Australian Government

Consumer Data Right

CDR and joint accounts

Australian Competition and Consumer Commission

Guidance

Version 6

September 2026

Contents

1. Joint accounts and CDR

This guide gives data holders in the banking and energy sectors an overview of the Consumer Data Right (CDR) rules on joint accounts.

A joint account is an account with a data holder for which there are 2 or more joint account holders, each of which is an individual who is acting in their own capacity and is eligible in relation to the data holder.[1]

Note that partnership accounts are different from joint accounts.[2]

There is no requirement that the name of a joint account include the words 'joint account'. It is enough that it has the characteristic of a joint account; that is, there are 2 or more named owners.

The CDR Rules include specific rules about how joint account holders can authorise and approve CDR data sharing.

---

[1] See Competition and Consumer (Consumer Data Right) Rules 2020 (CDR Rules), rule 1.7(1), for definitions.

[2] For more information about sharing data from partnership accounts, see the Nominated representatives of non-individuals and partnerships in CDR fact sheet.

2. Application of joint account rules by sector

Start dates and application of the CDR Rules for joint account data sharing vary by sector.

2.1 Banking sector

A data holder in the banking sector must support consumer data sharing for all in-scope joint accounts. An entity that becomes an unrestricted authorised deposit-taking institution (ADI) must support consumer data sharing for joint accounts no later than 18 months of becoming an unrestricted ADI.[3]

> **More information**
>
> More information on what is in scope is available in Assessing whether a banking or non-bank lending product is in scope for CDR.

2.2 Energy sector

Initial retailers and larger retailers in the energy sector must support consumer data sharing for joint accounts.[4]

Small retailers in the energy sector have data sharing obligations only if they become accredited by the CDR Accreditor – the Australian Competition and Consumer Commission (ACCC) – or voluntarily participate in CDR.[5] A small retailer that voluntarily participates must notify the ACCC's CDR team at accc-cdr@accc.gov.au of the date it will begin participating. A small retailer that becomes an accredited person must support consumer data sharing for joint accounts within 18 months of becoming an accredited person.[6]

> **More information**
>
> Information about whether an energy retailer is an initial, larger or small retailer is provided in CDR compliance for energy sector data holders.

2.3 Non-bank lenders sector

A data holder in the non-bank lenders sector is not currently required to respond to a request that relates to a joint account, or to provide the services needed to respond to such a request.[7] This is because data sharing obligations in relation to complex requests (which include requests that relate to joint accounts) do not currently apply to data holders in the non-bank lenders sector.[8]

---

3 CDR Rules, Schedule 3, clause 6.9(2)(c) states that an entity that becomes an unrestricted ADI after 4 March 2025 must respond to complex requests 18 months after becoming an unrestricted ADI. Clause 6.1 sets out the meaning of complex request, which includes a consumer data request that relates to a joint account.

4 CDR Rules, Schedule 4, clause 8.6 sets out relevant obligation dates for complex requests, which include a consumer data request related to a joint account. See clauses 8.2 and 8.3 for meanings of initial retailer and larger retailer.

5 CDR Rules, Schedule 4, clause 8.6(8)-(9). See also the *Competition and Consumer Act 2010* (Cth), section 4 for the meaning of 'accredited person'.

6 CDR Rues, Schedule 4, clause 8.6(8). Clause 8.1 defines a complex request to include a consumer data request that relates to a joint account.

7 These services are referred to in rules 4A.6 and 4A.13 of the CDR Rules.

8 CDR Rules, Schedule 3, clauses 6.4(2) and 6.5(4). A complex request means a consumer data request that is made on behalf of a secondary user, or relates to a joint account or partnership account, or is made on behalf of a CDR consumer who has a nominated representative (see clause 6.1). For more information, see Assessing whether a non-bank lender has CDR obligations.

3. Eligibility and joint account data sharing

To share joint account data, each joint account holder must be an individual and an eligible CDR consumer in relation to the data holder.[9]

3.1 Eligibility in the banking sector

In the banking sector, to be an ‘eligible CDR consumer’, a joint account holder must:[10]

- be aged 18 years or older, and
- hold an open account with the data holder; this may be the joint account or another account, and must be accessible online.

Each joint account holder must be eligible before joint account data can be shared.

Example - online access scenario 1

Anna and Benni are both over 18 years old and hold a joint account with Bright Bank.

Only Benni has online access to the joint account. Anna has never registered for online banking with Bright Bank, so does not have online access to the joint account or any other account with Bright Bank. Therefore, Anna is not an eligible CDR consumer for Bright Bank.

Because both joint account holders must be eligible CDR consumers for the account to be available for CDR data sharing, neither Benni nor Anna can make requests to share data from the joint account.

Example - online access scenario 2

Chen and Dan are both over 18 years old and hold a joint account with Bright Bank.

