

CONSUMER DATA STANDARDS

Consultation draft - CDR consent management and revocation

7 August 2019

Contents

Management dashboard	3
Revocation	11
Appendix	17

Management dashboard

MANAGEMENT DASHBOARD

See InVision prototype

The Management dashboard enables a consumer to view their data sharing arrangements from different perspectives, allowing them to see: the organisations that they are sharing data from and to; the products they are sharing data for; the use cases enabled by their data sharing; and the specific details for each of their data sharing arrangements.

Consumer dashboard landing page

From this view, the consumer will be able to see a list of all their data sharing arrangements. By default, it may display the organisations that they are sharing data from and to.

Product view

From this view, the consumer will be able to see a list of the products that are utilising the data that they have shared e.g. a Budget Planner.

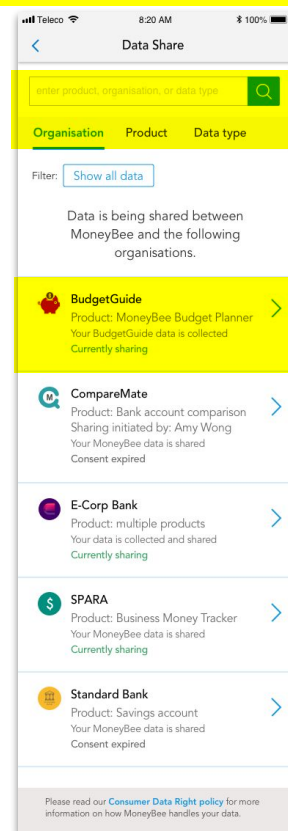
Use case view

From this view, the consumer will be able to see the use case(s) for their data e.g. tailored forecasting provided within the Budget Planner.

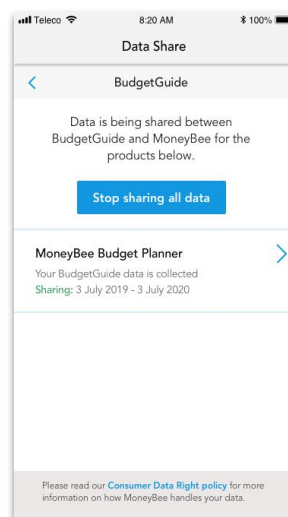
Data sharing arrangement

From this view, the consumer will be able to see a detailed breakdown of a specific data sharing arrangement including: the data clusters being shared; the account(s) data is being shared from; and timeframes related to the sharing arrangement.

