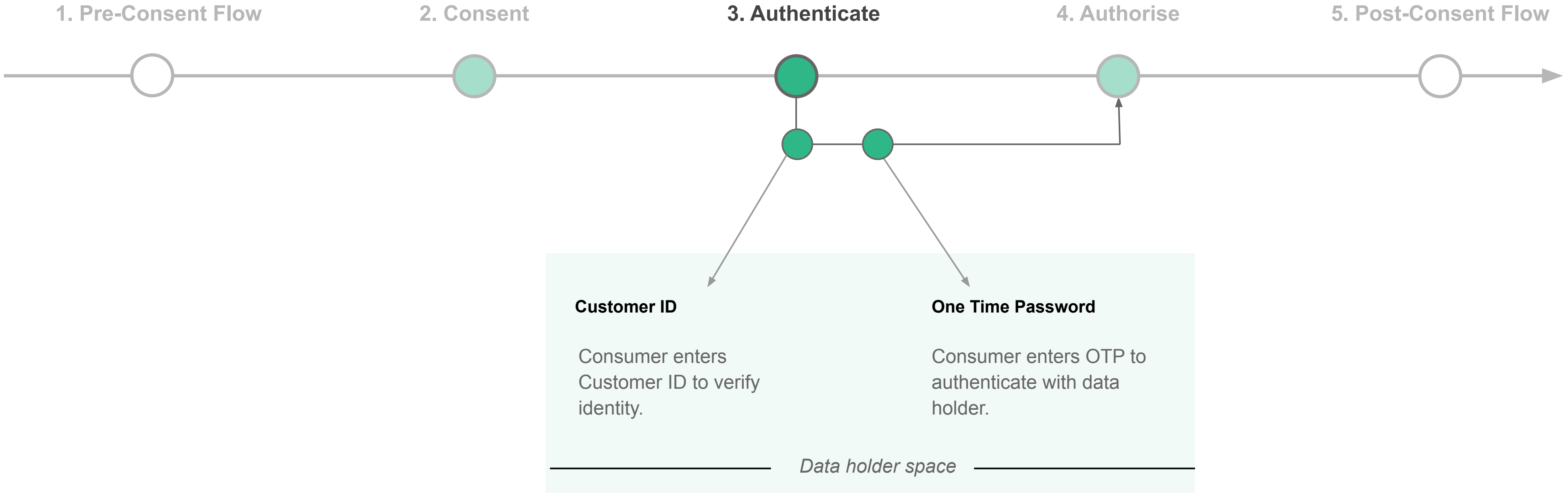
Using this model, the authentication stage is broken down into two steps: Customer ID; and One Time Password.

Customer ID

At this step, the consumer will be able to enter their Customer ID in order to verify their identity 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.



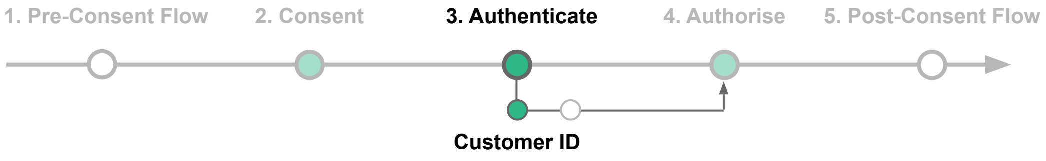
Customer ID

Consumer enters Customer ID to verify identity.

One Time Password

Consumer enters OTP to authenticate with data holder.

Data holder space



Authenticate | Customer ID

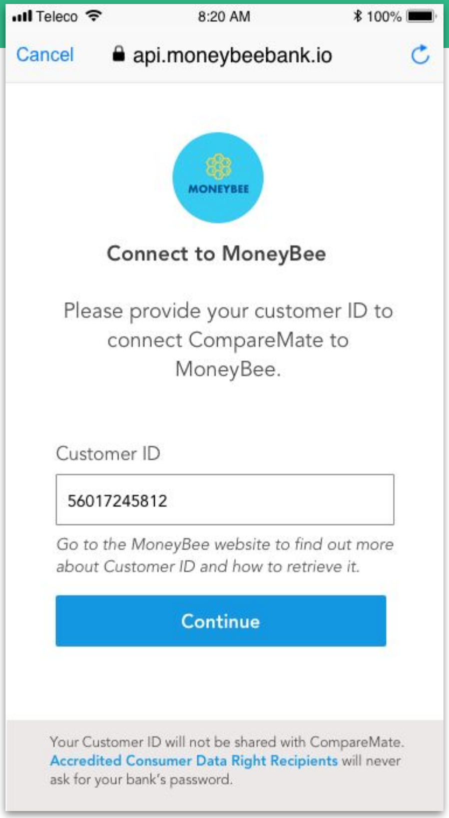
Component 3.1

This section provides examples illustrating how the guidelines may be implemented, in particular focusing on the part of the flow where the consumer inputs their 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.

"Log in to the bank inside the app and with verification code as well. Feels more secure"

CX Research 17



Connect to MoneyBee

Please provide your customer ID to connect CompareMate to MoneyBee.

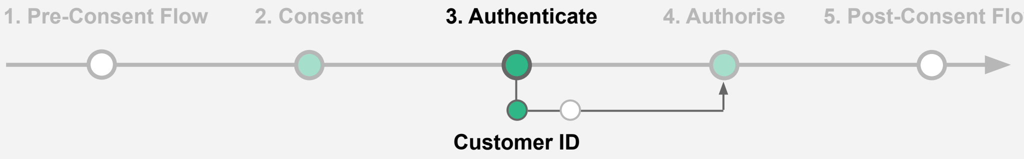
Customer ID

56017245812

Go to the MoneyBee website to find out more about Customer ID and how to retrieve it.

Your Customer ID will not be shared with CompareMate. Accredited Consumer Data Right Recipients will never ask for your bank's password.

Example wireframe 3.1



1. Pre-Consent Flow

2. Consent

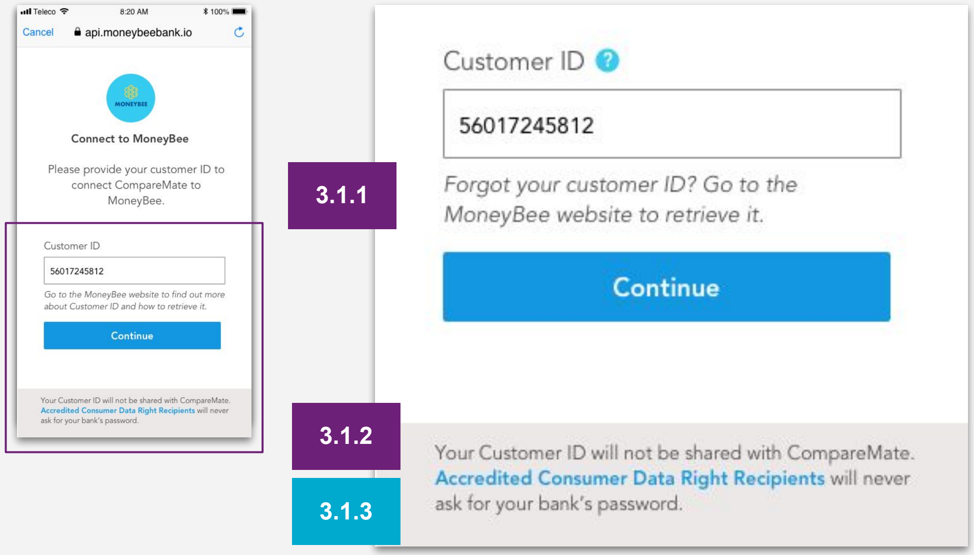
3. Authenticate

4. Authorise

5. Post-Consent Flow

Customer ID

Component 3.1: Customer ID



Teleco 8:20 AM 100%

Cancel api.moneybeebank.io

MONEYBEE

Connect to MoneyBee

Please provide your customer ID to connect CompareMate to MoneyBee.

