Australian Government

Office of the Australian Information Commissioner

Guide to privacy for data holders

March 2023

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 27 March 2023	• 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 system for the conduct of its third-party service providers.
4.0	28 March 2023 to …	• Updated guidance to reflect amendments to the CDR Rules introduced by the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021* and *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 2) 2021*, including changes to reflect:

  - primary data holder responsibilities for shared responsibility data
  - data holders in the energy sector
  - joint accounts obligations in each CDR sector.
- Updated guidance to reflect amendments to the *Competition and Consumer Regulations 2010* introduced by the *Competition and Consumer Amendment (Consumer Data Right) Regulations 2021*, including changes to the privacy safeguard obligations applicable to energy retailers.

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]
- This Guide focuses on data holder privacy obligations for CDR data that is not SR (shared responsibility) data. For further information about primary data holder obligations in relation to SR data, see Appendix A.[2]
- 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), the Competition and Consumer (Consumer Data Right) Rules 2020 (CDR Rules) and the *Competition and Consumer Regulations 2010* (Competition and Consumer Regulations).
- 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.
- The Guide focuses on the key privacy obligations of data holders. For detailed guidance on other data holder compliance obligations under the CDR Rules and Consumer Data Standards, see the compliance guides for data holders in the banking and energy sectors issued by the Australian Competition and Consumer Commission (ACCC) and guidance issued by the Data Standards Body (DSB).
- 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 various privacy obligations, including obligations relating to:
  - the privacy safeguards
  - consumer data request services
  - managing disclosure options for joint accounts
  - disclosure of CDR data
  - authorisation
  - consumer dashboards
  - notification of consumers, and
  - maintaining and providing access to certain records.

[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] The Guide does not cover the privacy obligations of secondary data holders. This is because the Australian Energy Market Operator Limited (AEMO) is currently the only secondary data holder in the CDR system, and AEMO is exempt from most privacy obligations that usually apply to data holders. For further information on secondary data holders, see the CDR Privacy Safeguard Guidelines.

- 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.
- 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.[3]

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).[4] In the energy sector, an example of a data holder is a retailer.[5]
- In the CDR system, a data holder discloses CDR data to an accredited person where required or authorised to do so in response to a consumer data request.[6]
- 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[7]
  - the CDR data is held by (or on behalf of) the person on or after the earliest holding day[8]
  - 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[9]

---

[3] 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 the Privacy Act, sections 6C, 13 and 15.

[4] 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 Competition and Consumer Act, subsections 56AJ(1) and 56AJ(2); Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019, subsection 5(2).

[5] Retailers are specified as a relevant class of persons who hold CDR data in the designation instrument for the energy sector: see Competition and Consumer Act, subsections 56AJ(1) and 56AJ(2): Consumer Data Right (Energy Sector) Designation 2020, subsection 6(2) and section 12.

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

[7] The designation instruments for each sector set out matters including the classes of information that are subject to the CDR system. 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 Competition and Consumer Act, paragraph 56AC(2)(a).

[8] 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: Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019, subsection 5(3). For the energy sector, the earliest holding day is 1 July 2018: Consumer Data Right (Energy Sector) Designation 2020, subsection 6(3).

[9] 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].

- the person is not a designated gateway for the CDR data, AND
- any of the following three cases apply:[10]
  - **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
  - **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.[11]

- 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)[12]
  - providing consumer data request services
  - managing disclosure options for joint accounts, including by providing a disclosure option management service to joint account holders
  - 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.

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 in Chapter B (Key concepts) of the CDR Privacy Safeguard Guidelines are met by the entity): see Note 2 under the Competition and Consumer Act, section 56AJ.

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

[11] The conditions for the banking sector are contained in the CDR Rules, clause 7.2 of Schedule 3. The conditions for the energy sector are contained in the CDR Rules, clause 9.2 of Schedule 4.

[12] In the energy sector, AEMO is exempt from privacy safeguards 1, 11 and 13, and is exempt from privacy safeguard 10 in relation to CDR data held by AEMO that AEMO discloses to an energy retailer as required or permitted by the Competition and Consumer Act: Competition and Consumer Regulations, sub-regulation 28RA(2).

- 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.[13]
- 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.[14] These are not covered in this Guide. For information on these obligations, see the ACCC's compliance guides for data holders in the banking and energy sectors.

Staged application

The CDR Rules may provide for the 'staged application' of CDR Rules in a particular sector. Staged application means that the CDR Rules apply to a broader range of data holders or a broader range of CDR data within that sector over time. The result of staged application is that data holders may be required to comply with particular CDR data sharing obligations from different dates.