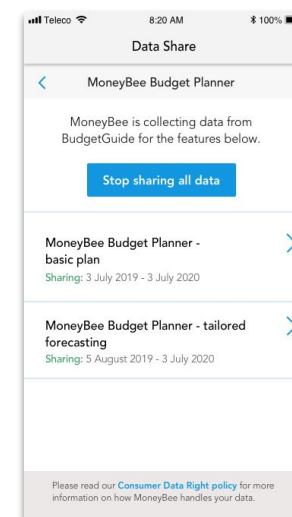
1. Consumer dashboard landing page



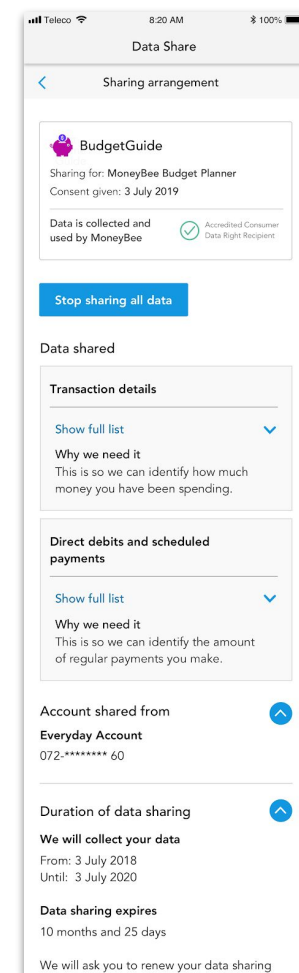
2. Product specific



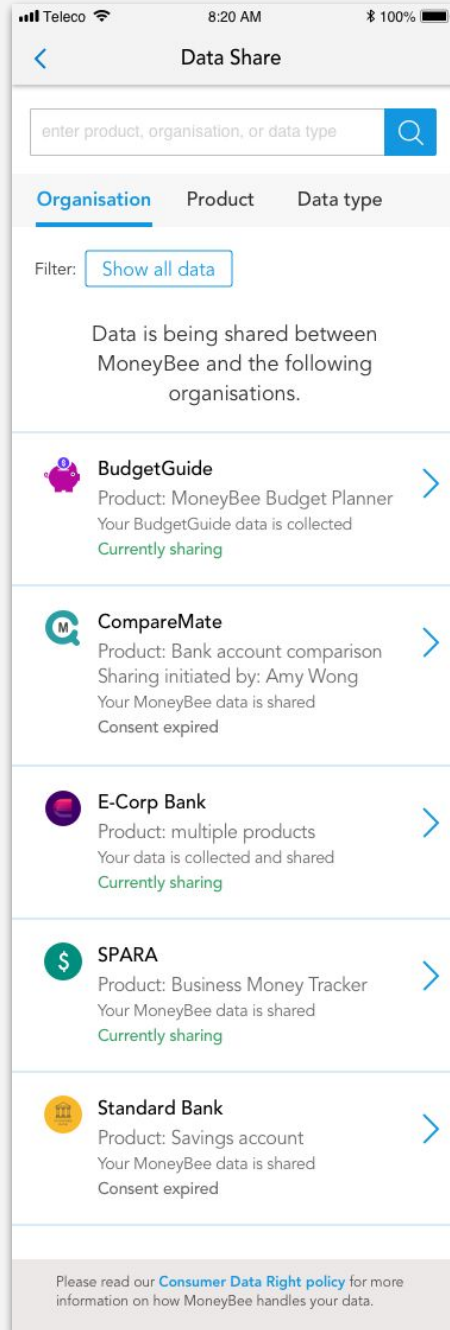
3. Use case specific



4. Data sharing arrangement



Note: The screens shown in this consultation draft are examples of how the following rules and recommendations can be implemented.



Note: The image on the right illustrates a data recipient consumer dashboard.

A data holder consumer dashboard would not show product specific information as purpose information is absent. Purpose is assumed to include purpose specification (why we need it), product/service and use case.

Management dashboard | Consumer dashboard landing page

Guidelines

Guideline 1.1 Mandatory

The data recipient and the data holder **must** provide an online service for the consumer to manage and revoke the consent of CDR data. This is known as the consumer dashboard.

CDR Rules 1.13(1) and (2), 1.14(1) and (2)

Guideline 1.2 Mandatory

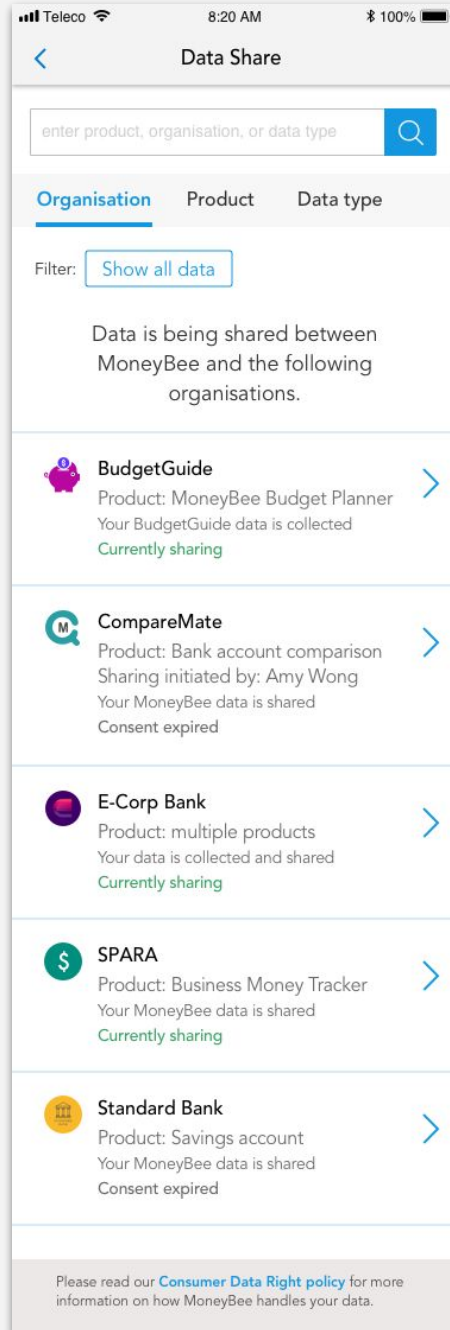
The data recipient **must** make their **CDR policy** readily available on their website or mobile app. This **may** be included at this point with the data recipient's own **privacy policy**.

CDR Rules 7.2(4), 7.2(5)

Guideline 1.3 Recommended

As sharing instances initiated by other account holders may be unfamiliar, data holders **should** show 'initiated by [other account holder name]' as part of sharing instance in dashboard to indicate to user if they did or did not initiate the sharing instance.

Ref TBC



Note: The image on the right illustrates a data recipient consumer dashboard.

A data holder consumer dashboard would not show product specific information as purpose information is absent. Purpose is assumed to include purpose specification (why we need it), product/service and use case.

