Australian Government

Office of the Australian Information Commissioner

Guide to privacy for data holders

7 September 2021

OAIC

Version	Currency dates	Changes and other comments
1.0	12 June 2020 to 15 July 2020	
2.0	16 July 2020 to 6 September 2021	• Updated guidance to reflect amendments to the CDR Rules introduced by the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2020*, including changes to: – when a data holder may refuse to seek an authorisation or disclose CDR data, and – how a data holder must allow a consumer to withdraw authorisation. • Minor redrafting of text to aid with readability.
3.0	7 September 2021 to …	• Updated guidance to reflect amendments to the CDR Rules introduced by the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020*, including changes to: – reflect that authorisations may now be amended – the situations in which a data holder may refuse to seek authorisation or disclose CDR data – reflect the introduction of non-individual consumers, partnership accounts and secondary users – joint accounts obligations for the banking sector (see grey boxes throughout). Updated guidance to reflect amendments to Part IVD of the *Competition and Consumer Act 2010* introduced by the *Treasury Laws Amendment (2020 Measures No. 6) Act 2020*, including changes to the definition of 'data holder' (regarding CDR data that is held before the earliest holding day). • Additional guidance on topics such as when a data holder may be accountable under the CDR regime for the conduct of its third-party service providers.

Contents

Introduction

- This Guide outlines key privacy obligations for data holders in the Consumer Data Right (CDR) system, and should be read in conjunction with the CDR Privacy Safeguard Guidelines.[1]
- In addition to several obligations under the privacy safeguards, data holders must also comply with some key privacy obligations in the CDR Rules, which are set out in this Guide.
- Data holders should read this Guide together with the full text of Division 5 of Part IVD of the *Competition and Consumer Act 2010* (Competition and Consumer Act) and the CDR Rules.
- Chapter B (Key concepts) of the CDR Privacy Safeguard Guidelines contains guidance on general matters, including an explanation of key concepts that are used throughout this Guide.
- This Guide is not legally binding and does not constitute legal advice about how an entity should comply with the CDR Rules and/or the privacy safeguards. Entities may wish to seek independent legal advice where appropriate.

Key points

- In the CDR system, a data holder must comply with privacy obligations relating to:
  - the privacy safeguards
  - consumer data request services
  - disclosure of CDR data
  - authorisation
  - consumer dashboards
  - notification of consumers, and
  - the provision of access to certain records.
- A data holder discloses CDR data to an accredited person where required or authorised to do so in response to a consumer data request.
- A data holder must ask a consumer to authorise the disclosure of their CDR data to an accredited person (unless an exception applies).
- For a data holder that is also subject to the *Privacy Act 1988* (Privacy Act), the Australian Privacy Principles (APPs) will apply to CDR data that is also personal information, with some exceptions.[2]
- In the banking sector, an example of a data holder is an authorised deposit-taking institution (such as a bank). In the energy sector, an example of a data holder is an energy retailer.

[1] The CDR Privacy Safeguard Guidelines provide guidance on the privacy safeguards and related CDR Rules. They focus primarily on the privacy obligations of accredited persons and accredited data recipients.

[2] Data holders are likely to be bound by the Privacy Act, which applies to most organisations that have an annual turnover of over $3 million. See e.g. sections 6C, 13 and 15 of the Privacy Act for more information.

Who is a data holder?

- In the banking sector, an example of a data holder is an authorised deposit-taking institution (such as a bank).[3] In the energy sector, an example of a data holder is a retailer.[4]
- In the CDR system, a data holder discloses CDR data to an accredited person or the consumer themselves, where required or authorised to do so in response to a consumer data request.[5]
- A person is a 'data holder' of CDR data if:
  - the CDR data falls within a class of information specified in the designation instrument for the relevant sector[6]
  - the CDR data is held by (or on behalf of) the person on or after the earliest holding day[7]
  - the CDR data began to be held by (or on behalf of) the person before that earliest holding day, is of continuing use and relevance, and is not about the provision of a product or service by (or on behalf of) the person before the earliest holding day[8]
  - the person is not a designated gateway for the CDR data, AND
  - any of the following three cases apply:[9]
    - **The entity is specified as a data holder in the Designation Instrument** — The person belongs to a class of persons specified in a designation instrument, and the CDR data was not disclosed to the person under the CDR Rules
    - **Reciprocity** — The CDR data was not disclosed to the person under the CDR Rules, and the person is an accredited data recipient of other CDR data, or

---

[3] Authorised-deposit taking institutions are specified as a relevant class of persons who hold CDR data in the designation instrument for the banking sector: see ss 56AJ(1) and 56AJ(2) of the Competition and Consumer Act; s 5(2) of the banking sector designation instrument.

[4] Retailers are specified as a relevant class of persons who hold CDR data in the designation instrument for the energy sector: see ss 56AJ(1) and 56AJ(2) of the Competition and Consumer Act; ss 6(2) and 12 of the energy sector designation instrument.

[5] Further information is available under the section Consumer data requests made by accredited persons.

[6] The designation instruments for each sector set out matters including the classes of information that are subject to the CDR regime. For the banking sector, see the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019. For the energy sector, see the Consumer Data Right (Energy Sector) Designation 2020. See also s 56AC(2)(a) of the Competition and Consumer Act.

[7] Being the earliest holding day specified in the designation instrument for the relevant sector. For the banking sector, the earliest holding day is 1 January 2017: s 5(3) of the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019. For the energy sector, the earliest holding day is 1 July 2018: s 6(3) of the Consumer Data Right (Energy Sector) Designation 2020.

[8] An example of CDR data that would be captured here is a current account number. An example of CDR data that would not be captured here is a transaction on an account that preceded the earliest holding day: Explanatory Memorandum, Treasury Laws Amendment (2020 Measures No. 6) Bill 2020, [2.35].

For a product or service that the person began providing before the earliest holding day and continued providing after that day, the person will:

- not be the data holder of CDR data about the person's provision of the product or service before that day, but
- will be the data holder of CDR data about the person's provision of the product or service on or after the earliest holding day (provided all the other criteria in s 56AJ of the Competition and Consumer Act, as discussed at paragraphs B.101 are met by the entity): see Note 2 to s 56AJ of the Competition and Consumer Act.

[9] Being one of the conditions set out in ss 56AJ(2) to 56AJ(4) of the Competition and Consumer Act.

- **As enabled by the CDR Rules** — The CDR data was disclosed to the person under the CDR Rules, and the person is an accredited person who meets conditions set out in the CDR Rules.[10]

- For further information on when a person will be a 'data holder' of CDR data, see Chapter B (Key concepts) of the CDR Privacy Safeguard Guidelines.

What privacy obligations in the CDR system apply to data holders?