Only Chen has access to the joint account online, because Dan has not set up online access for that account. Dan has a separate savings account with Bright Bank, which is open and set up for online banking.

Chen and Dan each meet the eligibility requirements, so the account is available for CDR data sharing. Either account holder could request that data be shared from their joint account (subject to other provisions of the CDR Rules).

3.2 Eligibility in the energy sector

In the energy sector, to be an eligible CDR consumer a joint account holder must:

- be aged 18 years or older
- hold an open account with the data holder
- be a customer of a retailer and hold an account that relates to an eligible arrangement, which is an arrangement that relates to one or more connection points or child connection points for which there is a financially responsible market participant in the National Electricity Market, and

9 CDR Rules, rule 1.7(1).

10 CDR Rules, rule 1.7(1) and Schedule 3, clause 2.1.

- have energy consumption associated with their account that is:
  - less than 5 GWh over the previous 12 months, or
  - estimated to be less than 5 GWh annually, if the account has been in existence for less than 12 months.[11]

It is not a requirement in the energy sector that the account be accessible online.

Each joint account holder must be eligible before joint account data can be shared.

Example – eligibility

Winnie and Ella hold an open joint account with Tiger Energy, a large energy retailer. The account relates to an eligible arrangement. Energy consumption is below the threshold set in the CDR Rules. Winnie is 18 years old and Ella is 17 years old.

Since Ella is not aged 18 years or older, she is not an eligible CDR consumer. Therefore, neither account holder can share CDR data from the joint account.

When Ella turns 18, she will become an eligible CDR consumer if the other eligibility criteria are met. Tiger Energy must then make the relevant joint account available for data sharing. Either Winne or Ella could request that data be shared from the joint account. This could include data generated before Ella turned 18 (subject to other requirements in the CDR Rules).

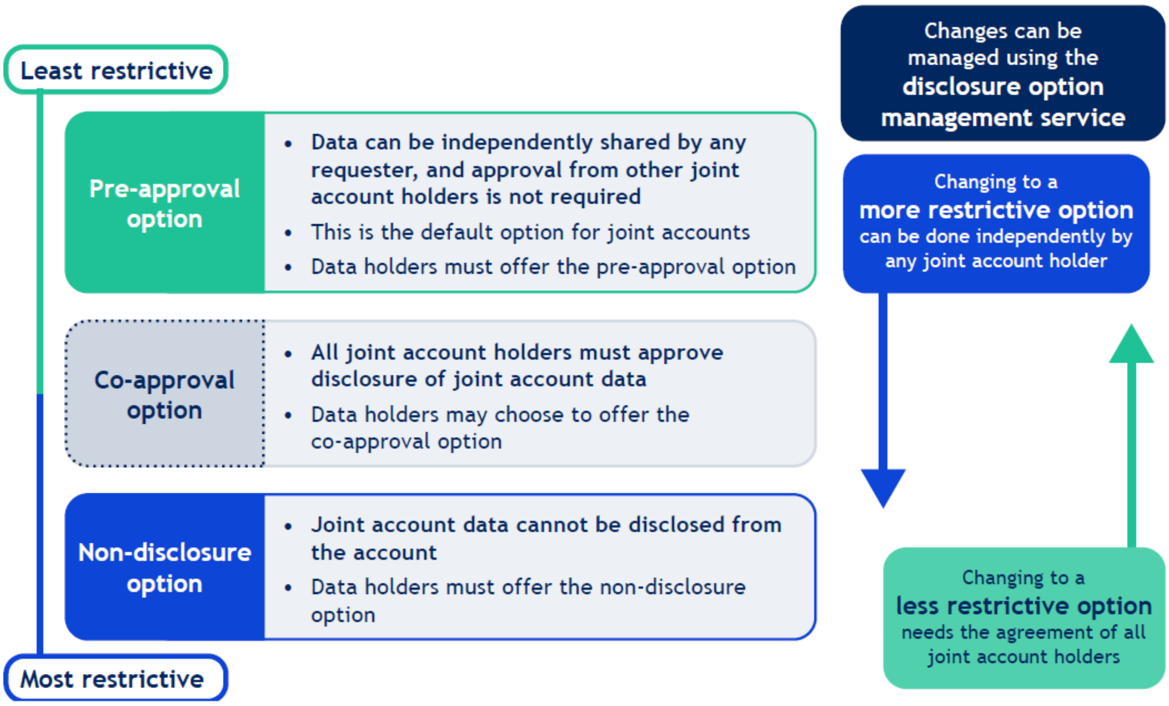
[11] CDR Rules, rule 1.7(1) and Schedule 4, clause 2.1.

4. Disclosure options for joint accounts

Three disclosure options can apply to joint accounts – pre-approval, co-approval and non-disclosure.[12]

These are summarised in Figure 1.