Customer ID

56017245812

Go to the MoneyBee website to find out more about Customer ID and how to retrieve it.

Continue

Your Customer ID will not be shared with CompareMate. Accredited Consumer Data Right Recipients will never ask for your bank's password.

3.1.1

3.1.2

3.1.3

Customer ID

56017245812

Forgot your customer ID? Go to the MoneyBee website to retrieve it.

Continue

Your Customer ID will not be shared with CompareMate. Accredited Consumer Data Right Recipients will never ask for your bank's password.

Note: The component above is an example of how the following rules and the recommendation can be implemented.

Authenticate | Customer ID

Component 3.1: Customer ID

Guidelines

3.1.1 Mandatory

Data holders **must not** include a forgotten password link in redirect screens. The inclusion of links to reset password is considered to increase the likelihood of phishing attacks.

CX Research 21

3.1.2 Mandatory

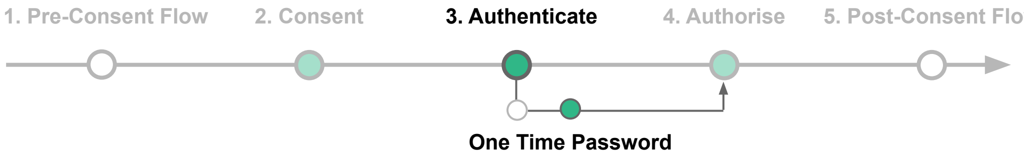
Data holders and data recipients **must** state in consumer-facing interactions and material that ADRs will never ask consumers for their banking password to access CDR data.

CX Research 21 | Security Standards

3.1.3 Recommended

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.

Nielsen and Molich's 10 User Interface Design Heuristics: Consistency and standards


1. Pre-Consent Flow

2. Consent

3. Authenticate

4. Authorise

5. Post-Consent Flow

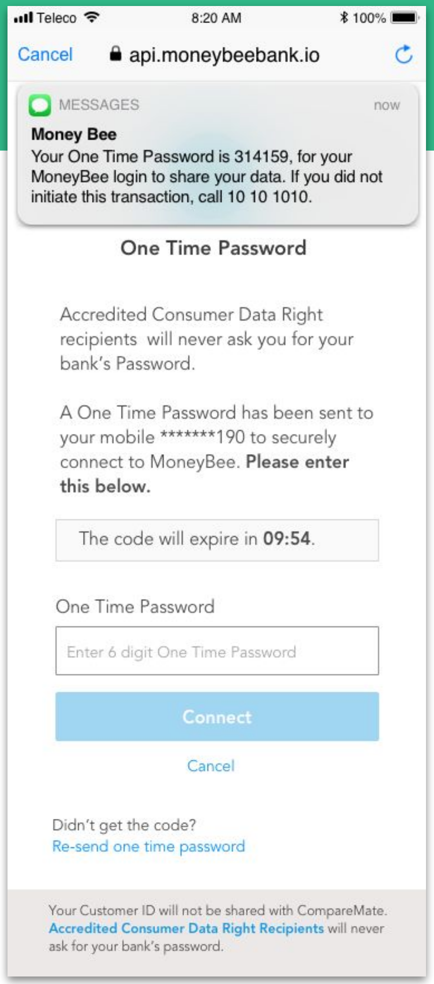
One Time Password

Authenticate | One Time Password

Component 3.2 - 3.3

This section provides examples illustrating how the guidelines may be implemented, in particular focusing on the ability of a consumer to use a One Time Password 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”.


Teleco 8:20 AM 100%

Cancel api.moneybeebank.io

MESSAGES now

Money Bee
Your One Time Password is 314159, for your MoneyBee login to share your data. If you did not initiate this transaction, call 10 10 1010.

One Time Password

Accredited Consumer Data Right recipients will never ask you for your bank’s Password.

A One Time Password has been sent to your mobile *******190 to securely connect to MoneyBee. **Please enter this below.**

The code will expire in **09:54**.

One Time Password

Enter 6 digit One Time Password

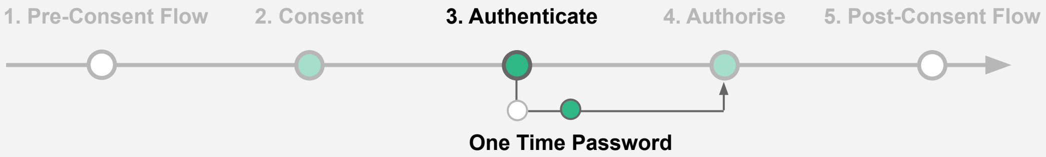
Connect

Cancel

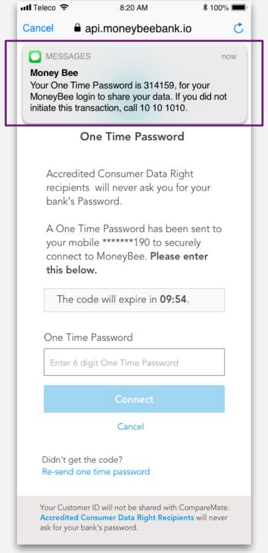
Didn’t get the code?
Re-send one time password

Your Customer ID will not be shared with CompareMate. **Accredited Consumer Data Right Recipients** will never ask for your bank’s password.

Example wireframe 3.2



Component 3.2: One Time Password delivery



Teleco 8:20 AM 100%

Cancel api.moneybeebank.io

MESSAGES now

Money Bee
Your One Time Password is 314159, for your MoneyBee login to share your data. If you did not initiate this transaction, call 10 10 1010.

One Time Password

Accredited Consumer Data Right recipients will never ask you for your bank's Password.

A One Time Password has been sent to your mobile *******190 to securely connect to MoneyBee. **Please enter this below.**

The code will expire in **09:54**.

One Time Password

Enter 6 digit One Time Password

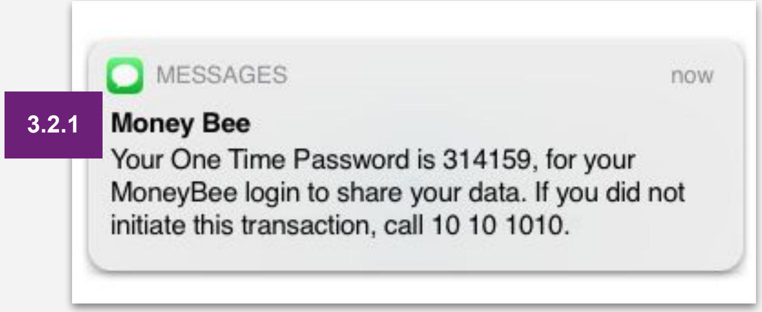
Connect

Cancel

Didn't get the code?
Re-send one time password

Your Customer ID will not be shared with CompareMate. Accredited Consumer Data Right Recipients will never ask for your bank's password.

3.2.1



MESSAGES now

Money Bee
Your One Time Password is 314159, for your MoneyBee login to share your data. If you did not initiate this transaction, call 10 10 1010.

Note: The component above is an example of how the following rule can be implemented.