- In the CDR system, a data holder must comply with privacy obligations relating to:
  - Privacy Safeguards 1 (open and transparent management of CDR data), 10 (notifying of the disclosure of CDR data), 11 (quality of CDR data) and 13 (correction of CDR data)
  - providing consumer data request services
  - disclosing CDR data in response to consumer data requests
  - asking consumers to give or amend authorisations
  - managing authorisations, including by providing consumer dashboards
  - notifying consumers of certain matters in relation to their data sharing arrangements, and
  - providing access to copies of records where requested by consumers.
- These privacy obligations are discussed in this Guide.
- Several of these privacy obligations require actions to be taken in accordance with the data standards. The data standards are available on the Consumer Data Standards website.[11]
- A data holder should also be aware that they have other, non-privacy related obligations under the CDR Rules. For example, the requirements relating to product data requests.[12] These are not covered in this Guide. For information on these obligations, see the ACCC's Compliance guidance for data holders in the banking sector.

Certain obligations delayed for the banking sector

For the banking sector, any provisions in the CDR Rules which impose obligations on data holders in relation to:

- non-individual consumers
- partnerships
- nominated representatives, or
- secondary users,

[10] The conditions for the banking sector are contained in clause 7.2 of Schedule 3 to the CDR Rules.

[11] For guidance regarding examples of data standards that are relevant to particular obligations, see the ACCC's Compliance guidance for data holders in the banking sector.

[12] See, e.g, CDR Rule 1.12 and Part 2 of the CDR Rules.

apply only to initial data holders in respect of NAB, CBA, ANZ, and Westpac branded products on and from 1 November 2021.For all other data holders, these obligations apply on and from 1 November 2022.[13]

Does the Privacy Act apply to data holders?

- Where a data holder is an APP entity,[14] they must continue to comply with the Privacy Act.
- The APPs will apply to CDR data held by data holders (where it is also personal information), with the exception of APP 10 (quality of personal information) and APP 13 (correction of personal information).
- These APPs are replaced by Privacy Safeguard 11 (quality of CDR data) and Privacy Safeguard 13 (correction of CDR data), once the data holder is required or authorised to disclose the CDR data under the CDR Rules.[15]

Privacy Safeguards

- A data holder must comply with the following privacy safeguards:
  - Privacy Safeguard 1 (open and transparent management of CDR data)
  - Privacy Safeguard 10 (notifying of the disclosure of CDR data)
  - Privacy Safeguard 11 (quality of CDR data), and
  - Privacy Safeguard 13 (correction of CDR data).
- Information about how to comply with these privacy safeguards is available in Chapters 1, 10, 11 and 13 of the CDR Privacy Safeguard Guidelines.

Consumer data request services

- A data holder may be required to disclose CDR data at the request of a consumer. The request is known as a 'consumer data request' and can be made to the data holder by:
  - an accredited person, on the consumer's behalf, or
  - the consumer themselves.[16]

[13] See cl 6.7 of Schedule 3 to the CDR Rules.

[14] For information regarding an 'APP entity', see Chapter B (Key concepts) of the APP Guidelines.

[15] For further information regarding the interaction between the APPs and the privacy safeguards for data holders, see Chapter A (Introductory matters) of the CDR Privacy Safeguard Guidelines.

[16] For the banking sector, a data holder's obligations under Part 3 of the CDR Rules (regarding consumer data requests made by consumers) do not commence until 1 November 2021: clause 6.6 of Schedule 3 to the CDR Rules. This Guide focuses upon consumer data requests made by accredited persons to data holders, on a consumer's behalf, and the obligations associated with that, rather than the direct to consumer data sharing obligations set out in Part 3.

- A data holder must provide an 'accredited person request service' to allow accredited persons to make consumer data requests, on behalf of consumers, to the data holder.
- This service must comply with the requirements in CDR Rule 1.13(1)(b).
- A data holder must also provide the following services, depending on the nature of the consumer or account. These services can be provided online, but are not required to be:[17]
  - For each non-individual consumer, and each consumer who is a partner in a partnership[18] – a service that allows the consumer to nominate one or more individuals (known as 'nominated representatives') who may give, amend and manage authorisations to disclose CDR data on the consumer's behalf, and also allows the consumer to revoke such nominations.[19]
  - For each account in relation to which a person has account privileges[20] – a service that allows the account holder to make a secondary user instruction,[21] and revoke that instruction.[22]

Consumer data request services in the banking sector — Joint accounts

For the banking sector, where all joint account holders are eligible CDR consumers,[23] the data holder must provide a joint account management service (JAMS) to each joint account holder.[24]

The JAMS allows each joint account holder to indicate a disclosure option in relation to a joint account, being:

- the **pre-approval option**: this option allows data on the joint account to be independently shared by all requesting joint account holders, or
- where offered by the data holder, the **co-approval option**: this option requires all joint account holders to approve the disclosure of joint account data before it may be shared.

This is important because a data holder may only share CDR data in relation to a joint account where a disclosure option applies to the account, unless an exception applies.[25] A disclosure option applies where each account holder has indicated they would like the same disclosure

[17] Note 4 under CDR Rule 1.13(c).

[18] That relates to a partnership account with the data holder: CDR Rule 1.13(1)(d).

[19] CDR Rules 1.13(1)(c) and 1.13(1)(d). For each consumer who is a partner in a partnership, the nominated representative may give, amend and manage authorisations that relate to the partnership accounts only: CDR Rule 1.13(1)(d).

[20] 'Account privileges' for the banking sector are defined in clause 2.2 of Schedule 3 to the CDR Rules.

[21] This is an instruction from an account holder to a data holder to treat a person with requisite 'account privileges' as a secondary user for the purposes of the CDR Rules (CDR Rule 1.7). 'Account privileges' for the banking sector are defined in clause 2.2 of Schedule 3 to the CDR Rules.

[22] CDR Rule 1.13(1)(e).

[23] For the definition of 'eligible' CDR consumer in the banking sector, see clause 2.1 of Schedule 3 to the CDR Rules. See also Chapter B (Key concepts).

[24] See clauses 4.2 and 4.6 of Schedule 3 to the CDR Rules.

[25] In a situation where a consumer has authorised the disclosure of joint account CDR data but no disclosure option applies, a data holder will be authorised to disclose joint account CDR data where circumstances of physical or financial harm or abuse might exist: see clause 4.13(4) of Schedule 3 to the CDR Rules.

option to apply and none have indicated that they no longer want that disclosure option to apply.[26] Where no disclosure option applies, the data holder is not allowed to share CDR data in relation to the joint account.[27]

The JAMS also allows each account holder to change which disclosure option applies to the joint account, and/or remove a disclosure option.

The JAMS must meet the requirements set out in clauses 4.6(3) to 4.6(8) of Schedule 3 to the CDR Rules.