Figure 1 Overview of disclosure options for joint accounts



The disclosure option applied to an account dictates how a data holder must respond to a consumer data request made on behalf of a requester. A requester is the person on whose behalf a consumer data request is made.[13] This could be a joint account holder or a secondary user.

A data holder must offer joint account holders the pre-approval option and the non-disclosure option. It may choose whether to offer the co-approval option.[14]

Any account holder can make changes to disclosure options by using the disclosure option management service (see Section 7.1).

If a data holder provides a consumer dashboard to joint account holders, the disclosure option management service may be provided via the dashboard. Section 7.2 explains when a dashboard must be provided, and what information and functionality it must contain.

[12] CDR Rules, rule 4A.5(1).

[13] CDR Rules, rule 4A.3.

[14] CDR Rules, rule 4A.5(3).

More information

Examples of authorisation flows for the pre-approval and co-approval options that can be selected for a joint account are given in the Consumer Experience (CX) Guidelines on Authorisation to disclose joint account data.

While not specific to joint accounts, data holders can refer to the CX Guidelines for Authorisation to disclose: Unavailable account for examples of authorisation flows for the non-disclosure option.

4.1 Pre-approval option

The pre-approval option applies by default to joint accounts. It allows any account holder to request disclosure of data from the account without approval from the other joint account holders.[15]

The ACCC recommends data holders notify relevant consumers that the pre-approval option will apply by default to their joint account. This notification could be provided through the data holder's ordinary means of contacting each joint account holder (see Section 7.3.1). The notification could also explain what the option means and give instructions for changing the disclosure option.

4.2 Co-approval option

If the co-approval option applies to a joint account and one account holder authorises a disclosure of data, the data holder must seek and receive approval from every other account holder before disclosing the data.

The data holder must inform the other account holders of the matters referred to in rule 4A.11, including the time allowed for them to provide the approval.

[15] In accordance with CDR Rules, rules 4.5 to 4.7 and rules 4A.5(4)(a) and 4A.10.

Example – co-approval and authorisation

Hope holds a savings account with Easy Credit Union. She also holds a joint transaction account at Easy Credit Union with Gian. Gian applied a co-approval option to the joint account using the disclosure option management service.

Hope wants to share data from both accounts with Go-Budget. She completes the consent and authorisation processes.

Easy Credit Union must disclose whatever data on Hope's savings account it has authorisation to disclose.

However, the co-approval option on the joint account means Gian's approval is needed to share data from the joint account. Easy Credit Union must invite Gian to approve the data sharing request within a specified time. It cannot disclose the data on the joint account until Gian approves it.

4.3 Non-disclosure option

When 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,[16] and
- the data holder must update the disclosure option management service (see Section 7.1) to reflect the change as soon as practicable.[17]

The disclosure option management service may be included in the consumer dashboard.[18] Even if the disclosure option management service is not part of the consumer dashboard, the ACCC recommends the data holder still update the dashboard with information about why data is not being shared.

4.4 Stopping the sharing of data

Sharing of data for a joint account must cease if:

- a joint account holder has applied the non-disclosure option (see Section 4.3)
- a joint account holder who has authorised a specific data sharing arrangement (the requester) has withdrawn the relevant authorisation, or
- a non-requesting joint account holder has withdrawn the relevant approval.

Data sharing may also be stopped when another provision of the CDR Rules applies – for example, an authorisation expires[19] or a consumer ceases to be eligible.[20]

---

[16] CDR Rules, rule 4A.7(3).

[17] CDR Rules, rule 4A.6(5).

[18] This is authorised by rule 4A.6(3).

[19] CDR Rules, rule 4.26.

[20] For the definition of an eligible CDR consumer in the banking sector, see CDR Rules, rule 1.10B(1) and Schedule 3, clause 2.1. For the definition of an eligible CDR consumer in the energy sector, see CDR Rules, rule 1.10B(1) and Schedule 4, clause 2.1.

5. Withdrawing an authorisation

The requester can withdraw an authorisation to disclose CDR data to a specified accredited person at any time. However, they cannot withdraw authorisations given by other account holders or secondary users.

If a joint account holder withdraws their authorisation:

- data sharing from any account associated with that authorisation, including the joint account, must cease[21]
- consumer dashboards must be updated to reflect the withdrawal[22]
- the data holder must notify joint account holders, through its ordinary means of contacting them, that the authorisation has been withdrawn,[23] and
- the data holder must notify the accredited person that the authorisation has been withdrawn, in accordance with the Consumer Data Standards.[24]

Example – withdrawing an authorisation

From the example in Section 4.2, Hope holds a joint transaction account at Easy Credit Union with Gian. Hope also holds a savings account with Easy Credit Union. Gian applied a co-approval option to the joint account using the disclosure option management service.