Authenticate | One Time Password

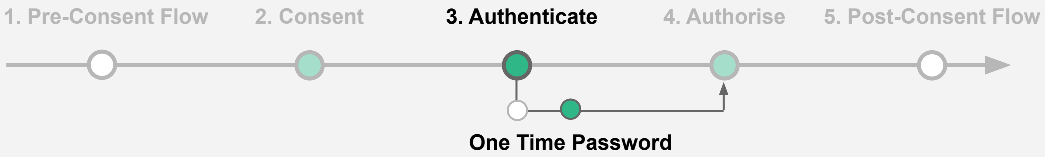
Component 3.2: One Time Password delivery

Guidelines

3.2.1 **Mandatory**

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.

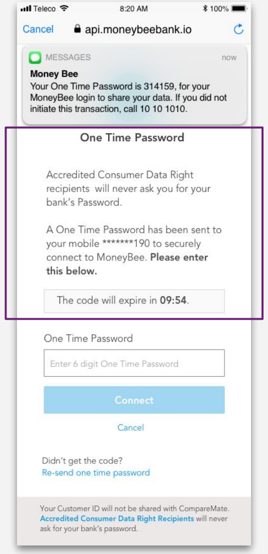
CX Research 12, 27 | *Security Profile*



1. Pre-Consent Flow 2. Consent 3. Authenticate 4. Authorise 5. Post-Consent Flow

One Time Password

Component 3.3: One Time Password instructions



Teleco 8:20 AM 100%

Cancel api.moneybeebank.io

MESSAGES now

Money Bee
Your One Time Password is 314159, for your MoneyBee login to share your data. If you did not initiate this transaction, call 10 10 1010.

One Time Password

Accredited Consumer Data Right recipients will never ask you for your bank's Password.

A One Time Password has been sent to your mobile *******190 to securely connect to MoneyBee. **Please enter this below.**

The code will expire in **09:54**.

One Time Password

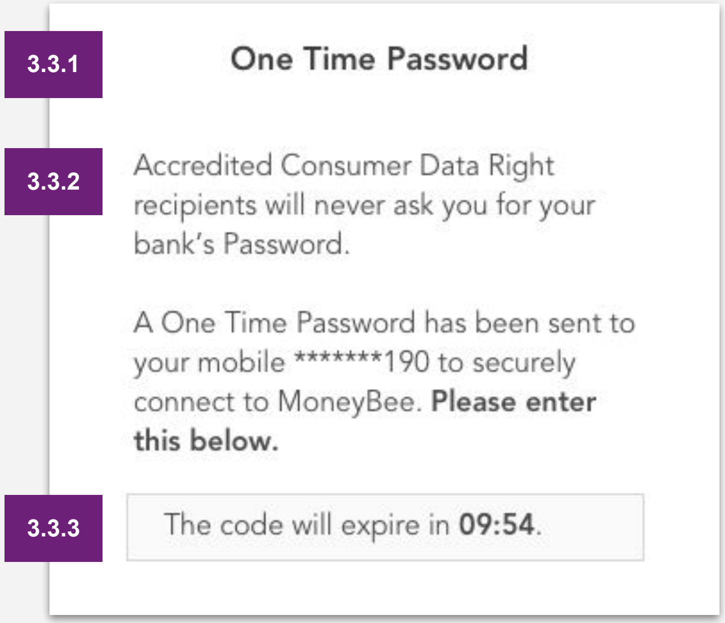
Enter 6 digit One Time Password

Connect

Cancel

Didn't get the code?
Re-send one time password

Your Customer ID will not be shared with CompareMate. Accredited Consumer Data Right Recipients will never ask for your bank's password.



One Time Password

Accredited Consumer Data Right recipients will never ask you for your bank's Password.

A One Time Password has been sent to your mobile *******190 to securely connect to MoneyBee. **Please enter this below.**

The code will expire in **09:54**.

Note: The component above is an example of how the following rules can be implemented.

Authenticate | One Time Password

Component 3.3: One Time Password instructions

Guidelines

3.3.1 Mandatory

Data holders and data recipients **must** clearly refer to the OTP as a "One Time Password" in consumer-facing interactions and material.

CX Research 10 | Security Profile

3.3.2 Mandatory

Data holders and data recipients **must** state in consumer-facing interactions and material that ADRs will never ask consumers for their banking password to access CDR data.

CX Research 21 | Security Standards

3.3.3 Mandatory

The provided OTP **must** be invalidated after a period of time at the discretion of the Data Holder. This expiry **must** be communicated in the authentication flow. This expiry period **should** facilitate enough time for the consumer to reasonably complete the authentication process.

CX Research 11 | Security Profile

4. AUTHORISE

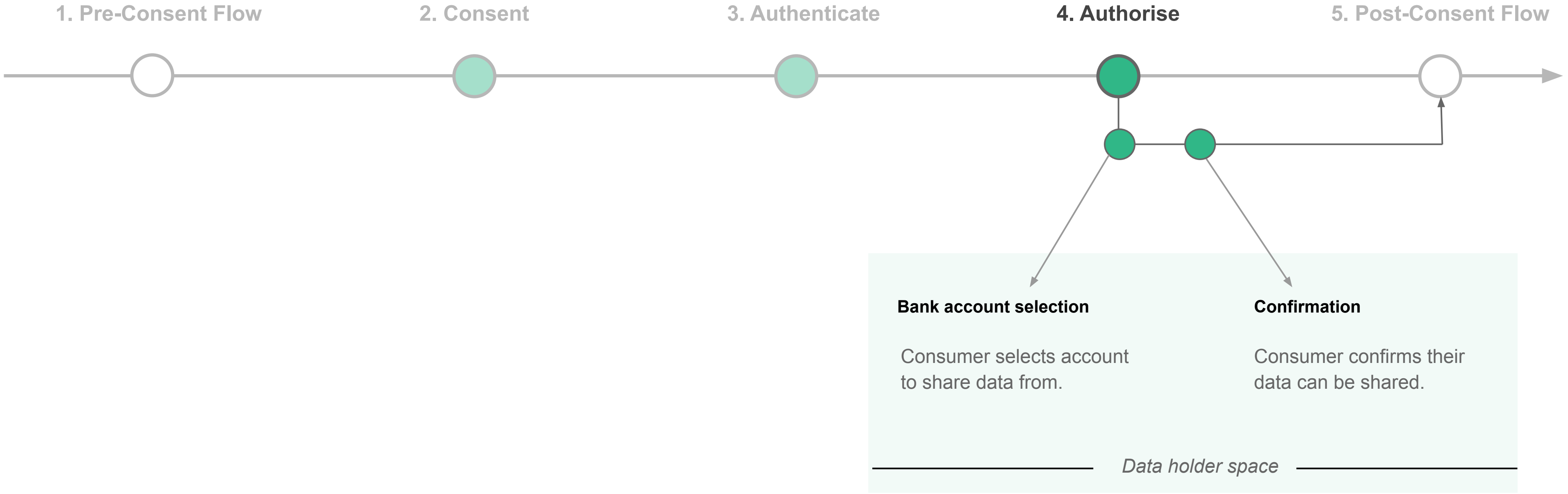
The Authorise stage is further broken down into two steps: Bank account selection; and Confirmation.

Bank 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.



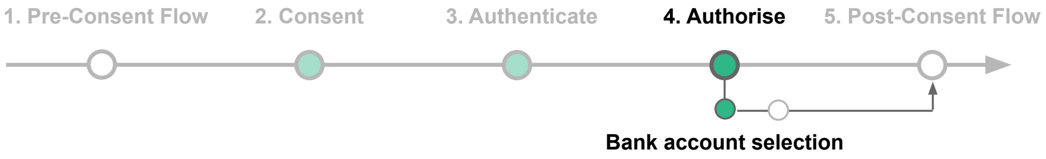
Bank account selection

Consumer selects account to share data from.