Management dashboard | Consumer dashboard landing page (continued)

Guidelines

Guideline 1.4 Recommended

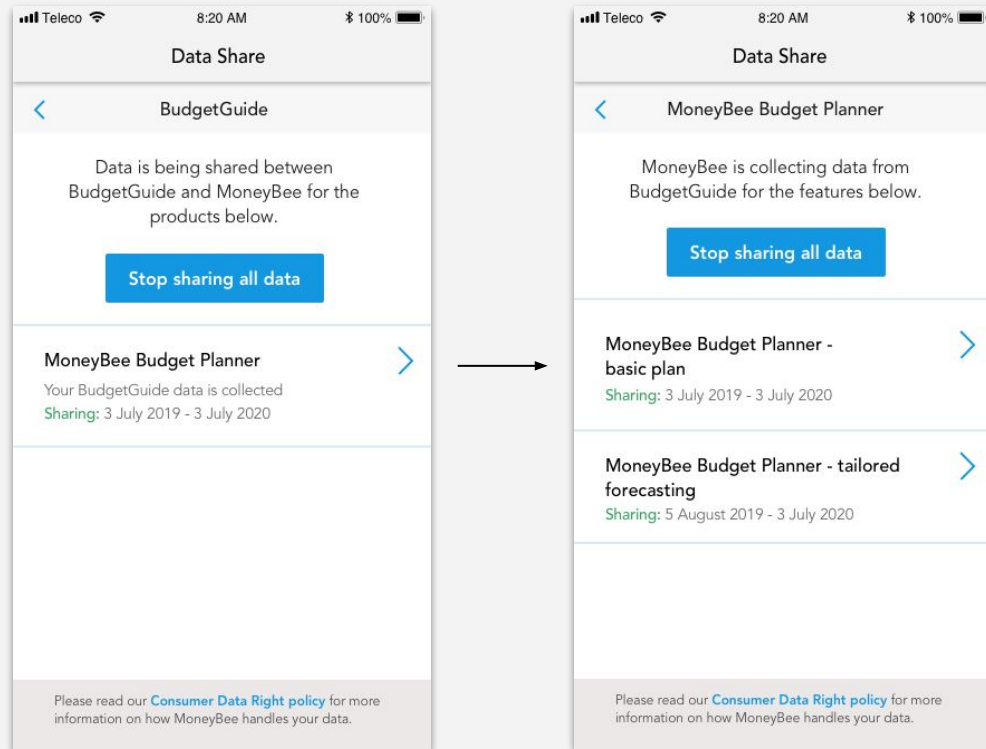
Dashboards **should** also be located in a consistently accessible location. The data recipient and data holder **should** also use consistent language for dashboards wherever possible but may use language that is specific to the platform if required.

Ref TBC

Guideline 1.5 Recommended

The consumer dashboard **should** allow consumers to view their information in various ways, including the ability to search for specific data sharing arrangements.

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



Note: The image above illustrates a data recipient consumer dashboard. A data holder consumer dashboard would not show product or use case specific information as purpose information is absent. Purpose is assumed to include purpose specification (why we need it), product/service and use case.