Hope authorised the disclosure to Go-Budget of data associated with:
- her joint transaction account with Gian
- the savings account held in her name alone.

Gian approves the disclosure of joint account data to Go-Budget in relation to that authorisation, allowing data to be shared.

Hope wants to stop sharing data with Go-Budget. She uses the Easy Credit Union consumer dashboard to withdraw her authorisation to disclose data. Easy Credit Union must:
- stop disclosing data on the joint account and on Hope’s savings account
- notify Gian that Hope has withdrawn her authorisation to share the joint account data with Go-Budget[25]
- update the consumer dashboards to reflect the change[26]
- notify Go-Budget of the withdrawal of the authorisation.[27]

21 CDR Rules, rule 4.25.

22 CDR Rules, rules 1.15, 4.27 and 4A.13(1)(c).

23 CDR Rules, rule 4A.14(1).

24 CDR Rules, rule 4.26A.

25 CDR Rules, rule 4A.14.

26 CDR Rules, rules 4.27, 1.15 and 4A.13(1)(c).

27 CDR Rules, rule 4.26A. This will trigger additional obligations for Go-Budget – see CDR Rules, rules 4.14 and 4.18A.

5.1 Withdrawing an approval

A data holder must allow a non-requesting joint account holder to withdraw an approval for each authorisation to disclose joint account data on an account that has a pre-approval or co-approval disclosure option applied.[28]

If a joint account holder withdraws an approval, the data holder:

- must stop sharing data from the joint account under that authorisation
- may continue to share data from other accounts (such as individual accounts) associated with the authorisation[29]
- must notify the other joint account holders, using its ordinary means of contacting them, that the approval has been withdrawn[30]
- must update the consumer dashboards to reflect the withdrawal.[31]

If several approvals are in place in relation to authorisations with a single accredited person, and a joint account holder has withdrawn their approval for one of them,[32] data sharing will stop only for the account associated with the relevant approval.

Data holders can choose to allow an individual joint account holder to reinstate their approvals in relation to an authorisation to share data on a joint account, when an authorisation and disclosure option are in place. This might be used, for example, if an account holder mistakenly removed an approval.

More information

Examples of how to implement the data holder authorisation withdrawal process and of the process for withdrawing approvals are given in the CX Guidelines on Withdrawal.

[28] CDR Rules, rule 4A.13(1)(e).

[29] CDR Rules, rule 4A.10.

[30] CDR Rules, rule 4A.14.

[31] CDR Rules, rules 4.27 and 4A.13.

[32] For example, if the accredited person uses concurrent consents or has multiple software products.

Example – withdrawing an approval (co-approval option)

From the example in Section 4.2, Hope holds a joint transaction account at Easy Credit Union with Gian. Hope also holds a savings account with Easy Credit Union. Gian applied a co-approval option to the joint account using the disclosure option management service.

Hope authorised the disclosure to Go-Budget of data associated with:
- her joint transaction account with Gian
- the savings account held in her name alone.

Gian approves the disclosure of joint account data to Go-Budget in relation to the authorisation to share data.

Gian decides she no longer wants data on the joint account to be shared with Go-Budget. She uses Easy Credit Union's consumer dashboard to withdraw her approval of this data sharing.[33]

Easy Credit Union must:
- stop disclosing data from Gian and Hope's joint account to Go-Budget in relation to the authorisation to share data
- continue disclosing the joint account data to other accredited persons who Gian and Hope have sharing arrangements with
- continue disclosing Hope's savings account data to Go-Budget
- notify Hope that Gian has withdrawn the approval to share data on the joint account with Go-Budget[34]
- update the consumer dashboards accordingly.[35]

Example – withdrawing an approval (pre-approval option)

Kieran and Lena have a joint energy account with Aquarius Energy.

A pre-approval disclosure option applies to the account. Kieran authorised the disclosure of data associated with the joint energy account to Energy Waves.

Lena decides she no longer wants data on the joint account to be shared with Energy Waves. She uses Aquarius Energy's consumer dashboard to withdraw her approval of this data sharing.

Aquarius Energy must:
- stop disclosing data from the joint account to Energy Waves
- continue disclosing the joint account data to other accredited persons with whom Kieran and Lena have sharing arrangements
- notify Kieran that Lena has withdrawn the approval to share data on the joint account with Aquarius Energy[36]
- update the consumer dashboards accordingly.[37]

---

[33] If a pre-approval disclosure option is applied in this scenario, Gian could also withdraw her approval, even though the approval is automatically applied when a pre-approval disclosure option applies to the account.

[34] To satisfy the requirements of the CDR Rules, rule 4A.14.

[35] To satisfy the requirements of the CDR Rules, rules 4.27 and 4A.13.

[36] To satisfy the requirements of the CDR Rules, rule 4A.14.

[37] To satisfy the requirements of the CDR Rules, rules 4.27 and 4A.13.