For further information on staged application, see Chapter B (Key concepts) of the CDR Privacy Safeguard Guidelines.

Does the Privacy Act apply to data holders?

- Where a data holder is an APP entity,[15] 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.[16]

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).

[13] For guidance regarding examples of data standards that are relevant to particular obligations, see the ACCC's compliance guidance for data holders.

[14] See, e.g, CDR Rules, rule 1.12 and Part 2.

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

[16] 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.

- Information about how to comply with these privacy safeguards is available in Chapters 1, 10, 11 and 13 of the CDR Privacy Safeguard Guidelines.

Services to make and manage consumer data requests

- The CDR Rules require data holders to provide particular services to accredited persons and consumers to assist in making and managing consumer data requests. The services required depend on the nature of the consumer and account type as outlined further below.

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.[17]
- 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 subrule 1.13(1)(b) of the CDR Rules.
- 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:[18]
  - For each non-individual consumer, and each consumer who is a partner in a partnership[19] – 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.[20]

[17] The CDR Rules also make provision for consumer data requests to be made directly by a CDR consumer to a data holder: CDR Rules, Part 3. A request directly from a CDR consumer must be made using a data holder's 'direct request service': CDR Rules, subrule 3.3(1). A data holder's 'direct request service' is an online service, that must comply with the data standards, that allows eligible CDR consumers to make consumer data requests under Part 3 of the CDR Rules directly to the data holder in a timely and efficient manner and allows consumers to receive the requested data in human-readable form: CDR Rules, subrule 1.13(2). However:

- for the banking sector, there is currently no compliance date for a data holder's obligations under Part 3 of the CDR Rules: CDR Rules, clause 6.6 of Schedule 3.
- for the energy sector, Part 3 of the CDR Rules does not apply in relation to energy sector data: CDR Rules, clause 8.5 of Schedule 4.

[18] Note 4 under the CDR Rules, subrule 1.13(c).

[19] That relates to a partnership account with the data holder: CDR Rules, paragraph 1.13(1)(d).

[20] CDR Rules, paragraphs 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 Rules, paragraph 1.13(1)(d).

- For each account in relation to which a person has account privileges[21] – a service that allows the account holder to make a secondary user instruction,[22] and withdraw that instruction.[23]

Joint accounts – disclosure options management

Disclosure options for joint accounts

- There are specific rules that apply to consumer data requests relating to joint accounts.
- Where joint account holders are 'eligible consumers',[24] data holders must allow them to choose what disclosure option applies to the joint account.[25] The options are:
  - **Pre-approval option**: this option is the least restrictive sharing preference and allows data on the joint account to be independently shared by all requesting joint account holders (without approval from other joint account holders). This option applies by default and must be offered on joint accounts.[26]
  - **Co-approval option**: this option is a more restrictive sharing preference and requires all joint account holders to approve the disclosure of joint account data before it may be shared.
  - **Non-disclosure option**: this option is the most restrictive sharing preference and means that joint account data cannot be disclosed under the CDR Rules.
- Data holders must offer the pre-approval option and non-disclosure option on joint accounts. Data holders may offer the co-approval option but are not required to.

Disclosure option management service

- Data holders must provide an online disclosure option management service to each joint account holder who is an eligible CDR consumer.[27] The disclosure option management service must allow the joint account holder to:[28]
  - change the disclosure option that applies to the account to a more restrictive option[29]

---

[21] 'Account privileges' for the banking sector is defined in the CDR Rules, clause 2.2 of Schedule 3. 'Account privileges' for the energy sector is defined the CDR Rules, clause 2.2 of Schedule 4.

[22] 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, rule 1.7. Relevant data standards can be found on the Data Standards Body's Consumer Data Standards website.

[23] CDR Rules, paragraph 1.13(1)(e).

[24] For the definition of 'eligible', see CDR Rules, rules 1.7 and 1.10B. There are additional criteria for eligibility in the banking and energy sectors. For the banking sector, see CDR Rules, clause 2.1 of Schedule 3. For the energy sector, see CDR Rules, clause 2.1 of Schedule 4. See also Chapter B (Key concepts).

[25] CDR Rules, rule 4A.5.

[26] While the pre-approval option applies by default to the joint account, any joint account holder can change the disclosure option to withdraw their presumed approval in relation to a request at any time.

[27] For the definition of 'eligible', see CDR Rules, rules 1.7 and 1.10B. There are additional criteria for eligibility in the banking and energy sectors. For the banking sector, see CDR Rules, clause 2.1 of Schedule 3. For the energy sector, see CDR Rules, clause 2.1 of Schedule 4. See also Chapter B (Key concepts).

[28] CDR Rules, rule 4A.6.