Certain actions by joint account holders via the JAMS may trigger further obligations for the data holder. For example, a data holder must provide the other joint account holders with the information outlined at clause 4.7(2) in the following circumstances:[28]

- where no disclosure option applies to the joint account, and a joint account holder indicates via the JAMs that they would like a particular disclosure option to apply, or
- where a disclosure option already applies to the joint account, and a joint account holder indicates via the JAMS that they would like a different disclosure option, or no disclosure option, to apply.

In relation to the above situations, where a joint account holder indicated that they would like a particular disclosure option to apply, the data holder must invite the other account holders to indicate whether they would like the same disclosure option to apply.[29]

Disclosing CDR data

- The following sections outline when a data holder is required or authorised to disclose CDR data to an accredited person under the CDR Rules, and how that data must be disclosed.[30]

Disclosing CDR data in the banking sector

For the banking sector, different 'categories' of data holders are required to share CDR data in relation to particular product phases at different stages.[31]

[26] See clause 4.5 of Schedule 3 to the CDR Rules.

[27] A disclosure option does not apply to a joint account if the joint account holders indicate they would like different disclosure options to apply, or any of the joint account holders do not indicate a disclosure option: See clause 4.5 of Schedule 3 to the CDR Rules.

[28] See clause 4.7 of Schedule 3 to the CDR Rules.

[29] Clause 4.7(2)(e) of Schedule 3 to the CDR Rules.

[30] This Guide focuses upon the disclosure of CDR data from data holders to accredited persons, rather than the disclosure of CDR data from data holders to consumers. This is because for the banking sector, a data holder's obligations under Part 3 of the CDR Rules (regarding consumer data requests made by consumers) do not commence until 1 November 2021: clause 6.6 of Schedule 3 to the CDR Rules.

[31] See Part 6 of Schedule 3 to the CDR Rules, which outlines the staged application of the CDR Rules to the banking sector.

Consumer data requests made by accredited persons

- An accredited person may request that a data holder disclose a consumer's CDR data to them (following a request to do so from that consumer). This is a 'consumer data request' by an accredited person on behalf of a consumer.[32]
- The consumer data request must be made using the data holder's accredited person request service, in accordance with the data standards.[33]
- Before a data holder can disclose CDR data to an accredited person, the consumer must first authorise the data holder to disclose the particular data to that accredited person.[34]
- A data holder is required to disclose CDR data in response to a consumer data request from an accredited person where:
  - the consumer has authorised the disclosure of some or all of the required consumer data,[35] and
  - the request relates to 'required' consumer data.[36]
- The following sections of this Guide outline:
  - when a data holder must seek authorisation
  - how that authorisation must be sought
  - circumstances where a data holder may refuse to disclose required consumer data, and
  - how authorisations must be managed.

Additional requirements for joint accounts in the banking sector

For the banking sector, where a data holder receives a consumer data request that relates to a joint account, the data holder must comply with additional requirements to be authorised to disclose requested CDR data that relates to that joint account. These are outlined in the following sections of this Guide (and contained in Part 4 of Schedule 3 to the CDR Rules).[37]

---

[32] CDR Rule 4.4.

[33] CDR Rule 4.4(3). Information regarding the 'accredited person request service' is contained under the section Consumer data request services.

[34] CDR Rule 4.5.

[35] CDR Rules 4.6(1) and 4.6(4).

[36] CDR Rule 4.6(4). Where a consumer data request from an accredited person relates to a consumer's 'voluntary' consumer data:

- if a data holder is considering disclosing any of the 'voluntary' consumer data, the data holder must ask the consumer to authorise disclosure of the requested data before disclosing that data to the accredited person (CDR Rule 4.5(2)), but
- is not otherwise required to disclose requested 'voluntary' consumer data (CDR Rule 4.6(2)).

For information regarding 'voluntary' consumer data and 'required' consumer data, see CDR Rule 1.7, clause 3.2 of Schedule 3 to the CDR Rules and Chapter B (Key concepts) of the CDR Privacy Safeguard Guidelines.

[37] See Note 2 to CDR Rule 4.6(2).

Authorisation

When to seek an authorisation, or an amendment to an authorisation

- A data holder must seek a consumer's authorisation for the disclosure of CDR data where the data holder:[38]
  - receives a consumer data request from an accredited person (on behalf of an eligible CDR consumer),[39] and
  - does not already have a current authorisation to disclose the CDR data.[40]
- A data holder must invite a consumer to amend their authorisation where:
  - the data holder is notified by the accredited person that the relevant consent has been amended,[41] and
  - the authorisation is current.[42]
- The data holder must seek authorisation, and amendments to authorisation, in accordance with Division 4.4 of the CDR Rules and the applicable data standards.[43]
- The authorisation requirements in Division 4.4 of the CDR Rules are outlined in the following sections of this Guide.
- The applicable data standards can be found on the Data Standards Body's Consumer Data Standards website, with guidance on these available in the ACCC's compliance guidance for data holders in the banking sector.

Authorisation in the banking sector — Joint accounts

For the banking sector, where a data holder receives a consumer data request relating to a joint account, the data holder must ask the other joint account holders to take certain actions. These are outlined below.

[38] CDR Rule 4.5.

[39] For the definition of an 'eligible' CDR consumer in the banking sector, see clause 2.1 of Schedule 3 to the CDR Rules. See also Chapter B (Key concepts) of the CDR Privacy Safeguard Guidelines. The data holder must reasonably believe that the consumer data request was made by an accredited person on behalf of an 'eligible' CDR consumer: CDR Rule 4.5(1)(c).

[40] An authorisation is current if it has not expired in accordance with CDR Rule 4.26.

[41] CDR Rule 4.22A. An accredited person may invite a consumer to amend their consent under the CDR Rules. Where a consumer amends a consent for the collection of CDR data from a data holder, the accredited person must notify the data holder, in accordance with the data standards, that the consent has been amended: CDR Rule 4.18C. An amendment of an authorisation to disclose CDR data other than in response to such a notification from the accredited person is of no effect: CDR Rule 4.22A(2).

[42] CDR Rule 4.22A(1). An authorisation is current if it has not expired in accordance with CDR Rule 4.26.

[43] CDR Rule 4.5.

Where the requesting joint account holder has not indicated a disclosure option, the data holder must ask the requesting joint account holder to indicate which disclosure option they would like to apply to the joint account.[44]

Where the requesting joint account holder has indicated a disclosure option, the data holder must ask the other joint account holders to indicate whether they would like the same disclosure option to apply to the joint account.[45]

Where a disclosure option applies to the account, the data holder must ask the requesting joint account holder to authorise the disclosure of CDR data.[46]

Where a co-approval option applies the joint account, the data holder must ask the other joint account holders to approve the disclosure of CDR data.[47]

- The following flow chart demonstrates the role of authorisation in the key information flow between a consumer, data holder and accredited person.