6. Changing disclosure options

6.1 Applying a more restrictive disclosure option

Any individual joint account holder can independently apply a more restrictive disclosure option. They do not need the agreement of the other joint account holders:[38]

- If a joint account has the pre-approval disclosure option, an individual joint account holder can use the disclosure option management service to apply the co-approval option (if the data holder offers it) or the non-disclosure option.
- If a joint account has the co-approval disclosure option, an individual joint account holder can use the disclosure option management service to apply the non-disclosure option.

When an individual joint account holder ('account holder A') applies a more restrictive disclosure option, the data holder must contact the other account holders to:

- explain to each of them what CDR 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 to change the disclosure option again.[39]

The CX Guidelines include an example of how to implement requirements for changing from the pre-approval option to the non-disclosure option.

6.2 Applying a less restrictive disclosure option

An individual account holder cannot unilaterally change a disclosure option to a less restrictive option. They can propose the change, but the other account holders must agree to it.[40] This means:

- if the non-disclosure option has been put in place for the joint account, an individual joint account holder can propose to change it to the co-approval option (if the data holder offers it) or the pre-approval option
- if the co-approval option has been put in place for the joint account, an individual joint account holder can propose to change it to the pre-approval option.

Account holders will use the disclosure option management service (Section 7.1) to manage proposals for option changes.

[38] CDR Rules, rules 4A.6(1)(a) and 4A.7.

[39] CDR Rules, rule 4A.7.

[40] CDR Rules, rules 4A.6(1)(b) [(a) refers to changing to a more restrictive disclosure option] and 4A.8.

If an individual joint account holder (account holder A) has proposed a change to a less restrictive disclosure option, the data holder must contact the other joint account holders[41] and:

- explain to each of them what CDR is
- inform them which disclosure option currently applies to the account
- inform them that account holder A has proposed to change to either the co-approval or pre-approval option
- explain that this change requires the agreement of all account holders
- explain any 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. This should be the time limit that applies to the data holder's equivalent non-CDR services and requests – for example, the time limit that would apply if an account holder wanted to change authorities to transact on a joint account.[42]

Privacy tip

When contacting the other joint account holders to explain a proposal for a less restrictive disclosure option, data holders should also explain how each disclosure option works. This will help the account holder make an informed decision about their data sharing arrangements. For example, if an account holder proposes to apply the pre-approval option instead of the co-approval option, a data holder could explain to the joint account holder(s):

- what the pre-approval option means (that it will be possible to share CDR data related to the joint account with only one joint account holder's approval)
- how this differs from the disclosure option that currently applies. For example, if the co-approval option currently applies, all joint account holders must give approval before the relevant CDR data may be shared.

At the end of the specified period, the data holder must inform the joint account holders whether:[43]

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

41 CDR Rules, rule 4A.8(2).

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

43 CDR Rules, rule 4A.8(3).

Example - changing disclosure option

From the example in Section 4.2, Hope holds a joint transaction account at Easy Credit Union with Gian. Hope also holds a savings account with Easy Credit Union. Gian applied a co-approval option to the joint account using the disclosure option management service.

Hope authorises the disclosure to Go-Budget of data for:

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

Gian approves the disclosure of joint account data to Go-Budget in relation to that authorisation, allowing data to be shared.

Gian then accidentally applies the non-disclosure option to the joint account. Easy Credit Union:

- notifies Hope (see Section 7.3.1) that Gian has applied the non-disclosure option, and of the matters referred to in Section 6.1
- does not disclose further data from the joint account with Go-Budget or any other accredited person
- continues to disclose Hope's savings account data to Go-Budget
- updates the disclosure option management service accordingly.

Gian, realising her mistake, later proposes a change back to the co-approval disclosure option.

Easy Credit Union therefore notifies Hher to agree to the change of disclosure option within a specified period.[44] If Hope agrees to the change, Easy Credit Union must:

- from the date and time of Hope's agreement to the co-approval option, reinstate all sharing of data from the joint account, for all authorisations that are still current
- update the disclosure option management service to give effect to the change.

When a data holder reinstates sharing after a disclosure option has been amended, the disclosure option management service and consumer dashboard will show consumers which sharing arrangements are in place.[45] However, a data holder may also choose to notify consumers through their ordinary means of contacting them.

The CX Guidelines include an example of how to implement requirements for changing from the non-disclosure option to the pre-approval option.

[44] To satisfy the requirements of the CDR Rules, rule 4A.8.

[45] CDR Rules, rules 4A.13 and 1.15.

7. Consumer oversight and joint account management

The main ways data holders give joint account holders oversight of accounts are the disclosure option management service and the consumer dashboard. Functions on these services should be prominently displayed and easy for consumers to understand.

