Australian Government

Consumer Data Right

Joint account implementation guidance for version 3 of the rules & onwards

January 2022

Table of Contents

1. Purpose of this document

1.1. This document provides an overview of the treatment of joint accounts under the *Competition and Consumer (Consumer Data Right) Rules 2020* (**rules**).

1.2. The rules deal with sharing Consumer Data Right (CDR) data from a joint account and prescribe how sharing arrangements can be authorised and approved by joint account holders.

1.3. This guidance is designed to be read in conjunction with the rules and has been updated to reflect changes to the treatment of joint accounts resulting from the Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021, commonly known as the version 3 rules. This guidance may also refer to previous and later versions of the rules. For the avoidance of doubt:

(a) The 'version 4 rules' are the principal rules as amended by the Competition and Consumer (Consumer Data Right) Amendment Rules (No. 2) 2021

(b) The 'version 2 rules' are the principal rules as amended by the Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020

(c) The 'version 1 rules' are the principal rules as amended by the Competition and Consumer (Consumer Data Right) Amendment Rules (No. 2) 2020

1.4. In a number of instances (for example, in relation to joint account notification requirements) the rules require data holders to act in accordance with relevant data standards. These data standards are made by the Data Standards Chair and maintained by the Data Standards Body (DSB). Data Standards can be accessed online.[1] In some instances, data standards are supported by DSB Consumer Experience Guidelines that provide examples and recommendations for how to implement key rules and standards that relate to the consumer experience. Where appropriate, relevant Consumer Experience Guidelines are referenced in this document.[2]

1.5. This document provides general guidance only. It does not constitute legal or other professional advice and should not be relied on as a statement of the law. We recommend that CDR participants obtain professional advice on how the rules apply to their specific circumstances.

2. Timeline for sharing CDR data from joint accounts

	Before 1 July 2022	**From 1 July 2022 onwards**
Major ADIs	Encouraged to share CDR data from joint accounts in accordance with version 3 of the rules. May elect to share CDR data from joint accounts in accordance with version 1 of the rules[3] until 1 July 2022.	Must share CDR data from joint accounts in accordance with version 3 of the rules.

[1] Consumer Data Right Consumer Data Standards, Data Standards Body
[2] Consumer Experience Standards and Guidelines, Data Standards Body
[3] The Joint Account Guidance for this version of the rules is available on the CDR Support Portal

Non-major ADIs	Not required to share CDR data from joint accounts. May voluntarily elect to share CDR data from joint accounts in accordance with version 3 of the rules.	Must share joint account data in accordance with version 3 of the rules.
Reciprocal data holders	Not required to share CDR data from joint accounts. May voluntarily elect to share joint account data in accordance with version 3 of the rules.	Must share joint account data in accordance with version 3 of the rules.

3. Key definitions

Joint account	Under the rules, a joint account is defined as an account for which there are two or more account holders who are: • individuals acting in their own capacity; and • eligible CDR consumers in relation to the data holder. This definition excludes partnership accounts. Data sharing from partnership accounts is enabled by a partnership's nominated representatives.
Joint account data	The joint account rules apply to the disclosure of account data, transaction data and product specific data (as defined in clause 1.3 of schedule 3). The joint account rules apply to these categories of data for any product in phase 1, 2, or 3.[4] Requesters may only ever share their own customer data; customer data of the other account holder(s) is not shareable (clause 3.2(3)(b) of Schedule 3). If a joint account holder requests the sharing of their customer data relating to a joint account, this request must be actioned as though it were a request in relation to an individually held account. Details of such data sharing must not appear on the dashboards of the other account holders.
Requester	A requester is the person who makes a consumer data request. This could be a joint account holder, or a secondary user.
Secondary user	A secondary user is a person who is not an account holder but who the account holder(s) have enabled to share data relating to their joint account.[5] See section 13 of this document for further information.

[4] See clause 1.4 of Schedule 3 of the rules for the meaning of phase 1, phase 2 and phase 3 products. See clause 6.6 of schedule 3 of the rules for the data sharing obligations timeline.
[5] Secondary users extend beyond joint accounts but are presented in this guidance in the joint account context only. For further information on secondary users, see r 1.7, r 1.15(5), r 4.6A and clause 2.1 of Schedule 3.