[29] CDR Rules, rules 4A.6 and 4A.7.

  - propose to the other joint account holders to change the disclosure option that applies to a less restrictive option,[30] and
  - respond to a proposal by another joint account holder to change the disclosure option.
- The disclosure option management service must meet the requirements set out in rule 4A.6 of the CDR Rules.[31]

Changing the disclosure option to a more restrictive option

- Data holders must allow each joint account holder to change to a more restrictive disclosure option using the disclosure option management service at any time, without needing the agreement of the other joint account holders.[32]
- That is, if the pre-approval option applies to a joint account, a joint account holder may at any time choose that the co-approval option or non-disclosure option will apply to the joint account. If the co-approval option applies, a joint account holder can use the disclosure option management service to apply the non-disclosure option.
- If a joint account holder applies a more restrictive disclosure option, the data holder must provide the other joint account holders with the information outlined in subrule 4A.7(3) of the CDR Rules.[33]

Obtaining agreement to change to a less restrictive disclosure option

- One joint account holder may use the disclosure option management service to propose a less restrictive disclosure option to the other joint account holders. The other account holders need to agree before that disclosure option will apply.
- That is, if the non-disclosure option applies, a joint account holder can use the disclosure option management service to propose the co-approval option (if offered by the data holder) or pre-approval option. If the co-approval option applies, a joint account holder can use the disclosure option management service to propose the pre-approval option. [34]
- Where a joint account holder makes a proposal to change to a less restrictive disclosure option, the data holder must provide the other joint account holders with the information outlined in subrules 4A.8(2) to 4A.8(3) of the CDR Rules.[35]

---

[30] CDR Rules, rules 4A.6 and 4A.8.

[31] See the ACCC's compliance guides for data holders in the banking and energy sectors and the Joint account implementation guidance for information on the requirements in CDR Rule 4A.6.

[32] CDR Rules, paragraph 4A.6(1)(a) and rule 4A.7.

[33] See the ACCC's compliance guidance for data holders and the Joint account implementation guidance for information on what must be provided. The Consumer Experience Guidelines also provide examples of how to present disclosure option changes for joint accounts.

[34] CDR Rules, paragraph 4A.6(1)(a) and rule 4A.8.

[35] See the ACCC's compliance guides for data holders in the banking and energy sectors and the Joint account implementation guidance for information on what must be provided. The Consumer Experience Guidelines also provide examples of how to present disclosure option changes for joint accounts.

Disclosing CDR data to 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).[36] This is a 'consumer data request' by an accredited person on behalf of a consumer.[37]
- The consumer data request must be made using the data holder's accredited person request service, in accordance with the data standards.[38]
- 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.[39]
- 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,[40] and
  - the request relates to 'required' consumer data.[41]
- 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
  - how authorisations must be managed, and
  - additional authorisation requirements for joint accounts.

[36] 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, there is currently no compliance date for a data holder's obligations under Part 3 of the CDR Rules: CDR Rules, clause 6.6 of Schedule 3.
- for the energy sector, Part 3 of the CDR Rules does not apply in relation to energy sector data: CDR Rules, clause 8.5 of Schedule 4.

[37] CDR Rules, rule 4.4.

[38] CDR Rules, subrule 4.4(3). Information regarding the 'accredited person request service' is contained under the section Consumer data request services.

[39] CDR Rules, rule 4.5.

[40] CDR Rules, subrules 4.6(1) and 4.6(4).

[41] CDR Rules, subrule 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 Rules, subrule 4.5(2)), but
- is not otherwise required to disclose requested 'voluntary' consumer data (CDR Rules, subrule 4.6(2)).

For information regarding 'voluntary' consumer data and 'required' consumer data and Chapter B (Key concepts) of the CDR Privacy Safeguard Guidelines. For the banking sector, see also CDR Rules, rule 1.7, clause 3.2 of Schedule 3; for the energy sector, see CDR Rules, clause 3.2 of Schedule 4.

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:[42]
  - receives a consumer data request from an accredited person (on behalf of an eligible CDR consumer),[43] and
  - does not already have a current authorisation to disclose the CDR data.[44]
- 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,[45] and
  - the authorisation is current.[46]
- 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.[47]
- When a data holder receives a consumer data request from an accredited person in relation to a joint account:[48]
  - if the pre-approval option applies to the joint account, the data holder must process the request as it would any other request on a non-joint account in accordance with rules 4.5 to 4.7 of the CDR Rules. That is, the data holder must comply with the rules for seeking authorisation and disclosing consumer data in response to a consumer data request.[49] If one account holder requests a disclosure of data, the other account holders are treated as having approved

[42] CDR Rules, rule 4.5.