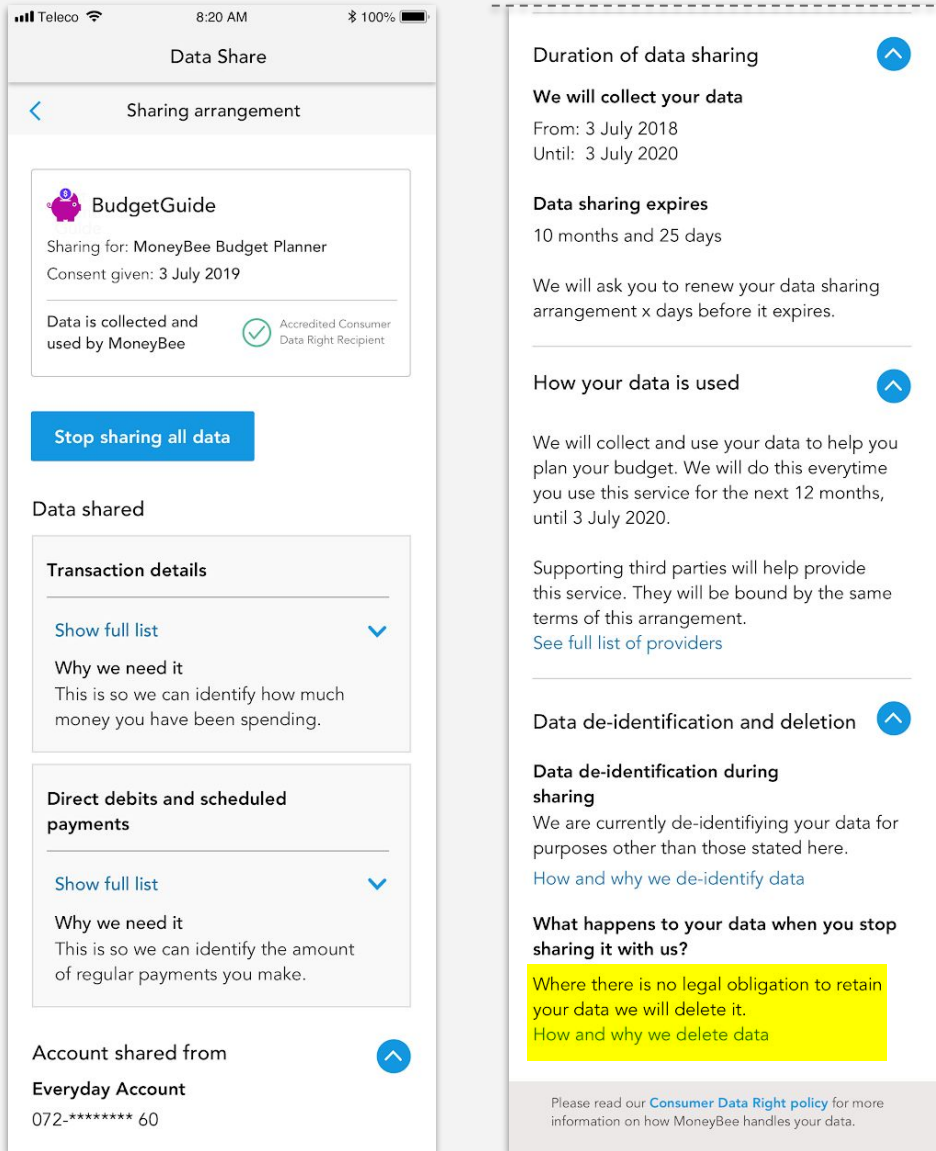
Management dashboard | Product specific and Use case specific

Guidelines

Guideline 2.1 / 3.1 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



Note: The image above illustrates a data recipient consumer dashboard. Information shown on **data de-identification** is an example of an additional use that would require consent during the Consent Flow.

Management dashboard | Data sharing arrangement

Data recipient consent management

Guidelines

Guideline 4.1 Mandatory

The consumer dashboard **must** show the following in regards to consent:

- The CDR data the consumer has consented to be collected and what the data will be used for;
- When the consumer gave consent;
- Whether consent was given for a single instance or over a period of time;
- If consent was given to collect and use CDR data over a period of time, the data recipient **must** show what that period is and how often data is expected to be collected over that period.
- When consent is scheduled to expire or has expired

CDR Rules 1.13(3)(a)(i)-(vi), 1.13(3)(b)

Guideline 4.2 Mandatory

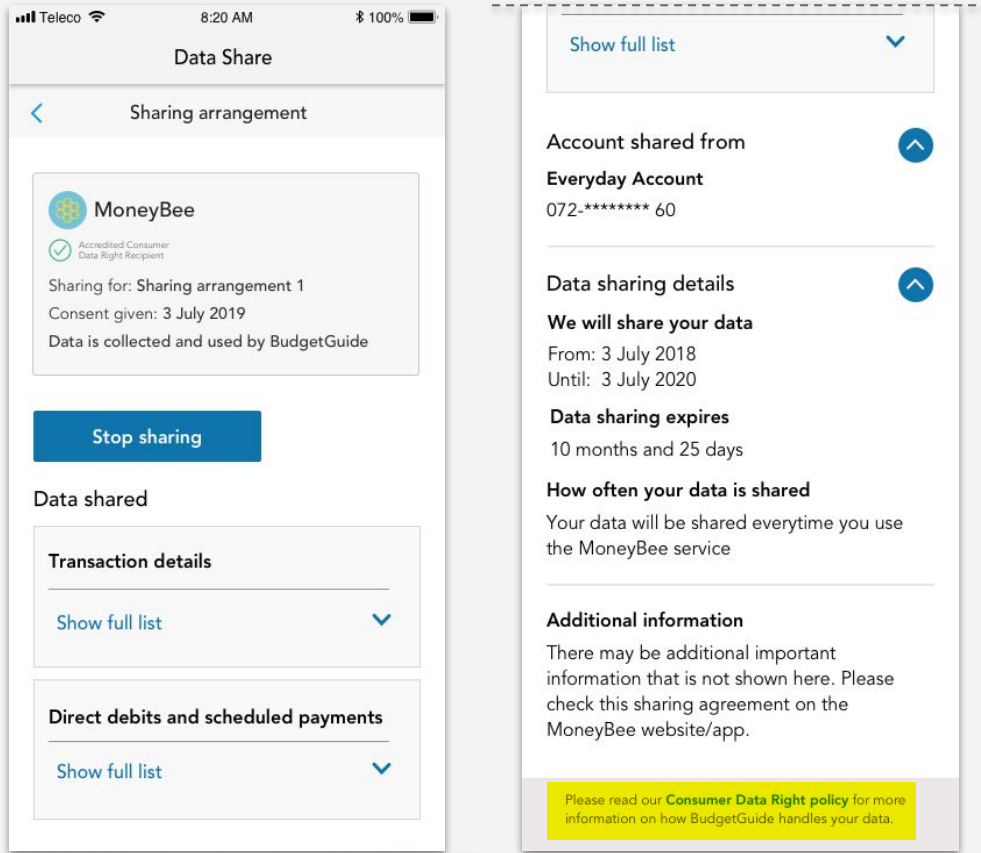
When the consumer has given consent for their data to be collected, the consumer dashboard **must** be updated to indicate what CDR data was collected, when this data was collected and the name of the data holder.