Disclosure option	A disclosure option determines the level of approval that is required before data relating to a joint account may be shared. Disclosure options are set at the account level. There are three types of disclosure options: • pre-approval option (this is the default option and is commonly called 'one to authorise') • co-approval option (commonly called 'two to authorise') • non-disclosure option (where joint account data cannot be disclosed). See section 5 for more information.
Approval	When a requesting joint account holder provides an authorisation for the disclosure of data on a joint account, the non-requesting joint account holders must each provide an approval in order for the data to be disclosed (noting that if a pre-approval option applies to the account, each relevant account holder is taken to have approved the disclosure). Data holders must allow non-requesting joint account holders to withdraw an approval to share their joint account data with a particular accredited person at any time.
Authorisation	When a requesting joint account holder wants to share CDR data from a joint account, they must provide an authorisation to the data holder. Once an authorisation is in place, approvals from all other joint account holders will also be needed for the data holder to make the disclosure.
Ordinary means of contacting an account holder	Throughout the joint account rules, there are requirements to notify consumers through the 'ordinary means of contacting them'. Rule 1.7 defines these ordinary means of contact as: • an agreed means of contact between the data holder and the account holder • otherwise, the data holder's default means of contacting the account holder. Some examples of the 'ordinary method for contacting a joint account holder' may include: • email • text message • online banking push notifications.

4. Eligibility and joint account sharing

4.1. In order to be able to share joint account data, all joint account holders must be 'eligible' consumers in their own right (r 1.7(1) and clause 2.1(2) of schedule 3). Each joint account holder must be aged 18 years or older and hold an account (either the joint account or another account) with the data holder that is open and accessible online.

Scenario 1a

Anna and Betty are both over 18 years old and hold a joint account with Bright Bank. Only Betty has access to the joint account online. Anna does not have any accounts with Bright Bank that she accesses online and is therefore not eligible. Neither Betty nor Anna can make requests for data sharing in relation to their joint account.

Scenario 1b

Anna and Betty are both over 18 years old and hold a joint account with Bright Bank. Only Betty has access to the joint account online. Anna also has a savings account with Bright Bank which is open and set up for online banking. Anna and Betty are both eligible consumers. Both Anna and Betty could request for data to be shared from their joint account (subject to other provisions of the rules).

5. Disclosure options and consumer oversight of joint account sharing

Disclosure options

5.1. The rules provide three disclosure options that can apply to joint accounts: the pre-approval, co-approval and non-disclosure options.

5.2. Data holders must offer joint account holders the pre-approval option and the non-disclosure option. The co-approval option is an optional implementation.

5.3. The pre-approval option means that data relating to a joint account can be independently shared by any requester.

5.4. A co-approval option is a more restrictive sharing preference. It means that all joint account holders must approve the disclosure of joint account data before it may be shared with the relevant accredited person.

5.5. The non-disclosure option is more restrictive still and means that joint account data cannot be disclosed.

5.6. While the pre-approval option applies by default, any joint account holder can independently select a more restrictive disclosure option to apply to the account (e.g. see Scenario 7). Conversely, all joint account holders must agree in order to apply a less restrictive disclosure option to a joint account. These changes are made using the disclosure option management service.

Disclosure option management service & changing the disclosure option

Key rules: Rules 1.15, 4A.6, 4A.7, 4A.8, 4A.13 and 4.A14

5.7. Data holders must provide an online disclosure option management service to each joint account holder that enables an account holder to indicate a disclosure option preference and, where necessary, respond to indications of other account holders. Data holders may include the disclosure option management service in the data holder dashboard.

5.8. The disclosure option management service and the data holder dashboard are the primary means by which data holders must provide visibility to consumers who have joint accounts. These functions should be prominently displayed and easily comprehensible for consumers.

5.9. Data holders must update the disclosure option management service as soon as practicable to give effect to:

- any disclosure option indicated by a joint account holder
- any changes to a disclosure option, and
- the withdrawal of a disclosure option.

Applying a more restrictive disclosure option

5.10. An individual joint account holder may use the disclosure option management service to apply a more restrictive disclosure option without needing the agreement of the other joint account holders (r 4A.6(1)(a) and r 4A.7). In other words:

- if the pre-approval option applies, an individual joint account holder can use the disclosure option management service to apply the co-approval option (if offered by the data holder) or non-disclosure option
- if the co-approval option applies, an individual joint account can use the disclosure option management service to apply the non-disclosure option.

The other joint account holders are not required to agree to the change.

5.11. If an individual joint account holder (account holder A) applies a more restrictive disclosure option, the data holder must contact the other account holders to (r 4A.7):

- explain to each of them what the consumer data right is
- inform them which disclosure option previously applied to the account
- inform them that account holder A has changed the disclosure option, and of the disclosure option that now applies
- explain how they can change the disclosure option again.