[43] For the definition of an 'eligible' CDR consumer in the banking sector, see the CDR Rules, clause 2.1 of Schedule 3. For the energy sector, see the CDR Rules, clause 2.1 of Schedule 4. 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 Rules, paragraph 4.5(1)(c).

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

[45] 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).

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

[47] CDR Rules, rule 4.5. The authorisation requirements in Division 4.4 of the CDR Rules are outlined in the following sections of this Guide. The applicable data standards include the Authorisation Standards, Amending Authorisation Standards, CDR arrangement ID, Specifying an existing arrangement and Request Object Submission and Notification Standard, which 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.

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

[49] This must be done in accordance with CDR Rules, rules 4.5 to 4.7. However, if a relevant joint account holder withdraws their approval, the data holder must not disclose any or any further requested CDR data. See CDR Rules, subrules 4A.10(2) and 4A.10(3) for further information on consumer data requests relating to the pre-approval option.

disclosing the data relating to the joint account and the data holder must make the requested disclosure.

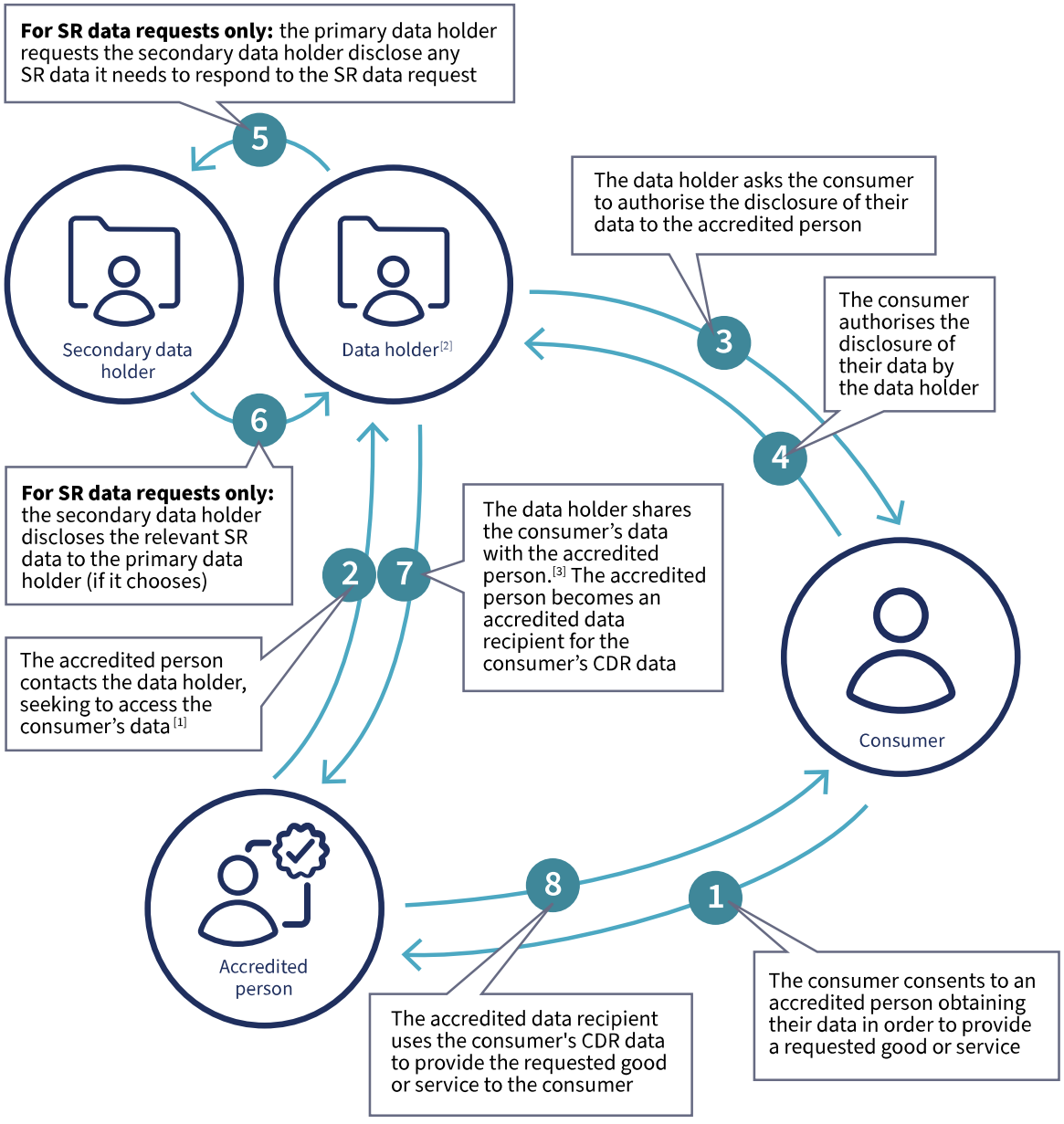
- if the co-approval option applies, the data holder must seek the requester's authorisation[50] and if this is given, invite the approval of the relevant account holders before disclosing data from the account[51]
- if the non-disclosure option applies, the data holder must refuse to disclose the requested CDR data.