Confirmation

Consumer confirms their data can be shared.

Data holder space



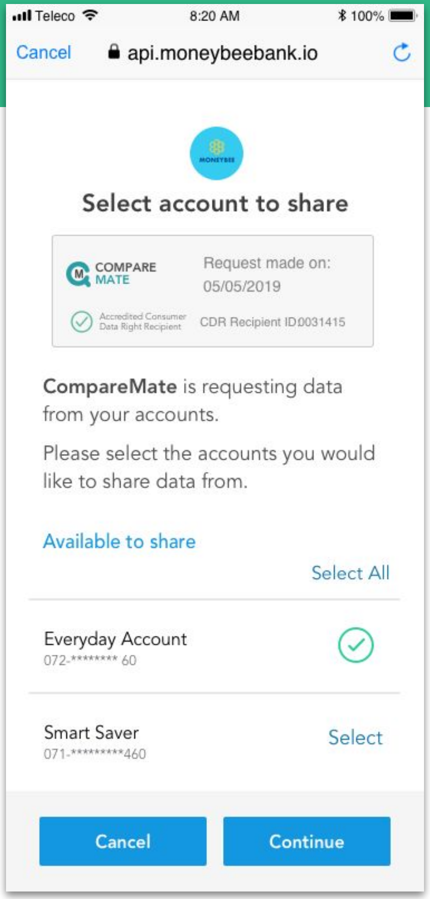
1. Pre-Consent Flow 2. Consent 3. Authenticate **4. Authorise** 5. Post-Consent Flow

Bank account selection

Authorise | Account selection

Component 4.1 - 4.2

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.



Select account to share

Request made on: 05/05/2019

CDR Recipient ID.0031415

CompareMate is requesting data from your accounts.

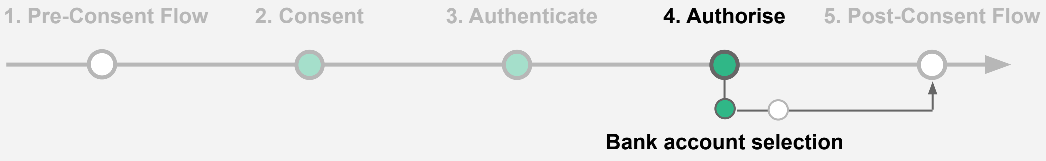
Please select the accounts you would like to share data from.

Available to share

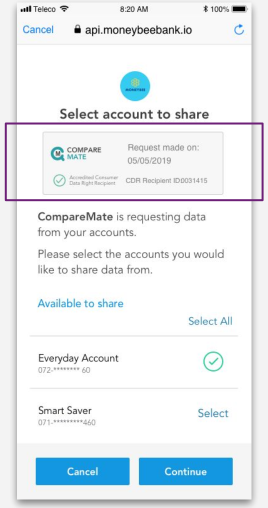
Everyday Account
072-******** 60 ✓

Smart Saver
071-*********460

Example wireframe 4.1



Component 4.1: Data recipient information


Teleco 8:20 AM 100%

Cancel api.moneybeebank.io

MONEYBEE

Select account to share

COMPARE MATE Request made on: 05/05/2019

Accredited Consumer Data Right Recipient CDR Recipient ID:0031415

CompareMate is requesting data from your accounts.

Please select the accounts you would like to share data from.

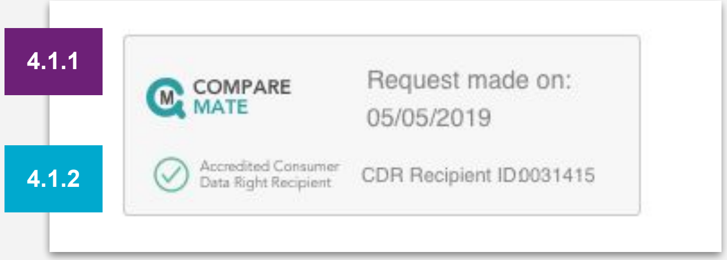
Available to share

Select All

Everyday Account ✓
072-******** 60

Smart Saver Select
071-*********460

Cancel Continue



COMPARE MATE Request made on: 05/05/2019

Accredited Consumer Data Right Recipient CDR Recipient ID:0031415

Note: The component above is an example of how the following rule and recommendation can be implemented.

Authorise | Account selection

Component 4.1: Data recipient information

Guidelines

4.1.1 Mandatory

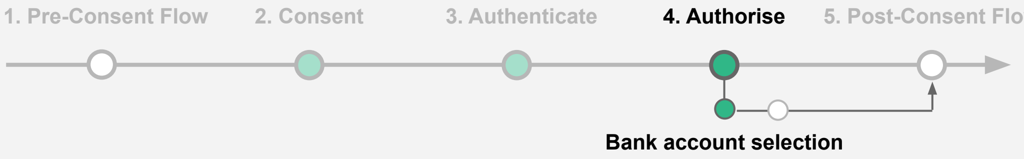
The data holder **must** state which data recipient is making the request. The data holder **should** show this information as soon as the authorisation flow begins.

CDR Rule 4.22(2)(a)

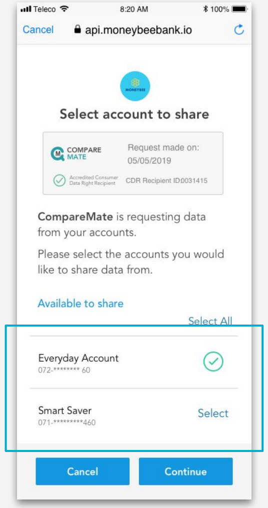
4.1.2 Recommended

The data holder **should** show the ACCC provided ‘trust mark’ and details of the request including a data recipient identifier, and the date the request was made.

CX Research 13, 23



Component 4.2: Account selection


Teleco 8:20 AM 100%

Cancel api.moneybeebank.io

Select account to share

COMPARE MATE Request made on: 05/05/2019

Accredited Consumer Data Right Recipient CDR Recipient ID0031415

CompareMate is requesting data from your accounts.

Please select the accounts you would like to share data from.

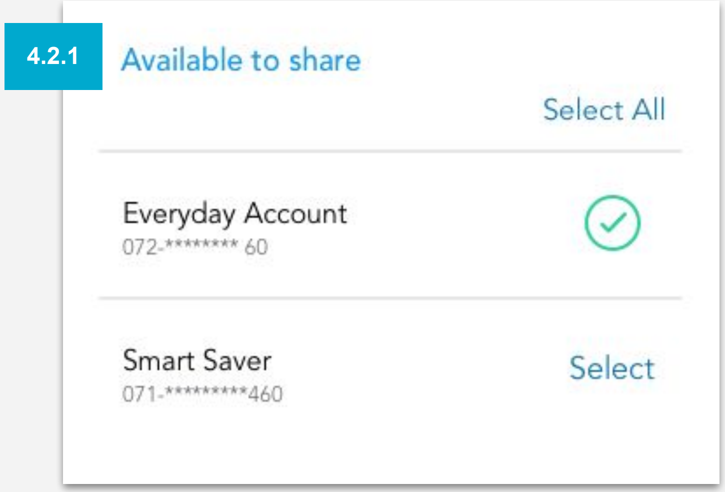
Available to share

Select All

Everyday Account
072-******** 60 ✓

Smart Saver
071-*********460 Select

Cancel Continue


4.2.1

Available to share

Select All

Everyday Account
072-******** 60 ✓

Smart Saver
071-*********460 Select

Note: The component above is an example of how the following recommendations can be implemented.