CDR Rules 1.13(3)(vii), 7.4

Guideline 4.3 Mandatory

Updates to the consumer dashboard **must** be done as soon as practicable. This includes when the consumer has consented to data collection and use, and when consent has expired.

CDR Rules 4.13, 4.19



Note: The above outlines what BudgetGuide would show their data holder consumer dashboard for the same product. This is what a data holder dashboard would show without purpose information present. **Purpose** is assumed to include purpose specification (why we need it), product/service and use case.

Management dashboard | Data sharing arrangement

Data holder authorisation management

Guidelines

Guideline 4.4 Mandatory

The consumer dashboard **must** show the following in regards to authorisation:

- The CDR data the consumer has authorised to share with the data recipient;
- When the consumer gave authorisation;
- The name of the data recipient who made the consumer data request;
- The period for which authorisation was given, whether it be a single instance or over a period of time;
- When authorisation is scheduled to expire or has expired

CDR Rules 1.14(3)(i)-(vi)

Guideline 4.5 Mandatory

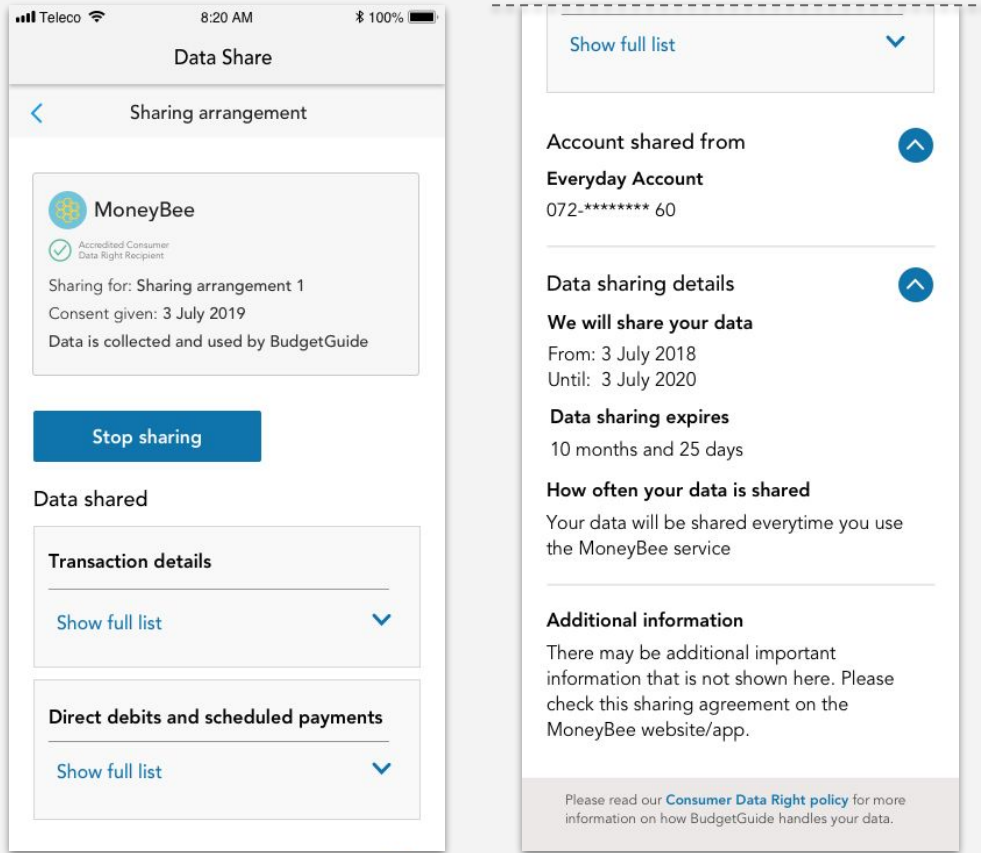
When the consumer has given authorisation for their data to be disclosed, the consumer dashboard **must** be updated to indicate what CDR data was disclosed, when this data was disclosed and the name of the data recipient.