- The following flow chart demonstrates the role of authorisation in the key information flow between a consumer, data holder(s) and an accredited person (including in relation to SR data requests, which are dealt with in Appendix A to this Guide). For flow charts that show key information flows involving CDR representative and sponsorship arrangements, see Chapter C of the Privacy Safeguard Guidelines.

[50] The data holder must ask the requester for authorisation in accordance with the CDR Rules, rule 4.5 and Division 4.4.

[51] The data holder must invite the approval of the relevant account holder in accordance with the CDR Rules, rule 4A.11.

Overview: key information flow in the CDR system



[1] If the accredited person is seeking CDR data that is or includes SR (shared responsibility) data, it contacts the primary data holder (rather than the secondary data holder)
[2] For SR data requests, this will be the primary data holder
[3] Where the data holder is a primary data holder and the secondary data holder has refused to disclose SR data to it, the primary data holder will not be able to share that SR data with the accredited person

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 rule 4.7 of the CDR Rules:
  - where the data holder considers this to be necessary to prevent physical, psychological or financial harm or abuse[52]
  - 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[53]
  - where the CDR data relates to an account that is blocked or suspended, or
  - where provided for in the data standards.[54]
- 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.[55]

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

- A data holder would not be required to seek an authorisation (and therefore would not disclose CDR data in response to that specific consumer data request) 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[56]
  - where the person who makes the request has account privileges, but the account holder has not provided a secondary user instruction for that person (or the account holder has provided a secondary user instruction for the person, but has subsequently withdrawn it),[57] or

[52] Certain 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.

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

[54] For example, in relation to unavailable accounts, the Consumer Experience Standards: Unavailable accounts deal with situations where a successfully authenticated user cannot proceed to establish an authorisation in accordance with the rules on eligible consumers and required consumer data.

[55] CDR Rules, rule 4.7. Relevant data standards can be found on the Data Standards Body's Consumer Data Standards website.

[56] This is because of the operation of the CDR Rules, paragraphs 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 the CDR Rules, rule 1.13.

[57] 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 is at least 18 years of age, 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 Rules, rule 1.7). 'Account privileges' for the banking sector is defined in the CDR Rules, clause 2.2 of Schedule 3. 'Account privileges' for the energy sector is defined in the CDR Rules, clause 2.2 of Schedule 4).

- where the consumer data request relates to a joint account and the non-disclosure option applies to the account.[58]

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.[59]
- In ensuring processes are easy to understand, a data holder must also have regard to the Consumer Experience Guidelines.[60]

Information to be provided

- When asking a consumer to give or amend a current authorisation, a data holder must provide the consumer with the following information as required by rule 4.23 of the CDR Rules:
  - 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 may be affected by the earliest holding day in the relevant sector)[61]
  - the types of CDR data that will be disclosed (the data holder must use the Data Language Standards to describe the CDR data)[62]

---

[58] CDR Rules, subrules 4A.10(1) and (6).

[59] CDR Rules, rule 4.22.

[60] CDR Rules, 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.

[61] 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 (Competition and Consumer Act, paragraph 56AJ(1)(b)). Under the designation instrument for the banking sector, the earliest holding day is 1 January 2017: Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019, subsection 5(3). Under the designation instrument for the energy sector, the earliest holding day is 1 July 2018: Consumer Data Right (Energy Sector) Designation 2020, subsection 6(3). This means that consumer data requests may be made for CDR data dating back to 1 January 2017 in the banking sector, and 1 July 2018 in the energy sector.

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 data holder before the earliest holding day: Competition and Consumer Act, paragraph 56AJ(1)(ba). An example of CDR data that would meet this criterion is a current account number: Explanatory Memorandum, Treasury Laws Amendment (2020 Measures No. 6) Bill 2020, [2.35].