7.1 Disclosure option management service

A data holder must provide an online 'disclosure option management service' to each joint account holder.[46] The service allows account holders to choose a disclosure option and respond as necessary to choices and proposals of other account holders.

The data holder may include the disclosure option management service in the consumer dashboard (see Section 7.2).

If the disclosure option is changed, the data holder must update the disclosure option management service to reflect the change as soon as practicable.

More information

Examples of how to implement requirements related to changing disclosure options for joint accounts are given in the CX Guidelines on Joint account disclosure option management service. This includes example flows for changing to less restrictive and more restrictive disclosure options.

A data holder must offer an online disclosure option management service.[47] It may also offer the service offline (for example, through a customer service phone line or service desk).[48] When an account holder changes a disclosure option using an offline service, the data holder must update the online service as soon as practicable.[49]

46 CDR Rules, rule 4A.6(1).
47 CDR Rules, rule 4A.6(3).
48 CDR Rules, rule 4A.6(4).
49 CDR Rules, rule 4A.6(5).

Example – offline disclosure option management service

Prema, Chandra and Carlos have an energy account with Super Energy. The pre-approval option applies by default.

Carlos wants to change to the non-disclosure option, so he calls the local Super Energy customer service centre. Carlos tells a Super Energy staff member that he would like the non-disclosure option, rather than the pre-approval option, to apply to his energy account.

Super Energy provides an offline disclosure option management service. Customers can contact the customer service centre and choose a disclosure option. The staff member processes Carlos' request so that the non-disclosure option now applies to the energy account.

Super Energy updates the online disclosure option management services for Prema, Chandra and Carlos to reflect the change to the non-disclosure option. Super Energy includes the disclosure option management service in the consumer dashboard, so this update is reflected in Prema's, Chandra's and Carlos's consumer dashboards (see Section 7.2). Super Energy also notifies Prema, Chandra and Carlos as described in Section 6.

7.2 Consumer dashboards

Data holders must provide a consumer dashboard to joint account holders when:

- a consumer data request in relation to a joint account has been made, and
- the pre-approval option or co-approval option applies, or has applied, to the joint account.[50]

If a joint account holder already has a dashboard because they are sharing CDR data from another account with the same data holder,[51] that dashboard must also serve as the dashboard for the joint account.[52]

The consumer dashboard for joint account holders must:

- contain details of each authorisation to disclose CDR data, including[53]
  - 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
- allow non-requesting joint account holders to manage approvals for each authorisation to disclose joint account data[54]
- allow for the withdrawal of approvals[55]

50 CDR Rules, rules 4A.13(1)(a) and (b).
51 CDR Rules, rule 1.15.
52 CDR Rules, rule 4A.13(2).
53 CDR Rules, rules 4A.13(1)(c) and 1.15.
54 CDR Rules, rule 4A.13(1)(d).
55 CDR Rules, rule 4A.13(1)(e).

- as part of the process of withdrawing approvals, display a message stating the consequences of the withdrawal; the form of the message should be in line with the CX Standards[56]
- be simple and straightforward to use[57]
- be prominently displayed and readily accessible.[58]

Any details of approvals that are shown on one joint account holder's dashboard must also be shown on the dashboards of the other joint account holders.[59]

If a joint account holder requests to share customer data[60] this must be actioned as it would be for an individually held account. Details of such data sharing must not appear on the dashboards of the other account holders. Note that a joint account holder or secondary user cannot share the customer data of another person. The CDR Rules ensure that only the customer data of the person making the request can be shared.[61] No other customer data, including personal information, can be shared.

Dashboards for joint account holders who make requests must also allow management of authorisations.[62]

7.3 Notifications

7.3.1 Ordinary means of contacting an account holder

Throughout the joint account provisions of the CDR Rules, there are requirements to notify consumers through the ordinary means of contacting them. Rule 1.7 defines these 'ordinary means of contact' as:

- the agreed means of contact between the data holder and the account holder
- otherwise, the data holder's default means of contacting the account holder.

For example, the ordinary means for contacting a joint account holder may be:

- email
- text message
- online banking push notifications.

7.3.2 Accredited persons

A data holder must notify accredited persons if an authorisation to share data is withdrawn or expires.[63] A data holder does not have to inform accredited persons when disclosure options are applied or when approvals are given or withdrawn.

---

56 CDR Rules, rule 4A.13(1)(f) and see CX Standard, Withdrawal Standards: Joint accounts, Data Standards Body.

57 CDR Rules, rule 4A.13(1)(g).

58 CDR Rules, rule 4A.13(1)(h).

59 CDR Rules, rule 4A.13(5). See also CX Guidelines on Authorisations relating to joint accounts.

60 CDR Rules, Schedule 3, clause 1.3(1) and Schedule 4, clause 1.3.

61 A person acting under a power of attorney on behalf of a CDR consumer may also request sharing of their customer data. For more information, please refer to guidance on Powers of attorney and the Consumer Data Right.