Applying a less restrictive disclosure option

5.12. An individual joint account holder may use the disclosure option management service to propose to apply a less restrictive disclosure option. The other account holders will need to agree to this proposal for that disclosure option to apply (r 4A.6(1)(a) and r 4A.8). In other words:

- if the non-disclosure option applies, an individual joint account holder can use the disclosure option management service to propose to apply the co-approval option (if offered by the data holder) or pre-approval option
- if the co-approval option applies, an individual joint account holder can use the disclosure option management service to propose to apply the pre-approval option.

The other joint account holders must agree to the proposal for the proposed disclosure option to apply.

5.13. Where an individual joint account holder (account holder A) makes a proposal to change to a less restrictive disclosure option, the data holder must contact the other joint account holders (r 4A.8(2)) and:

- explain to each of them what the consumer data right is

- inform them which disclosure option currently applies to the account
- inform them that account holder A has proposed that the co-approval or pre-approval option apply to the account, as the case may be
- explain that this change requires the agreement of all account holders
- explain any alternative options for change that are available and how they can be made
- invite them to either agree to or reject the proposal within a specified period.

5.14. The specified period of time should be consistent with time limits that apply to the data holder's equivalent non-CDR services and requests (e.g. where an account holder proposes to change authorities to transact on a joint account).[6] At the end of the specified period, the data holder must inform them whether (r 4A.8(3)):

- all the joint account holders have agreed to the change and so the proposed disclosure option applies, or
- not all the joint account holders have agreed to the change and so the proposed disclosure option will not apply.

Privacy tip:

When contacting the other joint account holders to explain the matters outlined in paragraph 5.13, we encourage data holders to also explain how each disclosure option operates in practical terms. This will assist the account holder to make an informed decision about their data sharing arrangements.

For example, where an account holder is electing to have a pre-approval option apply instead of the co-approval option, a data holder could explain to the joint account holder:

- what the pre-approval option means (i.e. that CDR data relating to the joint account will be able to be shared with only one joint account holder's approval), and
- how this differs from the disclosure option that currently applies (e.g. in a scenario where the co-approval option applies, that all joint account holders would be required to give approval before the relevant CDR data may be shared).

5.15. Note that the DSB has developed Consumer Experience Guidelines providing examples of how to implement requirements related to changing disclosure options for joint accounts. This includes an example flow for changing to a less restrictive disclosure option.[7]

Approval notifications

5.16. Data holders must provide an approval notification to each relevant joint account holder if (r 4A.14):

---

[6] Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021, Explanatory Statement: page 27, paragraph 3.

[7] Joint account disclosure option management service Consumer Experience Guidelines, Data Standards Body

- a requester gives, amends or withdraws an authorisation associated with a joint account
- an authorisation associated with a joint account expires
- a joint account holder does not provide an approval to disclose joint account data within a specified timeframe or withdraws an approval.

5.17. Data holders must provide notifications through their ordinary means for contacting the joint account holders (r 4A.14(2)(b)).

5.18. Data holders must make notifications as soon as practicable, unless a joint account holder has selected an alternative schedule of notifications (r 4A.14(2)(a)). Data holders must allow joint account holders to select alternative notification schedules and, once selected, must provide notifications in accordance with these schedules (r 4A.14(3)). This may include, for example, weekly, fortnightly or monthly bulk approval notifications, or not receiving notifications at all.[8] Data holders must also give joint account holders the option to change such a selection at any time (r 4A.14(3)(b)).

5.19. Note that the DSB has developed Consumer Experience Guidelines providing examples of how to implement requirements for providing alternative notification schedules.[9]

Consumer dashboards

5.20. Data holders must provide a consumer dashboard to joint account holders where either the pre-approval option or co-approval option applies, or has applied, to a joint account (r 4A.13(1)(b)). Where a data holder already provides a consumer dashboard to a joint account holder under r 1.15, the existing dashboard must also serve as the dashboard for the joint account (r 4A.13(2)). The dashboard must:

- allow non-requesting joint account holders to manage approvals in relation to each authorisation to disclose joint account data, including providing functionality to withdraw these approvals (r 4A.13(1)(d))
- as part of the process of withdrawing approvals, display a message relating to the consequences of the withdrawal in accordance with the data standards (r 4A.13(1)(d)(v))
- contain details of each authorisation to disclose CDR data, including (r 4A.13(1)(c)):
    - the CDR data that has been authorised to be disclosed, when it was disclosed and the name of the accredited data recipient to whom it was disclosed
    - the timing and period of the authorisation
    - if the authorisation is current, when it is scheduled to expire
    - if the authorisation is not current, when it expired.