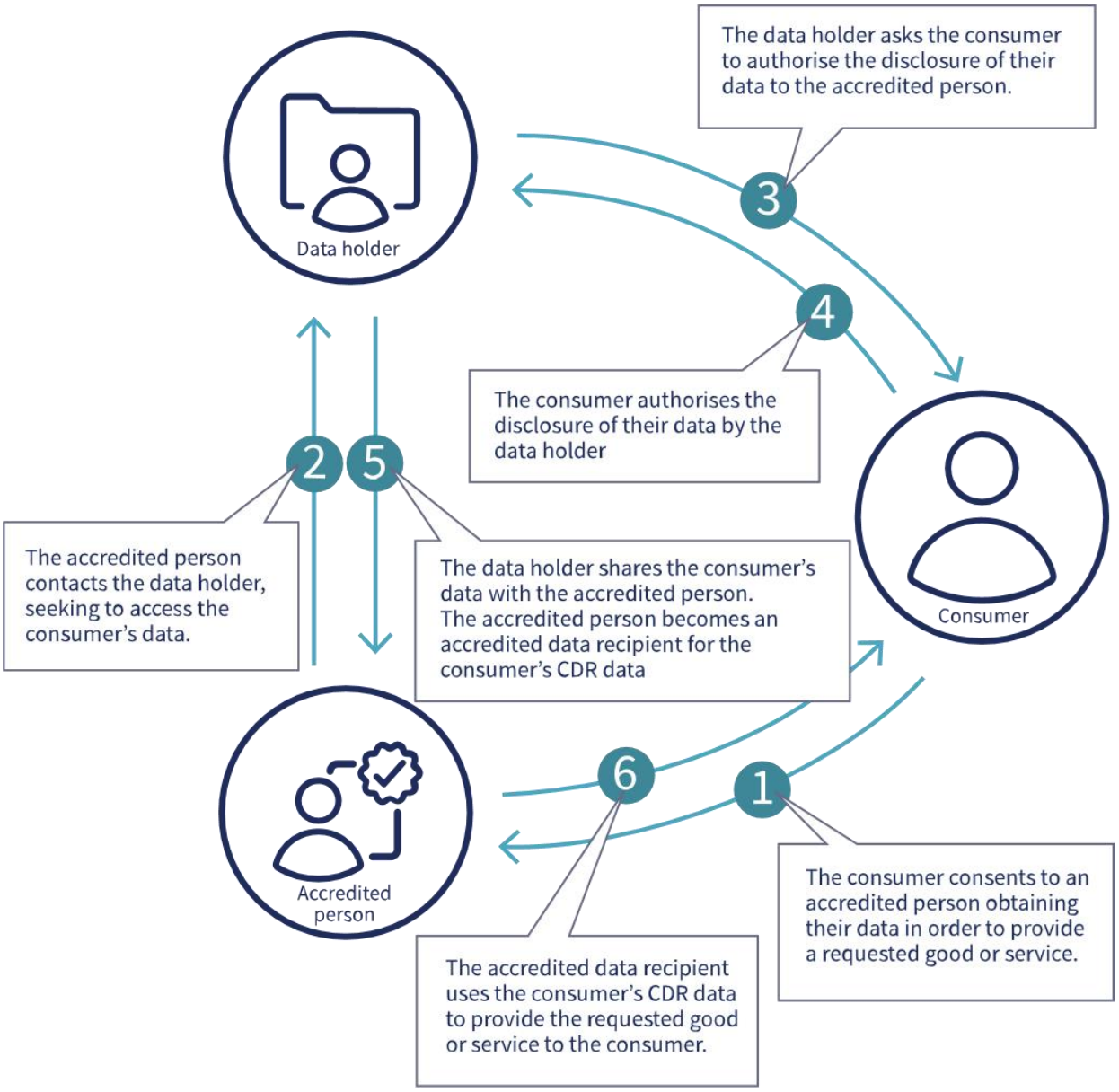
[44] This must be done through the joint account management service and in accordance with the data standards. See clause 4.10 of Schedule 3 to the CDR Rules.

[45] See clause 4.7(2)(e) of Schedule 3 to the CDR Rules. The disclosure option will not apply to the joint account unless the relevant joint account holders indicate that they would like the same disclosure option to apply: Note 2 to clause 4.10 of Schedule 3 to the CDR Rules.

[46] See Division 4.4 of the CDR Rules. Also note that a disclosure option does not apply to a joint account if the joint account holders indicate they would like different disclosure options to apply, or any of the joint account holders do not indicate a disclosure option: see clause 4.5 of Schedule 3 to the CDR Rules.

[47] This must be done in accordance with clause 4.11 of Schedule 3 to the CDR Rules. For information on co-approval options, see clause 4.5(2) of Schedule 3 to the CDR Rules.

Overview: key information flow in the CDR regime



Situations where a data holder may refuse to seek an authorisation

- A data holder may refuse to seek an authorisation in the following circumstances outlined in CDR Rule 4.7:
  - where the data holder considers this to be necessary to prevent physical or financial harm or abuse[48]
  - where the data holder has reasonable grounds to believe that disclosing some or all of the CDR data would adversely impact the security, integrity or stability of the Register of Accredited Persons or the data holder's ICT systems[49]
  - where the CDR data relates to an account that is blocked or suspended, or
  - where provided for in the data standards.
- Where the data holder refuses to seek an authorisation for a reason outlined above, they must inform the accredited person of the refusal in accordance with the data standards.[50]

Situations where a data holder is not required to seek an authorisation

- A data holder would not be required to seek an authorisation in the following circumstances:
  - where the consumer data request relates to a non-individual CDR consumer or partnership account, but there is no nominated representative,[51] or
  - where the person who makes the request has account privileges, but the account holder has not provided a secondary user instruction for that person.[52]

[48] For the banking sector, data holders (e.g. banks) may have existing internal frameworks which might assist in identifying these risks and deciding when this exception would apply. If a data holder requires further assistance in determining whether there is a risk of physical or financial harm or abuse, the OAIC recommends the data holder contact relevant advocacy organisations.

[49] The Register of Accredited Persons means the ACCC's Register of Accredited Persons established under s 56CE(1) of the Competition and Consumer Act.

[50] CDR Rule 4.7.

[51] This is because of the operation of CDR Rules 1.13(1)(c) and 1.13(1)(d). (For a non-individual consumer or consumer with a partnership account to participate in the CDR, they must nominate one or more individuals (known as a 'nominated representative') who is able to give, amend and manage authorisations to disclose CDR data on their behalf.) See also note 3 to CDR Rule 1.13.