[62] The Data Language Standards 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 help ensure there is a consistent

- whether the authorisation relates to a 'one-off' disclosure, or an ongoing disclosure over a period of time (no more than 12 months)[63]
- if authorisation is being sought for an ongoing disclosure — what the time period is (no more than 12 months)[64]
- 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

- Rule 4.24 of the CDR Rules 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

- Generally, once a data holder has received authorisation, or an amendment to authorisation, from the relevant consumer/s, the data holder:
  - *must* disclose the required consumer data (subject to rules 4.6A and 4.7 of the CDR Rules),[65] and
  - *may* disclose the relevant voluntary consumer data (subject to rule 4.6A of the CDR Rules).[66]
- Additional requirements apply if the account is a joint account and the co-approval option applies.[67] In these circumstances, the data holder will only be required or authorised to disclose

interpretation and description of the consumer data that will be shared in the CDR system. See Competition and Consumer Act, section 56FA; CDR Rules, rule 8.11.

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

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

[65] CDR Rules, subrule 4.6(4). For 'required consumer data' in the banking sector, see CDR Rules, subclause 3.2(1) of Schedule 3. For 'required consumer data' in the energy sector, see CDR Rules, clause 3.2 of Schedule 4. For further information, see Chapter B (Key concepts) of the CDR Privacy Safeguard Guidelines.

[66] CDR Rules, subrule 4.6(2). For 'voluntary consumer data' in the banking sector, see CDR Rules, clause 3.2(2) of Schedule 3. For 'voluntary consumer data' in the energy sector, see CDR Rules, clause 3.1 of Schedule 4. For further information, see Chapter B (Key concepts) of the CDR Privacy Safeguard Guidelines.

[67] See the 'Disclosure options for joint accounts' section for further information on these options.

the relevant CDR data if the requester has authorised the disclosure *and* each relevant joint account holder has approved the disclosure.[68]

- The data holder must disclose the data via its accredited person request service, and in accordance with the data standards.[69]
- A data holder must not charge a fee for the disclosure of required consumer data.[70]

Approval from relevant joint account holders

- As explained above, one disclosure option for joint accounts is co-approval.[71] If the co-approval option applies and the requesting joint account holder authorises the disclosure of CDR data, the data holder must ask all relevant account holders for their approval to disclose that data.[72] The data holder must not disclose the data unless all relevant account holders have given their approval.
- When seeking approval, the data holder must use its ordinary means of contacting each relevant account holder.[73] The data holder must ask each account holder to approve or not approve the disclosure,[74] and provide the following information required by rule 4A.11 of the CDR Rules:
  - that an accredited person has requested the disclosure of CDR data that relates to the joint account on behalf of the requesting joint account holder
  - that the requesting joint account holder has authorised disclosure of the joint account data (under Division 4.4 of the CDR Rules)
  - the information referred to in paragraphs 4.23(1)(a)-(e) of the CDR Rules, in so far as they relate to the request[75]
  - the time by which the data holder needs an approval, and the fact that the joint account data will not be disclosed if the approval is not received by that time, and
  - that any relevant account holder may withdraw their approval using the consumer dashboard at any time (and the effect of removing the approval).
- If all relevant account holders give their approval, the data holder must comply with rules 4.6 to 4.7 of the CDR Rules in relation to disclosing the joint account data.[76]

---

[68] See CDR Rules, paragraph 4A.5(1)(b). The requirements for asking relevant account holders for approval to disclose joint account data are outlined below.

[69] CDR Rules, rule 4.6. Information regarding the 'accredited person request service' is available under Consumer data request services.

[70] Competition and Consumer Act, section 56BU.

[71] Further information is available under the 'Disclosure options for joint accounts' heading in this Guide.

[72] Data holders must provide the pre-approval and non-disclosure options for joint accounts and may provide the co-approval option: CDR Rules, subrules 4A.5(1)(2)-(3).

[73] CDR Rules, rule 4A.11.

[74] CDR Rules, paragraphs 4A.11(d).

[75] Further information about these requirements is available under the 'Information to be provided' heading in this Guide.

[76] CDR Rules, paragraph 4A.10(4)(c).

- Approvals generally last for the same period as the associated authorisation to disclose CDR data.[77] However, any relevant account holder may withdraw their approval at any time using their consumer dashboard.[78]

Tip: For an example of the authorisation flow with co-approval joint accounts see the Consumer Experience Guidelines.

Situations where a data holder may refuse to or must not disclose CDR data once an authorisation is received

- Despite having received an authorisation (and where necessary, approval), or an amendment to authorisation, a data holder may refuse to disclose required consumer data in the following circumstances as outlined in rule 4.7 of the CDR Rules:
  - where the data holder considers this to be necessary to prevent physical, psychological or financial harm or abuse[79]
  - 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[80]
  - 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.[81]
- A data holder must not disclose CDR data that relates to a particular account if:
  - 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 to that accredited person in response to requests by or on behalf of that secondary user, [82] or

---

[77] CDR Rules, subrule 4A.12(1).