[8] Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021, Explanatory Statement: page 26, paragraph 5.
[9] Joint account notification settings Consumer Experience Guidelines, Data Standards Body

5.21. If an account holder's dashboard contains details of approvals in relation to a particular joint account, the dashboards of the other joint account holders on that account must also contain those details (r 4A.13(5)).

5.22. Dashboards for requesting joint account holders must also contain functionality to manage authorisations.[10] Where a dashboard is already provided to a CDR consumer under r 1.5, r 4A.13(2) requires joint account functionality to be included in the same dashboard.

Accredited persons

5.23. At this stage, data holders are not required to inform accredited persons when disclosure options apply, or when approvals are given or withdrawn. Additional data standards may be introduced in future that require notification to accredited persons where accounts are associated or disassociated from an authorisation.

5.24. However, data holders are required to notify accredited persons where an authorisation to share data is withdrawn, see Scenario 5.

6. Pre-approval option – the default disclosure option

Key rules: Version 3 amending instrument, schedule 7

6.1. If the pre-approval option applies to a joint account, each relevant account holder is taken to have approved any disclosure requested by another account holder and the relevant data holder must make the requested disclosure in accordance with rules 4.5 – 4.7 (see r 4A.5(4)(a) and r 4A.10).

Default application of the pre-approval option for major ADIs

6.2. A major ADI may elect to comply with the version 1 joint account rules until 1 July 2022. In this situation the following will apply from 1 July 2022:

- if a disclosure option has never previously applied to a joint account, the pre-approval disclosure option will apply
- if the pre-approval or co-approval applies to a joint account, the same disclosure option will apply
- if a disclosure option previously applied to the joint account but was removed so that no CDR could be disclosed from the account, the non-disclosure option will apply from 1 July 2022.[11]

6.3. If a major ADI implements the version 3 joint account rules prior to 1 July 2022, the above will apply from the day the bank implements those rules.

[10] See for example, r 1.15.

[11] For clarity:

- under the version 1 and version 2 rules, if the 'pre-approval' or 'co-approval' options did not apply to the account, no disclosure option would apply meaning no data could be shared
- the version 3 rules introduced the 'non-disclosure' option and this is equivalent to the situation where no disclosure option applied under the version 1 and 2 rules.

Default application of the pre-approval option for non-major ADIs

6.4. A non-major ADI may elect to implement the version 3 joint account provisions before 1 July 2022.[12] In this scenario the pre-approval option applies on the day the bank implements the version 3 joint account rules.

6.5. If a non-major ADI **has not** elected to implement the version 3 joint account provisions earlier than 1 July 2022, the pre-approval option applies to joint accounts from 1 July 2022.

Default application of the pre-approval option for new joint accounts

6.6. The pre-approval option will apply by default to new joint accounts that are established while a data holder is complying with the version 3 joint account provisions.

6.7. While it is not a requirement in the rules, to promote transparency we encourage data holders to notify relevant consumers that the pre-approval option will apply by default to their joint account. This notification could also include an explanation of what this means, and instructions for how to change the disclosure option.

6.8. This notification could be provided through the data holder's ordinary means of contacting each joint account holder, and:

(a) for existing joint account holders, be given a reasonable period before the data holder is required to (or has elected to) comply with the V3 joint account provisions, and

(b) for new customers, at the time of opening a joint account.

Scenario 2a: Early compliance by a Major ADI

A Major ADI has elected to comply with the version 1 joint account provisions until 1 July 2022. Yianni and Dimitra have a joint account with the Major ADI but have not yet chosen a disclosure option. The Major ADI revokes its election by implementing the new Part 4A provisions on and from 1 April 2022. The pre-approval option will apply by default to Yianni and Dimitra's account on and from 1 April 2022.

Scenario 2b: No early compliance by a non-major ADI

Mark and Abdul have a joint account with Bene Bank, a non-major ADI. Bene Bank has not made an election to comply with Part 4A prior to 1 July 2022. The pre-approval option will apply by default to Mark and Abdul's joint account on and from 1 July 2022.

Scenario 2c: Major ADI complying with version until 1 July 2022

A Major ADI has made an election to comply with version 1 of the joint account provisions until 1 July 2022. Sarah and Ying have a joint account with the Major ADI and have applied the co-approval option. The Major ADI does not revoke its election prior to 1 July 2022. The co-approval option will continue to apply to Sarah and Ying's joint account on and from 1 July 2022.