Authorise | Account selection

Component 4.2: Account selection

Guidelines

4.2.1 Recommended

The data holder **should** allow the consumer to select which accounts to share data from.

CX Research 9

4.2.1 Recommended

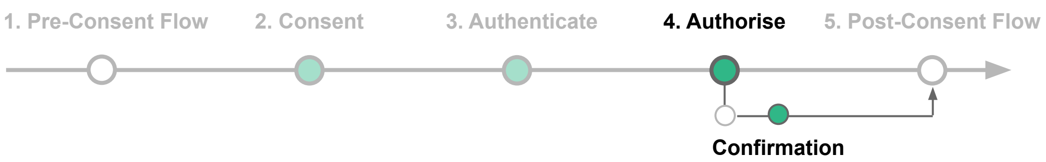
Data holders **should** state when accounts being selected are joint accounts.

Data holders **should** pay special attention to vulnerable consumers with joint accounts.

Data holders **should** provide exemptions for vulnerable consumers with joint accounts that can be triggered at the account selection stage. Such exemptions **should** prevent other joint account holders from being notified when a vulnerable consumer shares their own data.

Data holders **should** allow consumers to notify the data holder if they are vulnerable and/or at-risk during the authorisation flow.

Specific authorisation flows for joint accounts **should** be determined by data holders to align with existing mechanisms. Further versions of the CX Guidelines will provide standardised flows and guidance if required.



Authorise | Confirmation

Component 4.3 - 4.7

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.

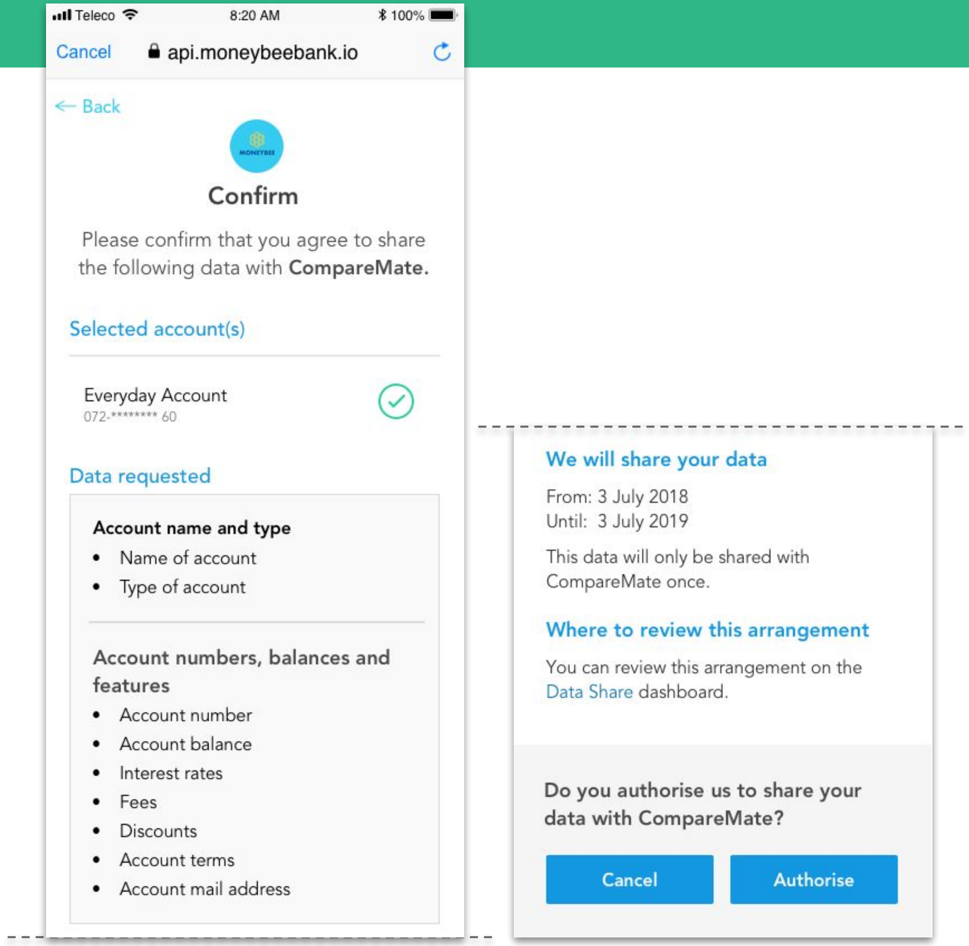
The data holder **should** not introduce any additional consumer-facing interactions, instructions, or communications except where legally required. This includes copy that may call into question the security of sharing data as part of the CDR, or introducing unnecessary friction (*CDR Rule 4.23*).

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.



Teleco 8:20 AM 100%

Cancel api.moneybeebank.io

← Back

Confirm

Please confirm that you agree to share the following data with **CompareMate.**

Selected account(s)

Everyday Account
072-******** 60 ✓

Data requested

Account name and type

- Name of account
- Type of account

Account numbers, balances and features

- Account number
- Account balance
- Interest rates
- Fees
- Discounts
- Account terms
- Account mail address

We will share your data

From: 3 July 2018
Until: 3 July 2019

This data will only be shared with CompareMate once.

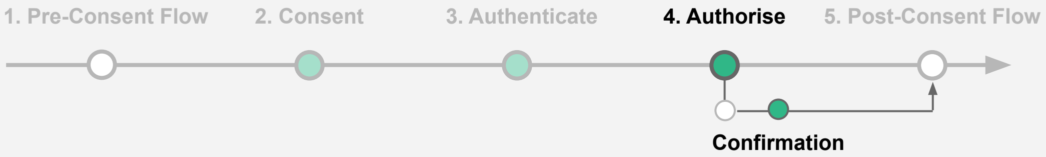
Where to review this arrangement

You can review this arrangement on the Data Share dashboard.

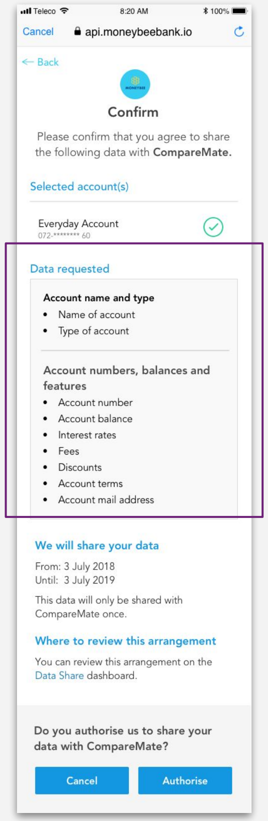
Do you authorise us to share your data with CompareMate?