CDR Rules 1.14(3)(vii), 7.6

Guideline 4.6 Mandatory

Updates to the consumer dashboard **must** be done as soon as practicable. This includes when the consumer has authorised for CDR data to be disclosed, and when authorisation has expired.

CDR Rule 4.26



Note: The above outlines what BudgetGuide would show as a data holder for the same product. This is what a data holder dashboard would show without purpose information present. Purpose is assumed to include purpose specification (why we need it), product/service and use case.

Management dashboard | Data sharing arrangement

Data holder authorisation management (continued)

Guidelines

Guideline 4.7 Mandatory

If authorisation was disclosed to share data from a joint account, the data recipient **must** provide a consumer dashboard to the other joint account holder.

CDR Rule 3.4(b)

Guideline 4.8 Mandatory

The data holder must include a functionality that permits the joint account holders to revoke authorisations, whether given by themselves or by the other joint account holder.

CDR Rules 3.2(1)(a)(iii) and (2)(b)(i)

Guideline 4.9 Recommended

All account holders, regardless of whether or not they initiated sharing, should receive the same level of detail on their dashboard.

Ref TBC

Revocation: Consumer journey

REVOCATION: CONSUMER JOURNEY OVERVIEW

See InVision prototype

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

Data sharing arrangement

Accessed via the Management dashboard, from this view, the consumer will be able to see the specific details of a data sharing arrangement and take action to stop sharing their data.

Revocation information

From this view, the consumer will be able to review and assess the implications of revoking a data sharing arrangement, including how it may impact their service and how their data will be managed.