[12] No formal process is needed to make this election, the DH may simply commence implementing the JA provisions in accordance with the version 3 rules. See also Schedule 7 of the Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021.

6.9. Note that the Data Standards Body has developed Consumer Experience Guidelines providing examples of how to implement the authorisation flow in relation to joint accounts. The Guidelines include an example authorisation flow where the pre-approval option applies to a joint account.[13]

7. Offline disclosure option management service (optional implementation)

Key rules: Rules 4A.5, 4A.6 and 4A.7

7.1. Data holders must provide a disclosure option management service online and may also offer the service offline (r 4A.6(4)). A data holder must update the disclosure option management service as soon as practicable to give effect to a disclosure option applying or not applying (r 4A.6(5)). Consequently, if a data holder offers an offline disclosure option management service and a disclosure option is indicated in the offline service, the data holder must update the online disclosure option management service to reflect the indicated disclosure option as soon as practicable.

Scenario 3: How consumers may use the disclosure option management service offline

Patty, Fred and Carlos have a home loan with Super Loans where the pre-approval option applies by default. Carlos wants to change to the non-disclosure option, so he attends the local Super Loans branch. Carlos tells a Super Loans staff member that she would like the non-disclosure option to apply to her home loan account rather than the pre-approval option.

Despite not being a requirement, Super Loans provides an offline disclosure option management service by allowing their customers to choose a disclosure option in person.

The staff member processes Carlos' request so that the non-disclosure option applies to the loan account.

Super Loans updates the online disclosure option management services for Patty, Fred and Carlos to indicate the non-disclosure option applies to the account. As Super Loans includes the disclosure option management service in the consumer dashboard, this update is reflected in Patty, Fred and Carlos' consumer dashboard. Super Loans also provides Patty, Fred and Carlos with the notification referred to in paragraph 5.11 of this guidance.

[13] Authorisation to disclose joint account data Consumer Experience Guidelines, Data Standards Body

8. Co-approval (optional implementation)

Key rules: Rules 4A.5, 4A.6, 4A.10 and 4.A11

8.1. Data holders may offer a co-approval disclosure option as well as a pre-approval option (r 4A.5(3)). Where the co-approval option applies to a joint account and a joint account holder has authorised the disclosure of CDR data for the account, the data holder must seek the other account holders' approval before disclosing data from the account. The data holder must inform the other account holders of the matters referred to in r 4A.11, including the time allowed for them to provide the approval. This time must be reasonable and should be consistent with time limits that apply to the data holder's non-CDR services and requests (e.g. the time allowed for a joint account holder to authorise a transaction on a 'both to sign' joint account).[14]

> **Scenario 4: How consumers indicate a co-approval option and authorise data sharing**
>
> Perry and Candice hold a joint transaction account with Easy Credit Union. Candice also holds a savings account with Easy Credit Union. Candice decides she wants to share data from both accounts with Go-Budget and goes through the consent and authorisation processes successfully. A co-approval option applies to Perry and Candice's joint account. This means that CDR data cannot be shared for the joint account unless Perry gives his approval for the disclosure of the joint account data from Easy Credit Union to Go-Budget. While Easy Credit Union waits for Perry to approve or deny the disclosure, it must disclose the data it has authorisation to disclose on Candice's savings account.

8.2. Note that the Data Standards Body has developed Consumer Experience Guidelines showing examples for how to implement the authorisation flow in relation to joint accounts. The guidelines include an example authorisation flow where the co-approval option applies to a joint account.[15]

9. Stopping sharing joint account data & the non-disclosure option

Key rules: Rules 1.15(1)(c)(i) and 4.25; rules 4A.5, 4A.6, 4A.10, 4A.12 and 4A.14

9.1. Sharing in relation to a joint account may cease for the following reasons:

- the requester has withdrawn the relevant **authorisation**
- a joint account holder has withdrawn the relevant **approval**
- a joint account holder has indicated they would like the non-disclosure option to apply
- as a result of another provision of the rules. For example, an authorisation expires (r 4.26) or a consumer ceases to be 'eligible'.[16]

---

[14] Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021, Explanatory Statement: page 27, paragraph 3.

[15] Authorisation to disclose joint account data Consumer Experience Guidelines, Data Standards Body

[16] For the definition of an 'eligible' CDR consumer in the banking sector, see r 1.10B(1) (introduced in the version 4 rules) and clause 2.1 of Schedule 3 to the rules.