Cancel | Authorise

Example wireframe 4.2



Component 4.3: Data clusters confirmation



Confirm

Please confirm that you agree to share the following data with **CompareMate.**

Selected account(s)

Everyday Account
072-******** 60

Data requested

Account name and type

- Name of account
- Type of account

Account numbers, balances and features

- Account number
- Account balance
- Interest rates
- Fees
- Discounts
- Account terms
- Account mail address

We will share your data

From: 3 July 2018
Until: 3 July 2019

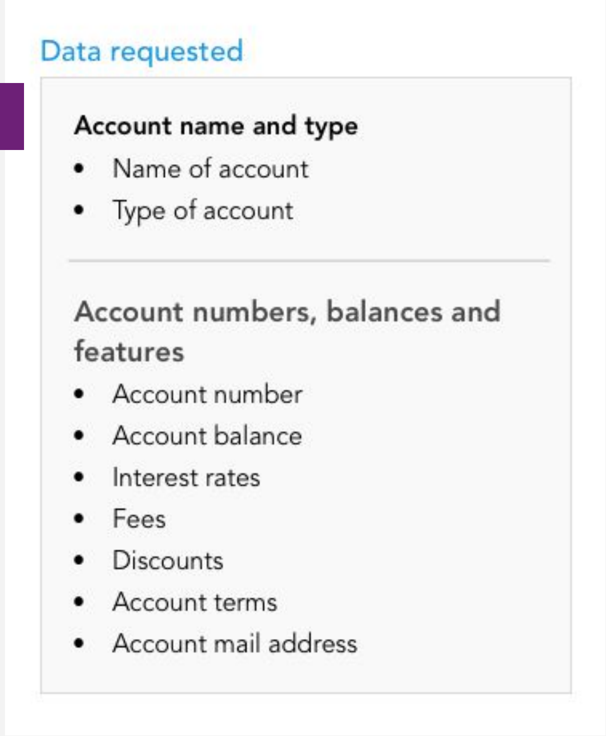
This data will only be shared with CompareMate once.

Where to review this arrangement

You can review this arrangement on the Data Share dashboard.

Do you authorise us to share your data with CompareMate?

4.3.1



Data requested

Account name and type

- Name of account
- Type of account

Account numbers, balances and features

- Account number
- Account balance
- Interest rates
- Fees
- Discounts
- Account terms
- Account mail address

Note: The component above is an example of how the following rules and the recommendation can be implemented.

Authorise | Confirmation

Component 4.3: Data clusters confirmation

Guidelines

4.3.1 **Mandatory**

The data holder **must** list the data clusters consented to be shared. Permission language within each data cluster **must** also be listed.

CDR Rule 4.22(2)(c)

4.3.1 **Mandatory**

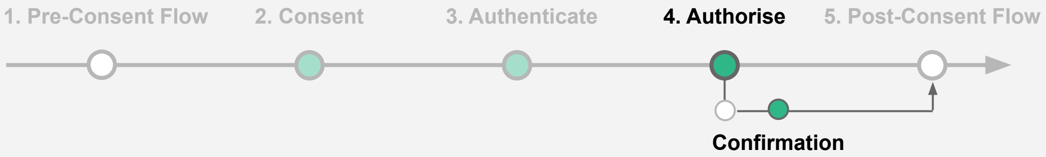
Specific language **must** be used for data clusters and permissions.

CDR Rule 8.11 | Data Language Standards

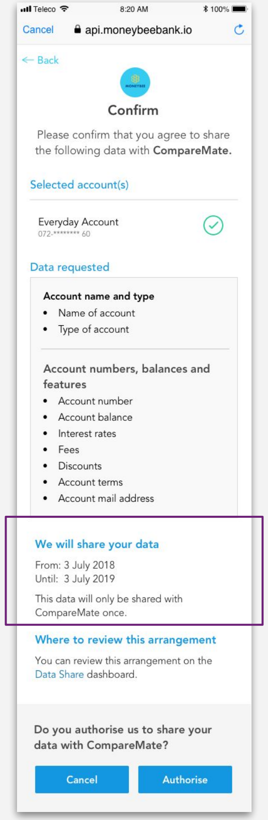
Recommended

The data holder **should** include in-line help (e.g. questions marks) to provide a more detailed but plain-English (grade 7 readability) descriptions of what is included in the data cluster, including permissions.

Nielsen and Molich's 10 User Interface Design Heuristics: Help and documentation; Match between system and the real world



Component 4.4: Duration


Teleco 8:20 AM 100%

Cancel api.moneybeebank.io

← Back

Confirm

Please confirm that you agree to share the following data with **CompareMate.**

Selected account(s)

Everyday Account
072-******** 60

Data requested

Account name and type

- Name of account
- Type of account

Account numbers, balances and features

- Account number
- Account balance
- Interest rates
- Fees
- Discounts
- Account terms
- Account mail address

We will share your data

From: 3 July 2018
Until: 3 July 2019

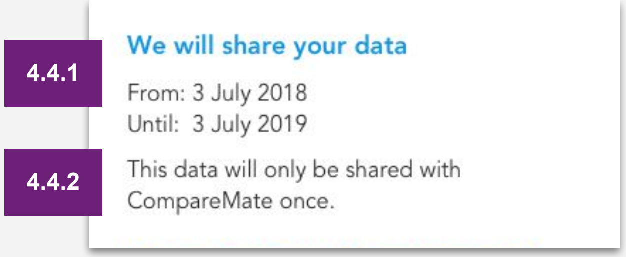
This data will only be shared with CompareMate once.

Where to review this arrangement

You can review this arrangement on the Data Share dashboard.

Do you authorise us to share your data with CompareMate?

Cancel | Authorise


4.4.1

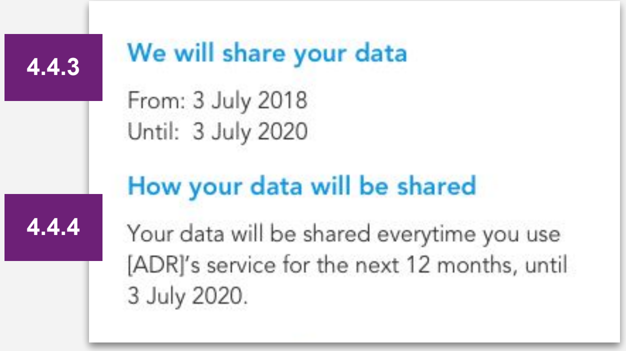
We will share your data

From: 3 July 2018
Until: 3 July 2019

4.4.2

This data will only be shared with CompareMate once.

On-going data sharing [Rule 4.22(2)(d)(ii)]


4.4.3

We will share your data

From: 3 July 2018
Until: 3 July 2020

4.4.4

How your data will be shared

Your data will be shared everytime you use [ADR]'s service for the next 12 months, until 3 July 2020.

Single collection aka 'once-off' [Rule 4.22(2)(d)(i)]

Note: The components above are examples of how the following rules can be implemented.

Authorise | Confirmation

Component 4.4: Duration

Guidelines

4.4.1 **4.4.3** **Mandatory**

The data holder **must** state the sharing duration to the consumer, including how far back in time data will be accessed.

The data holder **should** present the range of collection and use in a way that is easy to understand.

4.22(2)(b) and (e)

4.4.2 **4.4.4** **Mandatory**

The data holder **must** state whether data will be shared for single or on-going collection.

4.22(2)(d)

4.4.2 **4.4.4** **Mandatory**

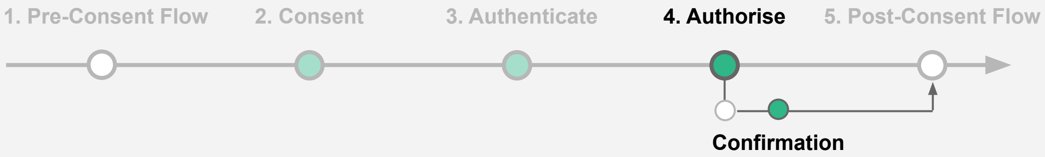
The data holder **must** state how often the data will be disclosed over the specific period.

4.22(2)(e)

4.4.3 **Mandatory**

The data holder **must** notify the consumer of the expiry date of their data sharing.