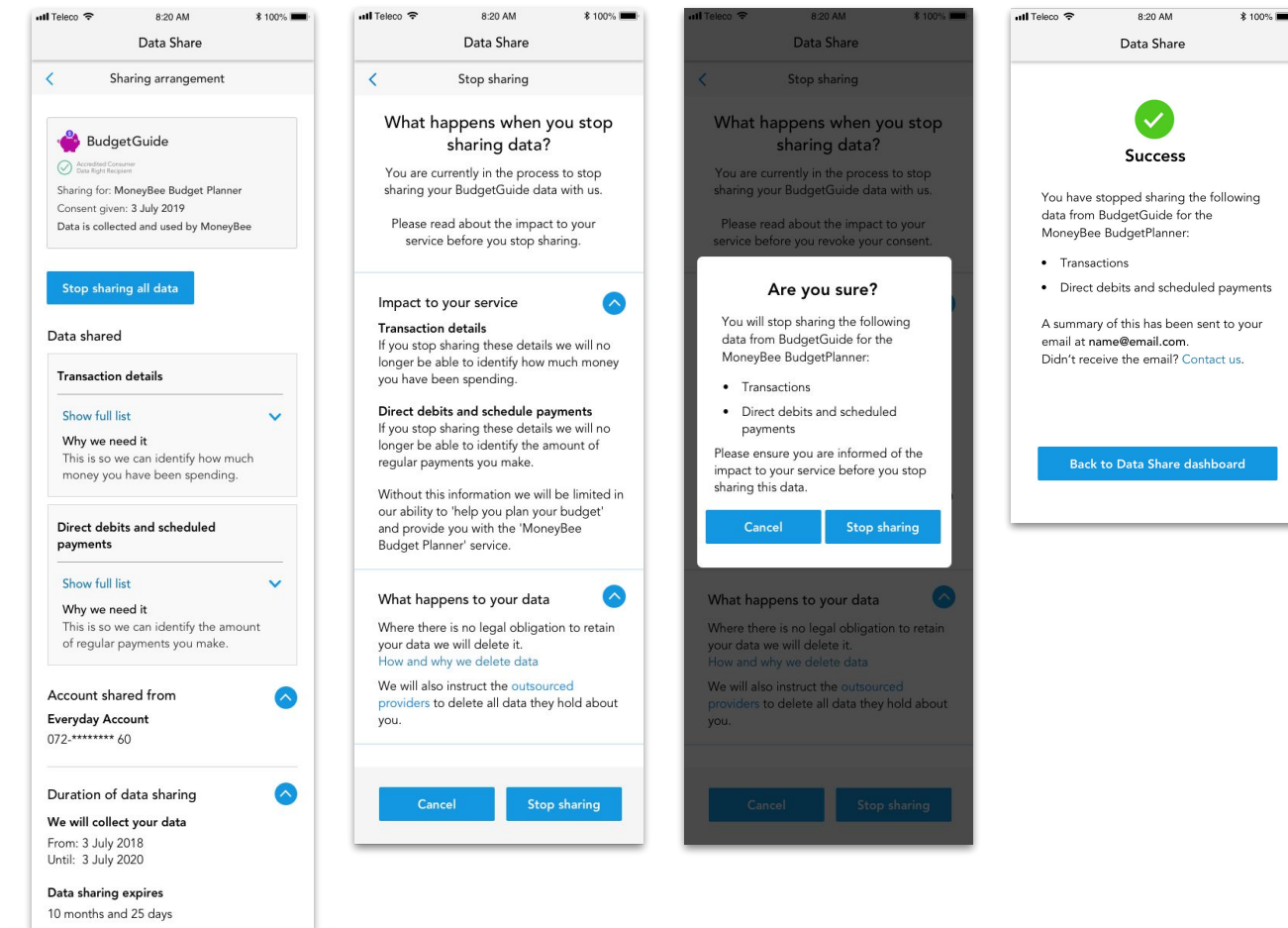
Confirmation

From this view, the consumer will be able to review a summary of the data sharing arrangement to be revoked and will have an opportunity to confirm or cancel.

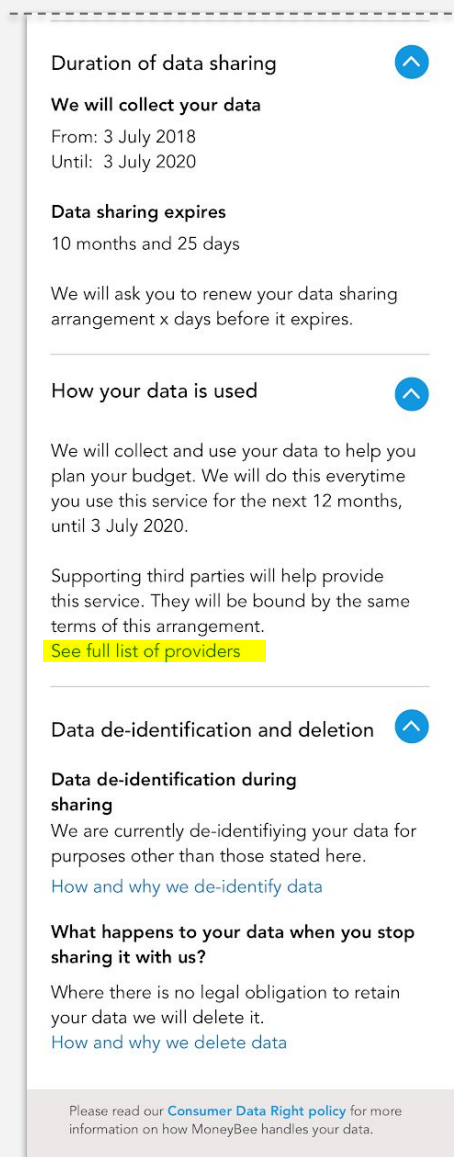
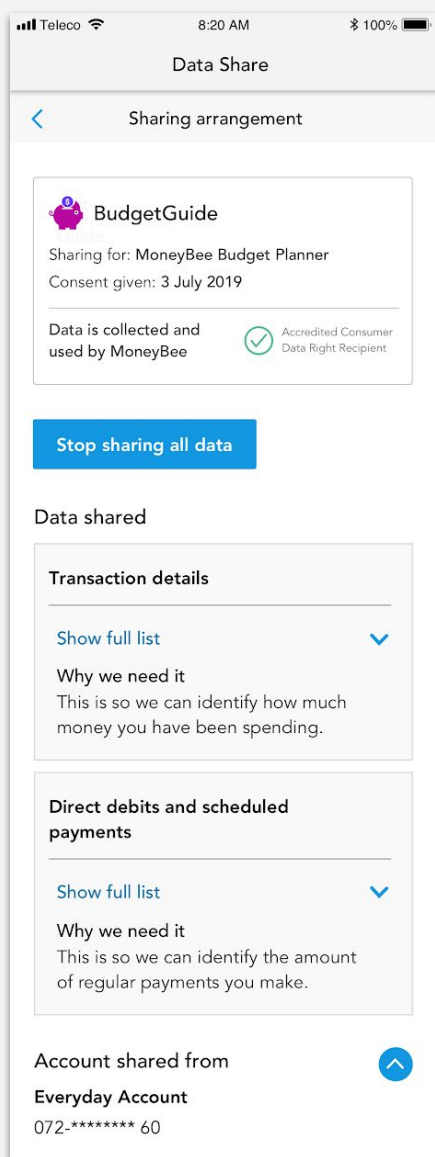
Revocation success

From this view, the consumer will be able to view a summary of the data sharing arrangement that they have successfully cancelled.