[52] This is because of the operation of the CDR Rules in relation to secondary users. (For a person other than the account holder to participate in the CDR, they must be a 'secondary user' for an account with a data holder. A person will be a secondary user if the person has 'account privileges' in relation to the account, and the account holder has given the data holder an instruction to treat the person as a secondary user for the purposes of the CDR Rules (i.e. a secondary user instruction) (CDR Rule 1.7). 'Account privileges' for the banking sector are defined in clause 2.2 of Schedule 3 to the CDR Rules.)

Requirements for seeking or amending an authorisation

General processes

- A data holder's processes for asking a consumer to give or amend an authorisation must:
  - accord with the data standards, and
  - be as easy to understand as practicable, including by using concise language and, where appropriate, visual aids.[53]
- In ensuring processes are easy to understand, a data holder must also have regard to the Consumer Experience Guidelines.[54]

Information to be provided

- When asking a consumer to give or amend an authorisation, a data holder must provide the consumer with the following information as required by CDR Rule 4.23:
  - the name of the accredited person that made the consumer data request, or provided notification of the relevant consent having been amended
  - any information held by the Register of Accredited Persons in relation to the accredited person that is specified as information that must be provided to a consumer when seeking or amending an authorisation
  - the period of time to which the CDR data relates (noting this period may extend back to 1 January 2017)[55]
  - the types of CDR data that will be disclosed (the data holder must use the Data Language Standards to describe the CDR data)[56]
  - whether the authorisation relates to a 'one-off' disclosure, or an ongoing disclosure over a period of time (no more than 12 months)[57]

---

[53] CDR Rule 4.22.

[54] CDR Rule 4.22. The 'Consumer Experience Guidelines' provide best practice interpretations of several CDR Rules relating to authorisation and are discussed in Chapter B (Key concepts) of the CDR Privacy Safeguard Guidelines.

[55] To be a data holder, one key requirement is that a person must have begun to hold the CDR data after the 'earliest holding day (s 56AJ(1)(b) of the Competition and Consumer Act). Under the designation instrument for the banking sector, the earliest holding day is 1 January 2017: s 5(3) of the designation instrument. This means that consumer data requests may be made for CDR data dating back to 1 January 2017.

Consumer data requests may also be made for CDR data that began to be held by a data holder before the earliest holding day, where that data is of continuing use and relevance and is not about the provision of a product or service by the person before the earliest holding day: s 56AJ(1)(ba) of the Competition and Consumer Act. An example of CDR data that would meet this criteria is a current account number: Explanatory Memorandum, Treasury Laws Amendment (2020 Measures No. 6) Bill 2020, [2.35].

[56] The Data Language Standards are contained within the Consumer Experience Guidelines. They provide descriptions of the types of data to be used by data holders when making and responding to requests. Adherence to the Data Language Standards is mandatory and will help ensure there is a consistent interpretation and description of the consumer data that will be shared in the CDR system. See s 56FA of the Competition and Consumer Act and CDR Rule 8.11.

[57] Authorisations to disclose CDR data expire at the latest 12 months after they are given: CDR Rule 4.26(1)(e).

- if authorisation is being sought for an ongoing disclosure — what the time period is (no more than 12 months)[58]
- a statement that the authorisation can be withdrawn at any time, and
- instructions for how the authorisation can be withdrawn.

Restrictions on seeking or amending an authorisation

- CDR Rule 4.24 provides that when asking a consumer to authorise the disclosure of CDR data, or to amend a current authorisation, the data holder must not:
  - add any requirements to the authorisation process aside from those set out in the data standards and the CDR Rules
  - provide or request additional information beyond those specified in the data standards and the CDR Rules
  - offer additional or alternative services, or
  - include or refer to other documents.
- The above practices are not permitted, because they may make authorisation harder for consumers to understand and have the potential to undermine the voluntary nature of the authorisation.

Obligations upon receiving an authorisation

- Once a data holder has received authorisation, or an amendment to authorisation, from the relevant consumer/s,[59] the data holder:
  - *must* disclose the required consumer data (subject to CDR Rules 4.6A and 4.7),[60] and
  - *may* disclose the relevant voluntary consumer data (subject to CDR Rule 4.6A).[61]
- The data holder must disclose the data via its accredited person request service, and in accordance with the data standards.[62]
- A data holder must not charge a fee for the disclosure of required consumer data.[63]

---

[58] Authorisations to disclose CDR data expire at the latest 12 months after they are given: CDR Rule 4.26(1)(e).

[59] In the banking sector, where the CDR data requested relates to a joint account, a data holder will be required to seek approval from the other joint account holders where a co-approval option applies to the joint account: see subdivision 4.3.2 of Schedule 3 to the CDR Rules. For further information about co-approval options and disclosure options for joint accounts more generally, see the grey box under the section Consumer data request services.

[60] CDR Rule 4.6(4). 'Required consumer data' for the banking sector is defined in clause 3.2(1) of Schedule 3 to the CDR Rules. Clause 3.2(3) of Schedule 3 to the CDR Rule sets out what CDR data will be neither required consumer data nor voluntary consumer data. For further information, see Chapter B (Key concepts) of the CDR Privacy Safeguard Guidelines.

[61] CDR Rule 4.6(2). 'Voluntary consumer data' for the banking sector is defined in clause 3.2(2) of Schedule 3 to the CDR Rules. Clause 3.2(3) of Schedule 3 to the CDR Rule sets out what CDR data will be neither required consumer data nor voluntary consumer data. For further information, see Chapter B (Key concepts) of the CDR Privacy Safeguard Guidelines.

[62] CDR Rule 4.6. Information regarding the 'accredited person request service' is available under Consumer data request services.

[63] Section 56BU of the Competition and Consumer Act.

Notification requirements in the banking sector — Joint accounts

For the banking sector, where a data holder receives an authorisation, or an amendment to an authorisation, in relation to a joint account, the data holder must:[64]

- as soon as practicable, notify each relevant account holder of this fact through its ordinary means of contacting them, and
- if the consumer is a secondary user of the joint account and no disclosure option applies to the joint account - ask the relevant account holders to indicate which disclosure option they would like to apply to the account,[65] and
- if a co-approval option applies to the joint account and authorisation has been amended, notify each relevant account holder of the nature of the amendment and how they can remove an approval to prevent further joint account CDR data being disclosed.