CDR Rule 4.25



1. Pre-Consent Flow

2. Consent

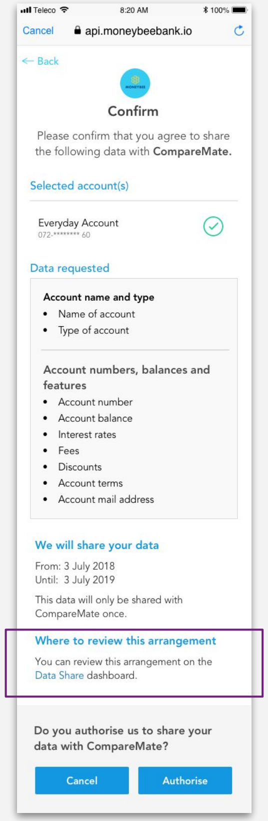
3. Authenticate

4. Authorise

5. Post-Consent Flow

Confirmation

Component 4.5: Review and revocation



Teleco 8:20 AM 100%

Cancel api.moneybeebank.io

Confirm

Please confirm that you agree to share the following data with **CompareMate.**

Selected account(s)

Everyday Account
072-******** 60 ✓

Data requested

Account name and type

- Name of account
- Type of account

Account numbers, balances and features

- Account number
- Account balance
- Interest rates
- Fees
- Discounts
- Account terms
- Account mail address

We will share your data

From: 3 July 2018
Until: 3 July 2019

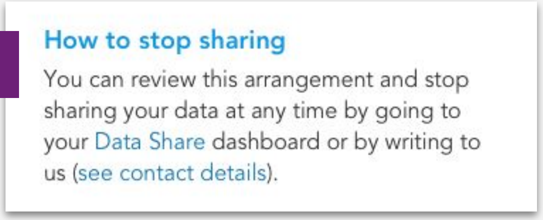
This data will only be shared with CompareMate once.

Where to review this arrangement

You can review this arrangement on the Data Share dashboard.

Do you authorise us to share your data with CompareMate?

4.5.1

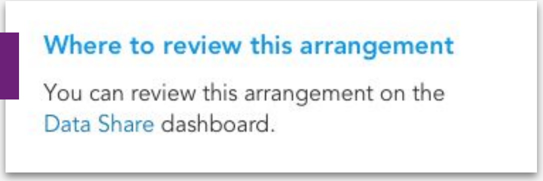


How to stop sharing

You can review this arrangement and stop sharing your data at any time by going to your Data Share dashboard or by writing to us (see contact details).

On-going data sharing [Rule 4.22(2)(d)(ii)]

4.5.2



Where to review this arrangement

You can review this arrangement on the Data Share dashboard.

Single collection aka 'once-off' [Rule 4.22(2)(d)(i)]

Note: The components above are examples of how the following rules can be implemented.

Authorise | Confirmation

Component 4.5: Review and revocation

Guidelines

4.5.1 Mandatory

The data holder **must** state that authorisation can be withdrawn at any time and provide instructions for how to withdraw authorisation.

The data holder **must** provide a clear and consistent location for the consent management dashboard via which consent can be withdrawn.

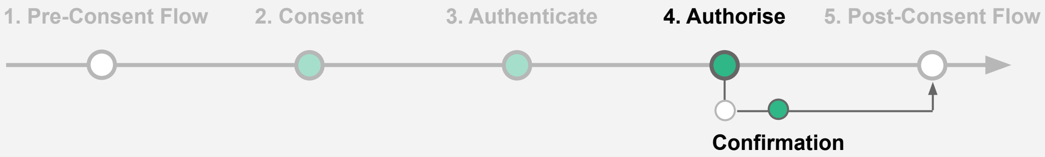
Data holders **must** allow the consumer to withdraw authorisation via an authorisation management dashboard or by writing to the data holder.

CDR Rules 4.22(2)(f) and (g), 4.24(1) | CX Research 30, 32, 33

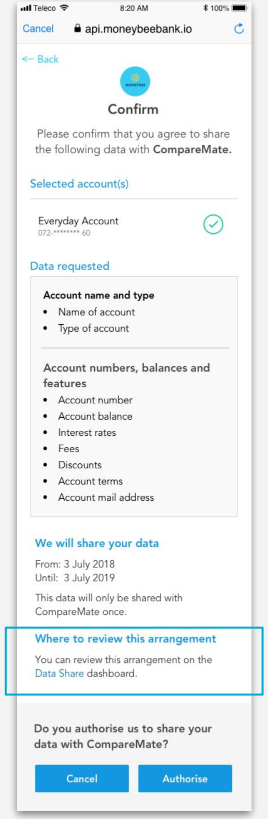
4.5.2 Mandatory

Data holders **must** state that sharing arrangements for single collection requests can be reviewed via authorisation management dashboards.

CX Research 20


1. Pre-Consent Flow
2. Consent
3. Authenticate
4. Authorise
5. Post-Consent Flow
Confirmation

Component 4.5: Review and revocation (continued)


Teleco 8:20 AM 100%

Cancel api.moneybeebank.io

← Back

Confirm

Please confirm that you agree to share the following data with **CompareMate.**

Selected account(s)

Everyday Account
072-******** 60

Data requested

Account name and type
- Name of account
- Type of account

Account numbers, balances and features
- Account number
- Account balance
- Interest rates
- Fees
- Discounts
- Account terms
- Account mail address

We will share your data

From: 3 July 2018
Until: 3 July 2019

This data will only be shared with CompareMate once.

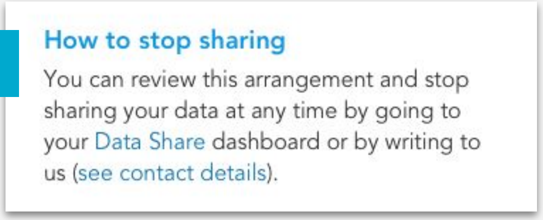
Where to review this arrangement

You can review this arrangement on the Data Share dashboard.

Do you authorise us to share your data with CompareMate?

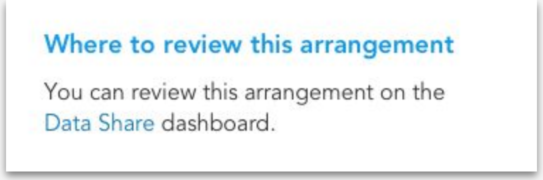
Cancel | Authorise

4.5.2


How to stop sharing

You can review this arrangement and stop sharing your data at any time by going to your Data Share dashboard or by writing to us (see contact details).

On-going data sharing [Rule 4.22(2)(d)(ii)]


Where to review this arrangement

You can review this arrangement on the Data Share dashboard.

Single collection aka 'once-off' [Rule 4.22(2)(d)(i)]

Note: The components above are examples of how the following recommendations can be implemented.

Authorise | Confirmation

Component 4.6: Review and revocation (continued)

Guidelines

4.5.2 Recommended

The data holder **should** use the phrase 'Stop Sharing' to refer to how a consumer can withdraw or revoke authorisation.

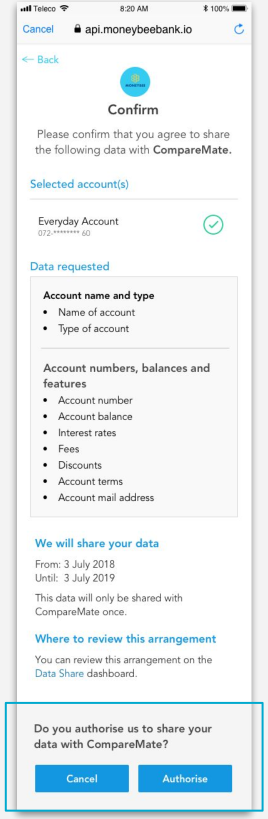
CX Research 29

4.5.2 Recommended

The data holder **should** allow consumers to initiate revocation via existing and preferred channels. These channels **should** be used as initial contact points that guide consumers towards the appropriate revocation pathway (i.e. a consent/authorisation dashboard).