Withdrawing an authorisation – stop sharing all data with a particular accredited person

9.2. A requester may withdraw an authorisation to disclose CDR data to a particular accredited person at any time.

9.3. A requester may withdraw their own authorisations, but they cannot withdraw the authorisations given by other account holders or secondary users.

9.4. Where a joint account holder withdraws an authorisation:

- data sharing from the joint account under the authorisation must cease, along with data being shared from any other account that is associated with that authorisation (r 4.25)
- consumer dashboards must be updated to reflect the withdrawal (r 1.15 and r 4A.13(1)(c))
- the data holder must notify joint account holders that the authorisation has been withdrawn through its ordinary means of contacting them (r 4A.14(1))
- the data holder must notify the accredited person that the authorisation has been withdrawn, in accordance with the data standards (r 4.25).

Scenario 5: withdrawing an authorisation – continuation of scenario 4

A co-approval disclosure option applies to Candice and Perry's joint transaction account with Easy Credit Union. Candice authorised the disclosure of data to Go-Budget associated with:

- her joint transaction account with Perry
- her savings account held in her name alone.

Perry also approved the disclosure of joint account data to Go-Budget.

Candice decides she no longer wants to share her data with Go-Budget. She withdraws her authorisation to disclose data with Easy Credit Union. Easy Credit Union:

- stops disclosing data on the joint account and her savings account
- sends Perry an email, notifying him that Candice has withdrawn her authorisation to share the joint account data with Go-Budget (see r 4A.14 and paragraph 9.4 of this guidance)
- updates the consumer dashboards accordingly (see r 4.27, r 4A.13 and paragraph 9.4 of this guidance)
- notifies Go-Budget of the withdrawal of authorisation (see r 4.25(2)(b) and paragraph 9.4 of this guidance).[17]

[17] This will trigger additional obligations for Go-Budget, see r 4.14 and r 4.18A.

Withdrawal of approvals – stop sharing joint account data with a particular accredited person

9.5. Non-requesting joint account holders must be allowed to withdraw an approval in relation to each authorisation to disclose joint account data. This applies regardless of whether there is a pre-approval or a co-approval disclosure option on the account. Withdrawing an approval means the data holder will stop sharing the joint account data in relation to the corresponding authorisation, it will not stop sharing joint account data in relation to other authorisations.

9.6. Data holders may also choose to offer functionality that allows an individual joint account holder to re-add their own approvals to share data on a joint account (e.g. where the account holder mistakenly removed the approval), where an authorisation and disclosure option are in place. This is not regulated in the rules, so is optional.

9.7. Where a joint account holder withdraws an approval:

- data from the joint account must no longer be shared with that particular accredited person, however data from any other accounts associated with the authorisation may continue to be shared[18] (r 4A.10)
- the data holder must notify the other joint account holders that the approval has been withdrawn through its ordinary means of contacting them (r 4A.14)
- the data holder must update the consumer dashboards accordingly (r 4A.13).

9.8. Where multiple approvals are in place with a single accredited person,[19] withdrawing an approval will only impact the data sharing from the joint account relevant to that particular approval.

[18] Whether the data holder must continue to share a consumer's CDR data from other accounts, or is merely authorised to do so, will depend on whether the CDR data is 'required consumer data' (which must be shared) or 'voluntary consumer data' (which may be shared). See r 4.6.
[19] For example, where the accredited person utilises concurrent consents or has multiple software products.

Scenario 6: Withdrawal of an approval – continuation of scenario 4

A co-approval disclosure option applies to Candice and Perry's joint transaction account with Easy Credit Union. Candice authorised the disclosure of data to Go-Budget associated with:

- her joint transaction account with Perry
- her savings account held in her name alone.

Perry also approved the disclosure of joint account data to Go-Budget.

Perry decides that he no longer wants data on the joint account to be shared with Go-Budget. He withdraws his approval of this data sharing via his consumer dashboard.[20]

Easy Credit Union:

- no longer discloses data from Perry and Candice's joint account with GoBudget, but continues to disclose the joint account data to other accredited persons who Perry and Candice have sharing arrangements with
- continues to disclose Candice's savings account data to Go-Budget
- sends Candice an email, notifying her that Perry has withdrawn the approval to share data with Go-Budget on the joint account (see r 4A.14 and paragraph 9.7 of this guidance)
- updates the consumer dashboards accordingly (see r 4.27, r 4A.13 and paragraph 9.7 of this guidance).