[78] CDR Rules, subrule 4A.12(2).

[79] In addition, a data holder is not liable for a failure to comply with their joint account obligation under Part 4A of the CDR Rules if it considered that the relevant act or omission was necessary in order to prevent physical, psychological or financial harm or abuse to any person. CDR Rules, rule 4A.15. Data holders (e.g. banks) may also 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.

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

[81] CDR Rules, rule 4.7. Relevant data standards can be found on the Data Standards Body's Consumer Data Standards website.

[82] CDR Rules, rule 4.6A. A person will be a secondary user if the person is at least 18 years of age, 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

  - a Schedule to the CDR Rules provides that the CDR data must not be disclosed. [83]
- 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.[84]Where a data holder has received a temporary direction from the Accreditation Registrar to refrain from processing consumer data requests, the data holder must not disclose CDR data in response to a consumer data request contrary to this direction.[85]

Tip: if the account is a joint account and the data holder considers it necessary to prevent physical, psychological, or financial harm or abuse, the data holder may:

- if the non-disclosure option applies, refuse to invite the relevant account holder(s) to agree to a different disclosure option before disclosing data relating to the joint account
- if the co-approval disclosure option applies, refuse to seek the approval of the relevant account holder(s) before disclosing data on the joint account
- refuse to provide relevant account holder(s) with a consumer dashboard or to update an existing dashboard with details regarding a joint account.[86]

How authorisations must be managed

Consumer dashboards

- A consumer dashboard is an online service which data holders must offer (and in most circumstances provide) to a consumer, following receipt of a consumer data request from an accredited person (on behalf of that consumer).[87]
- 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.
- A data holder must provide a consumer dashboard to a CDR consumer in the circumstances specified in the relevant sector schedule to the CDR Rules:[88]

---

user for the purposes of the CDR Rules (i.e. a secondary user instruction) (CDR Rules, rule 1.7). 'Account privileges' for the banking sector are defined in the CDR Rules, clause 2.2 of Schedule 3. 'Account privileges' for the energy sector is defined in the CDR Rules, clause 2.2 of Schedule 4. 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.

[83] CDR Rules, rule 4.6A. Schedule 3 (which relates to the banking sector) and Schedule 4 (which relates to the energy sector) do not currently include provisions for CDR Rule 4.6A.

[84] See Note 3 to CDR Rules, rule 1.13, citing paragraphs 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.)

[85] CDR Rules, rule 5.34.

[86] Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021, Explanatory Statement.

[87] CDR Rules, rule 1.15.

[88] For the banking sector, see CDR Rules, clause 2.3 of Schedule 3. For the energy sector, see CDR Rules, clause 2.3 of Schedule 4.

  - In the banking sector, when a data holder receives a consumer data request from an accredited person on behalf of an eligible CDR consumer, it must provide a consumer dashboard.
  - In the energy sector, when a data holder receives a consumer data request from an accredited person on behalf of a CDR consumer who:
    - has online access to the relevant account, it must provide a consumer dashboard, or
    - does not have online access to the relevant account, it must offer the CDR consumer a consumer dashboard and provide it if the CDR consumer accepts.[89]
- The general requirements for the dashboard are contained in subrule 1.15(1) of the CDR Rules 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.
- Where a consumer dashboard is provided to a consumer, it should be provided as soon as practicable after the data holder receives the relevant consumer data request.[90]
- The consumer dashboard must contain the following details for each authorisation:[91]
  - the CDR data to which the authorisation relates
  - the date on which the consumer gave the authorisation
  - the period for which the consumer gave the 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
    - the accredited data recipient for the CDR data, and[92]
  - 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.[93]

---

[89] Energy retailers must offer offline CDR consumers a dashboard and provide it if the CDR consumer accepts: CDR Rules, clause 2.3 of Schedule 4. For further information on offline consumers in the energy sector, see Chapter B (Key concepts).

[90] This is to assist the data holder in complying with its obligation under Privacy Safeguard 10 and CDR 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.

[91] CDR Rules, paragraph 1.15(1)(b) and subrule 1.15(3).

[92] 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 Rules, rule 7.9 and Chapter 10 (Privacy Safeguard 10) of the CDR Privacy Safeguard Guidelines.

[93] 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 Competition and Consumer Act, section 56EN(4) and Chapter 11 (Privacy Safeguard 11) of the CDR Privacy Safeguard Guidelines.

- The consumer dashboard must have a functionality that allows the consumer to withdraw authorisation at any time. This functionality must:[94]
  - be simple and straightforward to use, and prominently displayed,[95] 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 rule 1.15 of the CDR Rules in the data standards or on the Register of Accredited Persons.[96]
- A data holder must update a consumer's dashboard as soon as practicable after the information required to be contained on the dashboard changes.[97]

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.