4. Data sharing arrangement 5. Revocation information 6. Confirmation 7.. Revocation success



Note: The screens shown in this consultation draft are examples of how the following rules and recommendations can be implemented.



Note: The image above illustrates a data recipient consumer dashboard. Information shown on data de-identification is an example of an additional use that would require consent during the Consent Flow.

Revocation | Data sharing arrangement

Data sharing withdrawal functionality

Guidelines

Guideline 4.10 Mandatory

The data recipient and the data holder **must** allow the consumer to withdraw consent/authorisation at any time using the consumer dashboard.

CDR Rules 1.13(3)(c), 1.14(3)(c), 4.11(1)(b), 4.17(b), 4.24(1)(b)

Guideline 4.11 Mandatory

The withdrawal functionality must be clearly visibly displayed.

CDR Rules 1.13(4)(c), 1.14(4)(c)

Guideline 4.12 Mandatory

The data holder must allow all joint account holders to withdraw from consent.

CDR Rule 3.7(1)

Guidelines 4.13 Recommended

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

CX Research 1

Data Share

[Stop sharing](#)

What happens when you stop sharing data?

You are currently in the process to stop sharing your BudgetGuide data with us.

Please read about the impact to your service before you stop sharing.

Impact to your service

Transaction details
If you stop sharing these details we will no longer be able to identify how much money you have been spending.

Direct debits and schedule payments
If you stop sharing these details we will no longer be able to identify the amount of regular payments you make.

Without this information we will be limited in our ability to 'help you plan your budget' and provide you with the 'MoneyBee Budget Planner' service.

What happens to your data

Where there is no legal obligation to retain your data we will delete it.
[How and why we delete data](#)

We will also instruct the [outsourced providers](#) to delete all data they hold about you.

[Cancel](#) [Stop sharing](#)

Revocation | Revocation information

Guidelines

Guideline 5.1 Mandatory

Withdrawal of consent and authorisation must be simple and straightforward to use. It must not be more complicated than the process of consent and the ability to withdraw from data sharing must be clearly visibly displayed.

CDR Rules 1.13(4), 1.14(4)

Guideline 5.2 Recommended

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

CX Research 1

Guideline 5.3 Recommended

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.

CX Research 2

sharing your BudgetGuide data with us.

Please read about the impact to your service before you revoke your consent.


Are you sure?

You will stop sharing the following data from BudgetGuide for the MoneyBee BudgetPlanner:

- Transactions
- Direct debits and scheduled payments

Please ensure you are informed of the impact to your service before you stop sharing this data.

[Cancel](#) [Stop sharing](#)

What happens to your data 

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

[How and why we delete data](#)

We will also instruct the outsourced

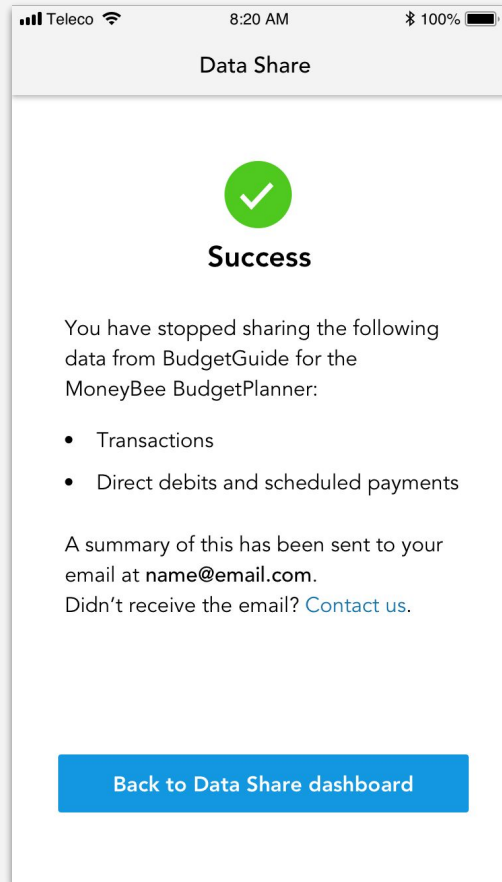
Revocation | Confirmation

Guidelines

Guideline 6.1 Recommended

The data recipient and holder should confirm user decision to stop sharing as a measure to mitigate user error.

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



Revocation | Revocation success

Guidelines

Guideline 7.1 Recommended

The data recipient or holder presents a 'confirmation' screen that includes a summary of what just occurred and send the consumer a **Consent Receipt** (e.g. via email).

Ref TBC

Appendix

CX Research references

Ref #	Research findings	Source
1	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
2	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



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