9.9. Note that the DSB has developed Consumer Experience Guidelines showing examples of how to implement the data holder authorisation withdrawal process.[21]

Applying the non-disclosure option – stop sharing the joint account data with <u>all</u> accredited persons

9.10. Any joint account holder may independently apply the non-disclosure option by using the disclosure option management service (r 4A.6 and r 4A.7).

9.11. Where the non-disclosure option is applied:

- data from the relevant joint account must not be shared with any accredited person
- the data holder must notify the other joint account holders that a joint account holder has applied the non-disclosure option to the account (r 4A.7(3))

[20] If a pre-approval disclosure option applied in this scenario, Perry could also withdraw his approval, even though the approval is automatically applied where a pre-approval disclosure option applies to the account.

[21] Withdrawal Consumer Experience Guidelines, Data Standards Body

- the data holder must update the disclosure option management service accordingly (r 4A.6(5)).

9.12. Where the disclosure option management service is not incorporated into the consumer dashboard (as is authorised by r 4A.6(3)), data holders are encouraged to ensure consumer dashboards also inform consumers why data on a joint account is not being shared.

Scenario 7: Applying the non-disclosure option – continuation of scenario 4

A co-approval disclosure option applies to Candice and Perry's joint transaction account with Easy Credit Union. Candice authorised the disclosure of data to Go-Budget associated with:

- her joint transaction account with Perry
- her savings account held in her name alone.

Perry also approved the disclosure of joint account data to Go-Budget.

Perry accidentally applies the non-disclosure option to the joint account.

Easy Credit Union:

- emails Candice, notifying her that Perry has applied the non-disclosure option and of the matters referred to in paragraph 5.11 of this guidance
- does not disclose data from Perry and Candice's joint account with Go-Budget, or any other accredited person
- continues to disclose Candice's savings account data to Go-Budget
- updates the disclosure option management service accordingly.

Perry, realising his mistake, later indicates his preference for a co-approval disclosure option again.

Easy Credit Union therefore emails Candice, inviting her to indicate the same disclosure option (r 4A.8).

If Candice indicates the same disclosure option, Easy Credit Union must:

- from the date and time of the co-approval option being indicated by Candice, reinstate all sharing from Perry and Candice's joint account where authorisations are still current
- update the disclosure option management service accordingly.

9.13. Where data holders reinstate sharing after a disclosure option has been amended, the disclosure option management service and consumer dashboard will provide consumers with an overview of sharing arrangements in place. However, data holders may choose to provide additional notifications to consumers if desired.

9.14. Note that the DSB has developed Consumer Experience Guidelines providing examples for how to implement requirements relating to changing disclosure options

for joint accounts. The guidelines include an example flow for applying the non-disclosure option.[22]

10. Alerts concerning notifications to other account holders

10.1. If an account holder (account holder A) intends to perform an action that may trigger a notification to other account holders, data holders must alert account holder A of this fact.[23] The precise wording of the notification to account holder A is at the discretion of the data holder.

11. Approach to vulnerable consumers

Key rules: Rule 4A.15

Exceptions to data holder obligations

11.1. We strongly encourage data holders to develop and implement processes to protect vulnerable consumers. The rules provide that a data holder will not be liable for a failure to comply with Part 4A where it considered an act or omission was necessary to prevent physical, psychological or financial harm or abuse to any person (r 4A.15). Robust internal frameworks for identifying vulnerable consumers will assist a data holder to make an informed decision as to whether it is appropriate to rely on the exceptions in the rules.

11.2. For example, data holders will not be liable for failing to undertake the following actions if they consider it necessary to prevent physical, psychological or financial harm or abuse:

- if the non-disclosure option is in place – invite relevant account holder(s) to choose a disclosure option before disclosing data on the joint account (which is ordinarily required under r 4A.8)
- where a co-approval disclosure option is in place - to seek the approval of the relevant account holder(s) before disclosing data on the joint account (which is ordinarily required under r 4A.10(4))
- to provide a relevant account holder(s) with a dashboard or to update an existing dashboard with details regarding a joint account (which is ordinarily required under r 4A.13)
- to give approval notifications to a joint account holder(s) (which is ordinarily required under r 4A.14)
- to seek an authorisation to disclose data (r 4.7)
- to disclose data (r 4.7).