CX Research 15, 31, 32

Component 4.6: Final affirmative action



Confirm

Please confirm that you agree to share the following data with **CompareMate.**

Selected account(s)

Everyday Account
072-******** 60

Data requested

Account name and type

- Name of account
- Type of account

Account numbers, balances and features

- Account number
- Account balance
- Interest rates
- Fees
- Discounts
- Account terms
- Account mail address

We will share your data

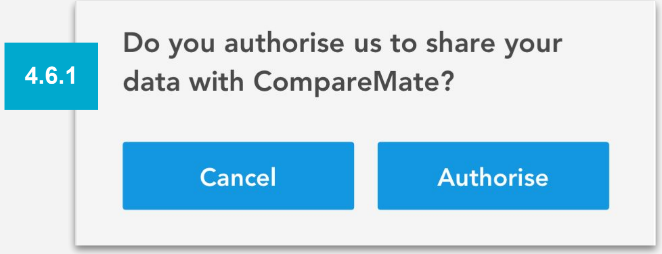
From: 3 July 2018
Until: 3 July 2019

This data will only be shared with CompareMate once.

Where to review this arrangement

You can review this arrangement on the Data Share dashboard.

Do you authorise us to share your data with CompareMate?



Do you authorise us to share your data with CompareMate?

Note: The component above is an example of how the following recommendation can be implemented.

Authorise | Confirmation

Component 4.6: Final affirmative action

Guidelines

4.6.1 Recommended

The data holder **should** use the term ‘Authorise’ 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.

Nielsen and Molich's 10 User Interface Design Heuristics: Error prevention

4.6.1 Recommended

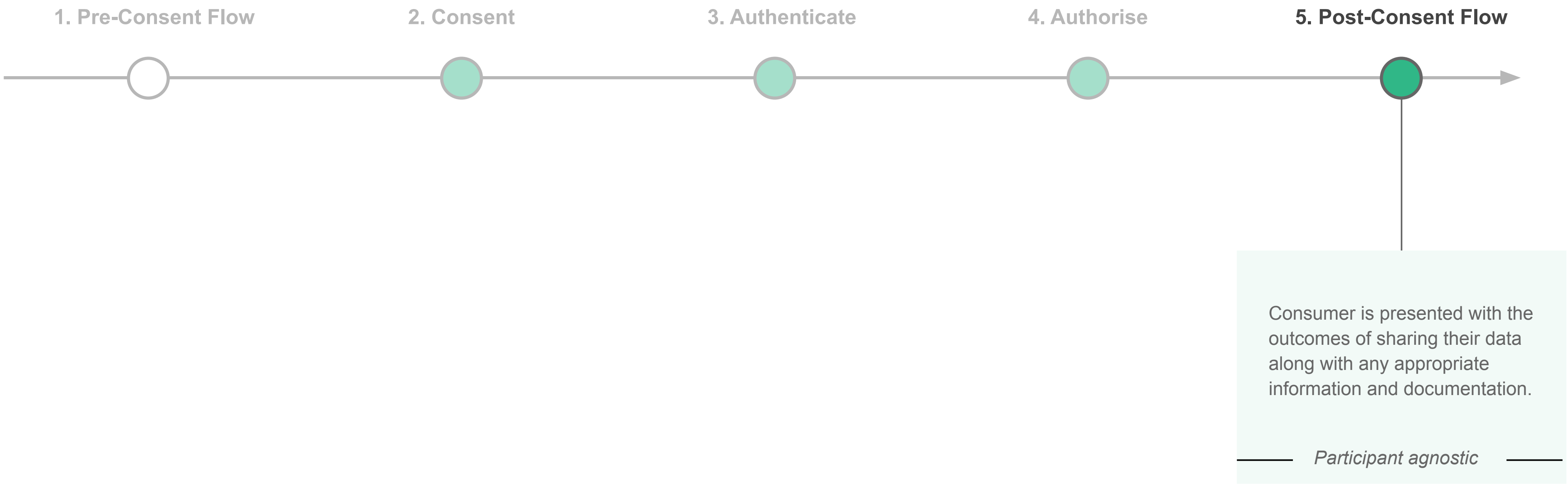
The data holder **should** redirect the consumer back to the data recipient.

CONSUMER
DATA
STANDARDS

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.



1. Pre-Consent Flow

2. Consent

3. Authenticate

4. Authorise

5. Post-Consent Flow

Consumer is presented with the outcomes of sharing their data along with any appropriate information and documentation.

Participant agnostic

Post-consent flow

This section describes how the guidelines may be implemented, in particular focusing on provision of a consent receipt and management of sharing arrangement(s) via a consumer dashboard.

This section will be expanded in future versions of the CX Guidelines to include additional detail on communications, notifications, consent management, revocation, and reauthorisation.

Guidelines

Recommended

The data recipient and data holder **should** send the consumer a record of the sharing arrangement after authorisation has occurred.

This information **should** also contain details on complaint handling and resolution processes, as well as details on how to review and revoke consent and authorisation.

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

CX Research 20

Recommended

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.

Following a joint account authorisation, the non-initiating account holder **should** be provided with instructions on how to review and revoke authorisation via a dashboard.

The data recipient and data holder **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.

RE-AUTHORISATION

The DSB has determined that for version 1 of the CDR implementation the full authorisation flow will be required for any extensions of approval.

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.

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 revoke the 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 revocation** Add revocation 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 revocation 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	**Trust mark should be strengthened by linking it to accreditation information** '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/revoked** 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 revoking 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	**Revocation 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 revoke 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

CX Research references

Ref #	Research findings	Source
31	**Multiple means of contact** Participants preferred to have a range of ways to contact data recipients and data holders, since certain situations required different contact methods. Participants sometimes preferred to use an app, email or website for speed and convenience; paper for record-keeping purposes; and phone to resolve complex issues quickly.	Phase 2, Stream 1 Research report, page 66
32	**Emphasis on ability to revoke consent important** Most participants felt reassured by the knowledge that they could easily revoke their consent whenever they wanted. Knowing that there were multiple options to revoke consent, including a way to revoke consent through the data recipient's app, was important to users.	Phase 2, Stream 1 Research report, page 34
33	**Repetition on the ability to revoke consent** Participants noted that repeating revocation information made them feel that the option was always available, and that they always had a choice when it came to revoking consent and ceasing to share data.	Phase 2, Stream 1 Research report, page 34
34	**De-identification language** De-identify is not a common term that consumers can easily understand. The process behind how this was done was unclear as well.	Phase 2, Stream 3 Research report, page 30
35	**Using appropriate security indicator provides trust** Have a visual indicator which is associated with being in a 'secure' environment. The use of appropriate language to assure consumers are in a secure environment, helped to alleviates some of the security and trust concerns raised in round 1 research.	Phase 2, Stream 3 Research report, page 44
36	**Consent should not be bundled with other purposes** Data recipients should not bundle consent with other directions, permissions, consents and agreements.	Consumer Data Right Rules Outline (Dec 2018), Rule 7.10(c)
37	**Accessibility - WCAG Guidelines** Accessibility was an important consideration brought up by many users, both to ensure that they would be able to read and understand the text, and to avoid accidentally performing unintended actions due to misclicks. The feasibility of requiring data recipients to have a font-magnification or zoom function in their apps should also be investigated.	Phase 2, Stream 1 report, page 51

CONSUMER
DATA
STANDARDS

Consumer Data Standards | Consumer Experience Workstream

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

www.consumerdatastandards.org.au