62 See for example, CDR Rules, rule 1.15(1)(a).

63 CDR Rules, rule 4.26A.

7.3.3 Approval notifications

A data holder must provide an approval notification to each relevant joint account holder if:[64]

- a requester gives, amends or withdraws an authorisation associated with a joint account, or
- an authorisation associated with a joint account expires.

A data holder must notify the requester if:[65]

- a joint account holder does not provide an approval to disclose joint account data within a specified period, or
- a joint account holder withdraws an approval to disclose joint account data.

The data holder must notify joint account holders using their ordinary means for contacting them.[66]

A data holder must make notifications as soon as practicable[67] or following an alternative schedule of notifications chosen by the joint account holder. [68] The data holder must allow joint account holders to select alternative notification schedules and to change their selection at any time.[69] For example, an account holder may choose weekly, fortnightly or monthly bulk approval notifications, or to not receive notifications at all.[70]

> **More information**
>
> Examples of how to provide alternative notification schedules are given in the CX Guidelines on Joint account notification settings.

7.3.4 Alerts concerning notifications to other account holders

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 to this.[71] The wording of the notification to account holder A is at the discretion of the data holder.

---

64 CDR Rules, rule 4A.14(1)(a).

65 CDR Rules, rule 4A.14(1)(b).

66 CDR Rules, rule 4A.14(2)(b).

67 CDR Rules, rule 4A.14(2)(a), CX Standards, Notification Standards, Data Standards Body.

68 CDR Rules, rule 4A.14(3).

69 CDR Rules, rule 4A.14(3)(b), CX Standards, Alternative Notification Schedules for Joint Accounts, Data Standards Body.

70 Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021, Explanatory Statement, page 26, paragraph 5.

71 CX Standards, Notification Standards, Joint account notifications: Contextual alert, Data Standards Body.

8. Vulnerable consumers

8.1 Approach to vulnerable consumers

A data holder will not be liable for a failure to comply with Part 4A of the CDR Rules if it is considered that an act or omission was necessary to prevent physical, psychological or financial harm or abuse to any person.[72] In those circumstances, data holders will not be liable for:

- not inviting relevant account holder(s) to approve a change to the disclosure option before disclosing data on the joint account if the non-disclosure option is in place (which is ordinarily required under rule 4A.8)
- not seeking the approval of the relevant account holder(s) before disclosing data on the joint account for which a co-approval disclosure option is in place, which is ordinarily required under rule 4A.10(4)
- not providing a relevant account holder with a consumer dashboard or updating an existing dashboard with details regarding a joint account, which is ordinarily required under rule 4A.13
- not giving approval notifications to a joint account holder, which is ordinarily required under rule 4A.14
- not seeking an authorisation to disclose data[73]
- not disclosing data.[74]

When joint account data is not shared because the data holder has identified a consumer as vulnerable, the data holder should issue a generic error code to the accredited data recipient. This will avoid disclosing the nature of the refusal and ensure there are no repercussions for the consumer. Data holders should choose appropriate error codes based on the error codes for requests for data. The form of the error codes should be in line with the Standards.[75]

8.2 Identifying vulnerable consumers

The ACCC strongly encourages data holders to develop and implement processes to protect vulnerable consumers.

Data holders should have a robust internal framework for identifying vulnerable consumers. The framework should support informed decision making about when it is appropriate to rely on the exceptions in the CDR Rules; that is, when an act or omission is necessary to prevent physical, psychological or financial harm or abuse.[76]

More information

Guidance for financial firms to recognise and support customers affected by family and domestic violence is provided in the Australian Financial Complaints Authority's AFCA Approach - Joint facilities and family violence. The Australian Banking Association provides Guidance on financial abuse prevention.

[72] CDR Rules, rule 4A.15.

[73] CDR Rules, rule 4.7.

[74] CDR Rules, rules 3.5(1)(a) and 4.7.

[75] See Consumer Data Standards, High Level Standards: Error Codes.

[76] CDR Rules, rule 4A.15.

A data holder may rely on a pre-existing identification that a consumer is vulnerable or at risk of harm. This may avoid the need for consumers to re-identify as vulnerable. For example, a data holder may refuse to share data from a joint account when a consumer has previously chosen to delink an account from their digital profile or to use a silent account digitally.

More information

A sample authorisation flow in which rule 4A.15 is used to allow a vulnerable account holder to share their joint account data as if it were an individual account is given in the CX Guidelines on Authorisation flow for vulnerable requesters. There are CX Standards for joint account notifications in which rule 4A.15 is used. See also the Notification Standards on Joint account alerts.

9. Streamlining processes for multiple joint accounts

A data holder may provide a streamlined process to enable a consumer to give their disclosure option preferences across several joint accounts.