11.3. It is important to note that a joint account holder or secondary user cannot share the customer data of another person. The rules ensure that customer data, including

[22] Joint accounts disclosure option management service Consumer Experience Guidelines, Data Standards Body

[23] Notification Standards, Joint account notifications: Contextual alert, Consumer Data Right Consumer Data Standards, Data Standards Body

personal information, cannot be shared unless it is the customer data relating to the person making the request.[24]

Identifying vulnerable consumers

11.4. Data holders may have existing processes for identifying vulnerable consumers which may assist in identifying whether the exception in r 4A.15 applies. If a consumer has previously been identified as vulnerable or at risk of harm, the data holder may be able to rely on that identification in the CDR context where they are satisfied that an act or omission would be necessary to prevent physical, psychological or financial harm or abuse to any person. Relying on existing processes may remove the need for consumers to re-identify as vulnerable.

11.5. In order to ensure there are no repercussions for consumers identified as vulnerable, data holders should issue generic error codes when joint account data is not shared in order to protect vulnerable consumers. The data holder can use a range of standardised error codes to provide a general error to the ADR without disclosing the nature of the refusal (for example, "Invalid Banking Account", "Unavailable Banking Account", "Consent Is Invalid" and "Expected Error Encountered"). Data Holders should choose appropriate error codes based on the applicable error codes for the data being requested in accordance with the Data Standards.

11.6. The ACCC recognises that data holders may refuse to share data from a joint account in the following situations where the data holder considers it necessary in order to prevent physical, psychological or financial harm or abuse to any person:

- where a consumer has chosen to delink an account from their digital profile
- where a consumer has chosen to use a silent account digitally.

11.7. Note that the DSB has developed Consumer Experience Guidelines providing examples for how to implement the authorisation flow in relation to joint accounts. This includes a sample authorisation flow where r 4A.15 is leveraged to allow a vulnerable account holder to share their joint account data as if it were an individual account.[25]

12. Approach for multiple joint accounts

Key rules: Rules 4A.6, 4A.7, 4A.8, 4A.11 and 4A.14

12.1. Where a consumer holds multiple joint accounts with a data holder, the data holder may enable the consumer to indicate disclosure option preferences in a streamlined process. For example, a data holder may allow consumers to select multiple accounts and apply a disclosure option to all the selected accounts.

12.2. Similarly, data holders may provide notifications to joint account holders in streamlined formats. For example, a data holder may ask the other joint account holders to indicate a disclosure option preference (as discussed at paragraph 5.12-5.14 of this guidance) for multiple accounts through a single notification.

12.3. Data holders must ensure their processes and messaging is compliant with the rules, including the prohibition on pre-selected options (see r 4.11(2)).

---

[24] An exception to this is where a person is acting under a power of attorney on behalf of a CDR consumer.

[25] Authorisation to disclose joint account data Consumer Experience Guidelines, Data Standards Body

13. Approach to secondary users

Key rules: Rules 1.13(1)(e) 4A.6, 4A.14

13.1. A person is a secondary user for an account if:

- the person has account privileges in relation to the account; and
- a secondary user instruction has been given to the data holder to treat the person as a secondary user.

Making or revoking a secondary user instruction

13.2. A data holder must provide a service that can be used by an account holder to make and withdraw secondary user instructions (see r 1.13(1)(e) and r 1.15(5)). Data holders have some flexibility as to the specific functionality of the service to make a secondary user instruction. For example, whether a pre-approval or a co-approval disclosure option applies, data holders may allow joint account holders to independently provide secondary user instructions, or may require the instruction of all account holders before a secondary user instruction can be made. Data holders must allow a joint account holder to individually withdraw a secondary user instruction (whether or not the joint account holder made the secondary user instruction).

13.3. Note that the DSB has developed Consumer Experience Guidelines providing examples for how account holders may change the sharing rights for other account users, including by withdrawing a secondary user instruction.[26]

General operation of secondary users and joint accounts

13.4. Once a secondary user instruction is in place, the secondary user rules generally operate as if the secondary user is also a joint account holder. That is:

- if a pre-approval option applies to the joint account, secondary users can independently authorise the sharing of data on the joint account, creating an approval as they do so. Oversight is provided to the joint account holders through notifications and the consumer dashboard.
- if a co-approval option applies to the joint account, a data holder must seek the approval of all joint account holders before data from the joint account may be shared.

13.5. However, a secondary user has a subordinate status to account holders on the joint account. A secondary user does not have oversight of sharing by the account holders or input into the disclosure option that applies to a joint account. This means that in their consumer dashboards, secondary users only have oversight of sharing they themselves have initiated on the joint account.

[26] Secondary users Consumer Experience Guidelines, Data Standards Body