Situations where a data holder may refuse to or must not disclose CDR data

- Despite having received an authorisation, or an amendment to authorisation, a data holder may refuse to disclose required consumer data in the following circumstances as outlined in CDR Rule 4.7:
  - where the data holder considers this to be necessary to prevent physical or financial harm or abuse[66]
  - where the data holder has reasonable grounds to believe that disclosing some or all of the CDR data would adversely impact the security, integrity or stability of the Register of Accredited Persons or the data holder's ICT systems[67]
  - where the CDR data relates to an account that is blocked or suspended, or
  - where provided for in the data standards.
- Where the data holder refuses to disclose CDR data for a reason outlined above, they must inform the accredited person of the refusal in accordance with the data standards.[68]
- A data holder must not disclose CDR data that relates to a particular account if:

[64] Clause 4.16 of Schedule 3 to the CDR Rules.

[65] Through the joint account management service and in accordance with the data standards: cl 4.16(1)(b) of Schedule 3 to the CDR Rules.

[66] For the banking sector, data holders (e.g. banks) may have existing internal frameworks which might assist in identifying these risks and deciding when this exception would apply. If a data holder requires further assistance in determining whether there is a risk of physical or financial harm or abuse, the OAIC recommends the data holder contact relevant advocacy organisations.

[67] The Register of Accredited Persons means the ACCC's Register of Accredited Persons established under s 56CE(1) of the Competition and Consumer Act.

[68] CDR Rule 4.7.

  - the request was made on behalf of a secondary user of the account, but the account holder has indicated through their consumer dashboard that they no longer approve of CDR data being shared in response to requests by or on behalf of that secondary user, [69] or
  - a Schedule to the CDR Rules provides that the CDR data must not be disclosed (for example, in relation to joint accounts for the banking sector, as outlined below). [70]
- In addition, a data holder must not disclose CDR data that relates to a non-individual CDR consumer account or partnership account for which there is no nominated representative.[71]

Exception to disclosure in the banking sector — Joint accounts

For the banking sector, where a consumer data request relates to a joint account, a data holder must not disclose CDR data relating to the joint account unless the data holder has received an authorisation from the requesting joint account holder, and one of the following applies:[72]

- a pre-approval option applies to the joint account, and has not been removed by any relevant account holder
- a co-approval option applies to the joint account, and has not been removed by any relevant account holder, and each relevant account holder has approved the disclosure within the required timeframes[73]
- a co-approval option applies to the joint account, and has not been removed by any relevant account holder, but the data holder considers it necessary to avoid seeking the approval of the relevant account holder in order to prevent physical or financial harm or abuse,[74] or

[69] CDR Rule 4.6A. A person will be a secondary user if the person has 'account privileges' in relation to the account, and the account holder has given the data holder an instruction to treat the person as a secondary user for the purposes of the CDR Rules (i.e. a secondary user instruction) (CDR Rule 1.7). 'Account privileges' for the banking sector are defined in clause 2.2 of Schedule 3 to the CDR Rules.

As a result, where a request is from or made on behalf of a person with account privileges, but the account holder has not provided a secondary user instruction in relation to that person, a data holder must also not disclose CDR data that relates to that account.

[70] CDR Rule 4.6A. For the banking sector, see cl 4.13 of Schedule 3 to the CDR Rules.

[71] See Note 3 to CDR Rule 1.13, citing CDR Rules 1.13(1)(c) and 1.13(1)(d). (For a non-individual consumer or consumer with a partnership account to participate in the CDR, they must nominate one or more individuals (known as a 'nominated representative') who is able to give, amend and manage authorisations to disclose CDR data on their behalf. Accordingly, where there is no such nominated representative, the data holder will be neither required nor permitted to disclose requested CDR data in relation to the particular account under the CDR Rules.)

[72] Clause 4.13 of Schedule 3 to the CDR Rules.

[73] Relevant account holders must approve the disclosure in accordance with cl 4.11 of Schedule 3, within the time frame referred to in cl 4.11(2)(e) of Schedule 3.

[74] For the banking sector, data holders (e.g. banks) may have existing internal frameworks which might assist in identifying these risks and deciding when this exception would apply. If a data holder requires further assistance in determining whether there is a risk of physical or financial harm or abuse, the OAIC recommends the data holder contact relevant advocacy organisations.

- no disclosure option applies to the joint account, but the data holder considers it necessary to avoid inviting at least one of the relevant account holders to choose a disclosure option in order to prevent physical or financial harm or abuse.[75]

How authorisations must be managed

Consumer dashboards

- A consumer dashboard is an online service which must be provided by a data holder to a consumer, following receipt of a consumer data request from an accredited person (on behalf of that consumer).[76]
- The purpose of the consumer dashboard is to help the consumer to manage and view the authorisations that they, or a secondary user, have given to disclose their CDR data.
- The general requirements for the dashboard are contained in CDR Rule 1.15(1) and outlined below.
- Additional requirements apply where the consumer is a secondary user or non-individual, or where the CDR data requested relates to a partnership or joint account. These are outlined further below in this section.
- The consumer dashboard should be provided to the consumer as soon as practicable after the data holder receives the relevant consumer data request.[77]
- The consumer dashboard must contain the following details for each authorisation:[78]
  - the CDR data to which the authorisation relates
  - the date on which the consumer gave authorisation
  - the period for which the consumer gave authorisation
  - if the authorisation is current — when it will expire
  - if the authorisation is not current — when it expired
  - the information required to notify the consumer of the disclosure of their CDR data, being:
    - what CDR data was disclosed
    - when the CDR data was disclosed, and

[75] For the banking sector, data holders (e.g. banks) may have existing internal frameworks which might assist in identifying these risks and deciding when this exception would apply. If a data holder requires further assistance in determining whether there is a risk of physical or financial harm or abuse, the OAIC recommends the data holder contact relevant advocacy organisations.

[76] CDR Rule 1.15.

[77] This is to assist the data holder in complying with its obligation under Privacy Safeguard 10 and Rule 7.9 to update the consumer's dashboard 'as soon as practicable' after the disclosure of CDR data to notify the consumer of certain matters. See Chapter 10 (Privacy Safeguard 10) of the CDR Privacy Safeguard Guidelines for further information.

[78] CDR Rules 1.15(1)(b) and 1.15(3).

    - the accredited data recipient for the CDR data.[79]
  - if the CDR data was disclosed in response to a request under Privacy Safeguard 11 for the data holder to disclose corrected CDR data – a statement of this fact.[80]
- The consumer dashboard must have a functionality that allows the consumer to withdraw authorisation at any time. This functionality must:[81]
  - be simple and straightforward to use, and prominently displayed,[82] and
  - as part of the withdrawal process, display a message outlining the consequences of withdrawing authorisation in accordance with the data standards.
- The consumer dashboard must also contain any information that has been specified as information for CDR Rule 1.15 in the data standards or on the Register of Accredited Persons.[83]

Tip: For examples of how to present this information on the consumer dashboard, and other best practice recommendations relating to the consumer dashboard, see the Consumer Experience Guidelines.