A data holder may also streamline notifications to joint account holders. For example, a data holder may use a single notification to ask joint account holders to indicate disclosure option preferences (see sections 4.1-4.3) for multiple accounts.

10. Secondary users of joint accounts

A person is a secondary user of an account if:[77]

- the person is at least 18 years of age
- the person has account privileges for the account, and
- the data holder has a current secondary user instruction to treat the person as a secondary user.

10.1 Secondary user instructions

Data holders must provide a service that allows an account holder to make and withdraw secondary user instructions.[78] Data holders can choose which specific functionality the service will have. For example, data holders may allow individual joint account holders to provide secondary user instructions, or they may require all account holders to approve a secondary user instruction. Data holders must allow a joint account holder to unilaterally withdraw a secondary user instruction (even if the joint account holder did not make that instruction).

> **More information**
>
> Examples of how account holders may change the sharing rights for other account users, including by withdrawing a secondary user instruction, are given in the CX Guidelines on Secondary users.

10.1.1 General operation of secondary users and joint accounts

A secondary user can authorise data sharing on a joint account in the same way as a joint account holder.

However, a secondary user has 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 which disclosure option applies to a joint account. This means that a secondary user's consumer dashboard shows only the data sharing that they themselves have initiated on the joint account. If the co-approval option applies and a joint account holder authorises the sharing of data on the joint account, a data holder does not have to seek the approval of a secondary user, because they are not a joint account holder.[79]

> **More information**
>
> Secondary users are described in the fact sheets on CDR and secondary users in the banking sector and CDR and secondary users in the energy sector.

---

[77] CDR Rules, rule 1.7, definition of secondary user.

[78] See CDR Rules, rules 1.13(1)(e) and 1.15(5).

[79] CDR Rules, rule 4A.3.

Background and more information

More information on the topics covered in this fact sheet is available in the following resources.

- CX Guidelines
- CDR compliance for bank and non-bank lender data holders
- CDR compliance for energy data holders

CDR provides consumers with greater control over their data. It gives consumers the power to require a data holder to safely share their data with a service provider, so they can get better deals and services.

The key compliance requirements of CDR are established by:

- Part IVD of the *Competition and Consumer Act 2010*
- the Competition and Consumer (Consumer Data Right) Rules 2020
- the Consumer Data Standards.

The CDR information map is a topic-based listing of CDR information published by the Australian Competition and Consumer Commission (ACCC), the Australian Office of the Information Commissioner (OAIC), Treasury and the Data Standards Body (DSB). A glossary of CDR terms can be found on the CDR website.

The CDR Support Portal includes guidance on commonly queried CDR topics. It can also be used to submit questions about the CDR Rules and Standards for CDR agencies to respond to directly.

The ACCC and DSB facilitate the CDR implementation call. It provides a forum for participants and other stakeholders to ask questions about their obligations and receive updates on the CDR system.

Important notice

The information in this publication is for general guidance only. It does not constitute legal or other professional advice and should not be relied on as a statement of the law.

Users should refer to the current versions of the *Competition and Consumer Act 2010*, the Competition and Consumer (Consumer Data Right) Rules 2020, and the Consumer Data Standards. Users should also review other compliance guidance material referred to throughout this publication.

It is the responsibility of each CDR Participant to be fully aware of its obligations under the CDR regulatory framework. The ACCC recommends that CDR participants obtain legal and/or professional advice on how the CDR framework applies to their specific circumstances.

Because the information in this publication is intended only as a general guide, it may contain generalisations. Any examples in this publication are provided for illustrative purposes only; they are not exhaustive and are not intended to impose or imply particular rules or requirements.

The ACCC has made every reasonable effort to provide current and accurate information, but it does not make any guarantees regarding the accuracy, currency or completeness of that information.

The ACCC welcomes feedback on this publication via email to accc-cdr@accc.gov.au.

Revision history

Version	Date	Description
1	January 2022	First version of guide.
2	December 2022	Updated to specify commencement dates and obligations for joint account data sharing in the energy sector.
3	May 2023	Updated to remove references to the telecommunications sector, noting the Government's decision to pause expansion to that sector.
4	February 2025	Amendments to reflect changes made by Competition and Consumer (Consumer Data Right) Amendment (2025 Measures No. 1) Rules 2025 - including to make clear that non-bank lenders are not currently required to respond to requests that relate to a joint account. This is because such requests are considered 'complex requests'.
5	October 2025	Amendments to enhance readability, reflect the passing of commencement dates in the energy sector and clarify that small energy retailers who become accredited will have joint account sharing obligations 18 months after accreditation.
6	September 2026	Revised to improve readability and accessibility. Changes include: • restructured content and clearer headings • use of plain English and more concise language • clarifying application of joint account data sharing obligations by sector • added an image illustrating disclosure options for joint accounts.