- For non-individual consumers, or where the requested CDR data relates to a partnership account, a data holder must ensure the dashboard allows only nominated representatives to manage authorisations.[84]
- Where the consumer is a secondary user,[85] in addition to providing the secondary user with a dashboard, the data holder must also ensure the dashboard for the relevant account holder:[86]
  - contains the details listed above about each authorisation given by that secondary user

[79] Privacy Safeguard 10 requires a data holder to notify consumers of the disclosure of their CDR data by updating the consumers' dashboard to include certain matters. For further information, see CDR Rule 7.9 and Chapter 10 (Privacy Safeguard 10) of the CDR Privacy Safeguard Guidelines.

[80] Privacy Safeguard 11 requires a data holder to disclose corrected CDR data to the original recipient of the disclosure if the entity has advised the consumer that some or all of the CDR data was incorrect when the entity disclosed it, and the consumer requests the entity to disclose the corrected CDR data. For further information, see s 56EN(4) of the Competition and Consumer Act and Chapter 11 (Privacy Safeguard 11) of the CDR Privacy Safeguard Guidelines.

[81] CDR Rule 1.15(1)(c).

[82] The functionality must be no more complicated to use than the process for giving the authorisation to disclose CDR data: CDR Rule 1.15(1)(c)(iii).

[83] CDR Rules 1.15(1)(ba) and 1.15(1)(bb).

[84] CDR Rule 1.15(2A). A nominated representative is a person who has been nominated by a non-individual consumer or consumer who is in a partnership, who may give, amend and manage authorisations to disclose CDR data on that consumer's behalf: see CDR Rules 1.13(1)(c) and 1.13(1)(d).

[85] A person is a 'secondary user' for an account with a data holder if the person has 'account privileges' in relation to the account, and the account holder has given the data holder an instruction to treat the person as a secondary user for the purposes of the CDR Rules (CDR Rule 1.7). 'Account privileges' for the banking sector are defined in clause 2.2 of Schedule 3 to the CDR Rules.

[86] CDR Rules 1.15(5) and 1.15(7).

  - allows the account holder to indicate that they no longer approve CDR data being shared with a particular accredited person by that secondary user [87]
  - allows the account holder to withdraw the secondary user instruction
  - is simple and straightforward to use,[88] and prominently displayed, and
  - as part of the withdrawal process, displays a message outlining the consequences of withdrawing a secondary user instruction, in accordance with the data standards.
- Where the data holder has not already provided a dashboard for the relevant account holder,[89] the requirements listed above can be provided via an online service.[90]
- A data holder must update a consumer's dashboard as soon as practicable after the information required to be contained on the dashboard changes.[91]

Consumer dashboards in the banking sector — Joint accounts

For the banking sector, a data holder must provide a dashboard to the other (non-requesting) joint account holders where a disclosure option applies (or has applied) to that joint account.[92] The dashboard must contain the details listed above about the authorisation given by the requesting consumer. Where a disclosure option applies to the joint account, the dashboard must also allow the other joint account holder/s to manage approvals to disclose CDR data, as well as remove their approval at any time.[93]

However, if a data holder considers it necessary to prevent physical or financial harm or abuse, they may decline to:[94]

- provide a relevant joint account holder with a dashboard, or
- reflect details of the consumer data request in any existing dashboard.

[87] Where an account holder makes such an indication, the data holder will no longer be able to disclose CDR data relating to that account to the particular accredited person: see note 2 to CDR Rule 1.15(5), citing CDR Rules 4.6(2), 4.6(4) and 4.6A(1).

[88] The online service must be no more complicated to use than the processes for giving authorisations or instructions: CDR Rule 1.15(5)(b)(iv).

[89] For example, because the data holder has never received a consumer data request from or on behalf of the relevant account holder.

[90] CDR Rules 1.15(5) and 1.15(7).

[91] CDR Rule 4.27.

[92] Clause 4.14 of Schedule 3 to the CDR Rules. For information regarding disclosure options, see the grey box under 'Consumer data request services'.

[93] Clause 4.14(1) of Schedule 3 to the CDR Rules.

[94] Clause 4.14(4) of Schedule 3 to the CDR Rules. For the banking sector, data holders (e.g. banks) may have existing internal frameworks which might assist in identifying these risks and deciding when this exception would apply. If a data holder requires further assistance in determining whether there is a risk of physical or financial harm or abuse, the OAIC recommends the data holder contact relevant advocacy organisations.

Consumers may withdraw authorisation

- A consumer who has given authorisation for a data holder to disclose their CDR data may withdraw the authorisation at any time.[95]
- Where a consumer withdraws authorisation, the data holder must notify the accredited person of the withdrawal in accordance with the data standards.[96]
- A data holder must allow a consumer to withdraw authorisation by:
  - using the data holder's consumer dashboard, or
  - using a simple alternative method of communication made available by the data holder.[97]

Tip: For examples of how to implement the withdrawal functionality on the consumer dashboard, and best practice recommendations for how to do this, see the Consumer Experience Guidelines.

- The functionality to withdraw authorisation on the consumer dashboard must:
  - be simple and straightforward to use
  - be prominently displayed
  - be as easy to use as the process for giving an authorisation, and
  - display a message outlining the consequences of withdrawing authorisation. This message must accord with the data standards.[98]
- The alternative method of communicating the withdrawal of authorisation must be simple.[99] In addition, it:
  - should be accessible and straightforward for a consumer to understand and use, and
  - may be written or verbal. Where it is written, the communication may be sent by electronic means (such as email) or non-electronic means (such as by post).
- A data holder may wish to ensure their alternative method of communication is consistent with existing channels already made available to its customers,[100] for example through their telephone helpline.

[95] CDR Rule 4.25(1). In relation to joint account holders, a joint account holder who has given an approval for the disclosure of CDR data may remove that approval at any time: clause 4.14(1)(c) of Schedule 3 to the CDR Rules. In relation to secondary user instructions, a consumer who has given a data holder a secondary user instruction may also withdraw that instruction at any time: CDR Rule 1.15(5)(b)(ii).

[96] CDR Rule 4.25(2).

[97] CDR Rule 4.25(1).

[98] CDR Rule 1.15(1)(c).

[99] CDR Rule 4.25(1).

[100] Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2020*.

Effect of withdrawing authorisation

- The main consequence of withdrawing an authorisation is that the authorisation expires, and CDR data can no longer be shared with the relevant accredited person.[101] Information about when authorisation expires is contained in the following section of this Guide.
- If a consumer withdraws authorisation using the data holder's consumer dashboard, the withdrawal is immediately effective.[102]
- If a withdrawal is not communicated over the consumer dashboard, the data holder must 'give effect' to the withdrawal as soon as practicable, but not more than two business days after receiving the communication.[103]
- The test of practicability is an objective test. In adopting a timetable that is 'practicable' a data holder can take technical and resource considerations into account. However, the data holder must be able to justify any delay in giving effect to the consumer's communication of withdrawal.
- 'Giving effect' to the withdrawal includes updating the consumer dashboard to reflect that the authorisation has expired,[104] as required by CDR Rule 4.27.[105]

When an authorisation expires

- Upon an authorisation expiring, CDR data can no longer be shared with the relevant accredited person. CDR Rule 4.26 provides that authorisation expires in the following circumstances:
  - **If the authorisation is withdrawn**
    - If a withdrawal notice is given via the consumer dashboard, the authorisation expires immediately. Where withdrawal is not given through the consumer dashboard, the authorisation expires when the data holder gives effect to the withdrawal, or two business days after receiving the communication, whichever is sooner.
  - **Upon the consumer ceasing to be 'eligible'**[106]
    - For example, in the banking sector, the consumer will cease to be 'eligible' upon closing the bank account/s that the authorisation relates to.[107]
  - **When the data holder is notified by the accredited person of the withdrawal of consent**
    - Upon notification from the accredited person that the consumer has withdrawn their collection consent, the authorisation expires immediately.

---

[101] Where a joint account holder removes an approval, or an account holder removes a secondary user instruction, the data holder will no longer be able to disclose CDR data relating to that account to the relevant accredited person.

[102] CDR Rule 4.26(1).

[103] CDR Rule 4.26(1).

[104] See CDR Rule 1.15(3)(e).

[105] CDR Rule 4.27 requires a data holder to update the consumer dashboard as soon as practicable after the information required to be contained on the dashboard changes.

[106] This is because only 'eligible' CDR consumers may make consumer data requests under the CDR Rules.

[107] For the definition of an 'eligible' CDR consumer in the banking sector, see clause 2.1 of Schedule 3 to the CDR Rules. See also Chapter B (Key concepts) of the CDR Privacy Safeguard Guidelines.

- **For ongoing disclosure, at the end of the period of authorisation, or the period of authorisation as last amended (no longer than 12 months after authorisation was given or amended)**
  - Authorisation expires at the end of the specified period for which the consumer gave authorisation for the data holder to disclose the CDR data. Where the period of the authorisation has been amended, authorisation expires at the end of this period. In both cases, the specified period cannot be longer than 12 months.
- **For disclosure on a single occasion, after the CDR data has been disclosed**
- **If another CDR Rule provides that authorisation expires**
  - For example: an authorisation to disclose CDR data expires once the accredited person becomes a data holder rather than an accredited data recipient for the CDR data.[108]
- **If the accredited person's accreditation is revoked or surrendered**
  - Authorisation for a data holder to disclose CDR data to that accredited person expires when the data holder is notified of the revocation or surrender.

Notification requirements

- A data holder must comply with the following notification requirements under the CDR Rules:
  - **Notification of disclosure**
    - A data holder must notify the consumer of the disclosure of their CDR data as soon as practicable after the disclosure occurs.[109]
  - **Update consumer dashboard**
    - A data holder must update a consumer's dashboard as soon as practicable after the information required to be contained on the dashboard changes. [110]
  - **Notification regarding authorisations given by secondary users**
    - Where a secondary user amends or withdraws an authorisation, or such an authorisation expires, a data holder must notify the account holder of this fact as soon as practicable.[111]

Additional notification requirements for the banking sector – Joint accounts

For the banking sector, where a joint account holder amends or withdraws an authorisation, or an authorisation expires, a data holder must notify the other account holders of the matters

[108] As a result of clause 7.2(3)(b) of Schedule 3 to the CDR Rules and section 56AJ(4) of the Competition and Consumer Act.

[109] Privacy Safeguard 10 requires a data holder to notify consumers of the disclosure of their CDR data by updating the consumers' dashboard to include certain matters. For further information, see CDR Rule 7.9 and Chapter 10 (Privacy Safeguard 10) of the CDR Privacy Safeguard Guidelines.

[110] CDR Rule 4.27.

[111] CDR Rule 4.28. Notification must be provided through the data holder's ordinary means of contacting the account holder: CDR Rule 4.28(2).

outlined in clause 4.16 of Schedule 3 to the CDR Rules. These are outlined under 'Obligations upon receiving authorisation' above.

Liability for third-party service providers

- In certain circumstances, a data holder may be accountable under the CDR regime for the conduct of its third-party service providers. For example, where the service provider is acting on the data holder's behalf, within the service provider's actual or apparent authority.[112]
- The CDR regime does not regulate a data holder's engagement of a third-party service provider. However, data holders must still ensure they meet their obligations under the CDR regime and any other relevant legislation (such as the Privacy Act).
- Where a data holder is also an accredited data recipient, they should be aware that the CDR regime does regulate an accredited data recipient's engagement of a third-party service provider (where that third party is considered an 'outsourced service provider' under the CDR Rules).[113]

Providing access to copies of records

- A consumer may request access to copies of the following data holder records:
  - authorisations given by the consumer to disclose CDR data, including amendments to any such authorisations
  - withdrawals of authorisations given by the consumer to disclose CDR data
  - disclosures of CDR data made by the data holder in response to consumer data requests made by or on behalf of the consumer, and
  - CDR complaint data relating to the consumer.[114]
- Data holders are required to keep and maintain these and other records under the Rules.[115]
- Where requested by a consumer, a data holder must provide the relevant copies of records as soon as practicable, but no later than 10 business days after receiving the request.[116]
- In adopting a timetable that is 'as soon as practicable', a data holder can take technical and resource considerations into account.

---

[112] Section 56AU(2) of the Competition and Consumer Act provides that acts done by or in relation to another person who is acting on behalf of a CDR entity, within the person's actual or apparent authority, are taken to have also been done in relation to the CDR entity, See also s 56AU(1), which provides that the conduct of agents of a CDR entity are attributable to the CDR entity, and s 84.

[113] See CDR Rule 1.10. For further information on outsourced service providers, see Chapter B (Key concepts).

[114] CDR complaint data is defined in CDR Rule 1.7.

[115] CDR Rule 9.5(1). A data holder must keep and maintain certain records as outlined in CDR Rule 9.3(1). For further information on record-keeping requirements, see the ACCC's Compliance guidance for data holders in the banking sector.

[116] CDR Rule 9.5(4).

- A data holder is not excused from providing access to copies of records in a prompt manner by reason only that it would be inconvenient, time consuming or costly to do so.
- A data holder must provide the requested copies in the form (if any) approved by the Australian Competition and Consumer Commission.

Reporting requirements

- A data holder must prepare and submit a report for each reporting period to the OAIC and the ACCC, under CDR Rule 9.4.
- For information on these reporting requirements, see the ACCC's website (on 'reporting forms (Rule 9.4)').