Non-individuals and partnership

- 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.[98]

Secondary users

- Where the consumer is a secondary user,[99] in addition to providing the secondary user with a dashboard, the data holder must also ensure the dashboard for the relevant account holder:[100]
  - contains the details listed above about each authorisation given by that secondary user

[94] CDR Rules, paragraph 1.15(1)(c).

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

[96] CDR Rules, paragraphs 1.15(1)(ba) and 1.15(1)(bb).

[97] CDR Rules, rule 4.27.

[98] CDR Rules, subrule 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, paragraphs 1.13(1)(c) and 1.13(1)(d).

[99] A person is a 'secondary user' for an account with a data holder if the person is at least 18 years of age, 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 Rules, rule 1.7). 'Account privileges' for the banking sector are defined in the CDR Rules, clause 2.2 of Schedule 3. 'Account privileges' for the energy sector is defined in the CDR Rules, clause 2.2 of Schedule 4.

[100] CDR Rules, subrules 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 on behalf of that secondary user [101]
  - allows the account holder to withdraw the secondary user instruction
  - is simple and straightforward to use,[102] and prominently displayed
  - is no more complicated to use than the processes for giving the authorisations or instructions, 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,[103] the requirements listed above can be provided via an online service.[104]

Joint accounts

- Data holders must provide all relevant account holders with a consumer dashboard for managing approvals to disclose CDR data in relation to their joint account. This requirement applies where either the co-approval option or the pre-approval option applies, or has applied, to the joint accounts.[105]
- The consumer dashboard must meet the requirements for individual account dashboards outlined above.
- Where a data holder already provides a consumer dashboard for a relevant account holder because that consumer is sharing CDR data from another account, that existing dashboard must be used.[106]
- All joint account holders should be able to view the same details about each approval as the requesting account holder.[107]

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.[108]

---

[101] 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 under CDR Rules, subrule 1.15(5), citing subrules 4.6(2), 4.6(4) and 4.6A(1).

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

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

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

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

[106] CDR Rules, rule 4A.13(2).

[107] CDR Rules, rule 4A.13(5).

[108] CDR Rules, subrule 4.25(1). In relation to joint account holders, a joint account holder may withdraw their approval at any time (CDR Rules, paragraph 4A.13(d)(ii)). 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 Rules, paragraph 1.15(5)(b)(ii). However, a joint account holder cannot withdraw the authorisations given by other account holders or secondary users.

- Where a consumer withdraws authorisation, the data holder must give effect to the withdrawal as soon as practicable, and in any case within 2 business days after receiving the withdrawal.[109] The data holder must also notify the accredited person of the withdrawal in accordance with the data standards.[110]
- 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.[111]

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.[112]
- The alternative method of communicating the withdrawal of authorisation must be simple.[113] 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,[114] for example through their telephone helpline.

[109] CDR Rules, paragraph 4.25(2)(a).

[110] CDR Rules, paragraph 4.25(2)(b).

[111] CDR Rules, subrule 4.25(1).

[112] CDR Rules, paragraph 1.15(1)(c). See for example the Consumer Experience Standards on withdrawing authorisation: consequences and withdrawing authorisation: redundant data.

[113] CDR Rules, subrule 4.25(1).

[114] 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.[115] 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.[116]
- 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 2 business days after receiving the communication.[117]
- 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,[118] as required by rule 4.27 of the CDR Rules.[119]

When an authorisation expires

- Upon an authorisation expiring, CDR data can no longer be shared with the relevant accredited person. Rule 4.26 of the CDR Rules 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 2 business days after receiving the communication, whichever is sooner.
  - **Upon the consumer ceasing to be 'eligible'**[120]
    - For example, the consumer no longer holds any open accounts with the data holder.
  - **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.

---

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

[116] CDR Rules, subrule 4.26(1).

[117] CDR Rules, subrule 4.26(1).

[118] CDR Rules, paragraph 1.15(3)(e).

[119] 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.

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

- **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.[121]
- **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 consumer 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.[122]
    - **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. [123]
    - **Additional notification obligation – joint accounts**
        - If the relevant account is a joint account, the data holders must provide a notice (called an 'approval notification') to:
            - a relevant account holder, where the requester has given, amended or withdrawn an authorisation, or the authorisation has expired, or

[121] As a result of the CDR Rules, subclause 7.2(3)(b) of Schedule 3 and clause 9.2 of Schedule 4; Competition and Consumer Act, subsection 56AJ(4).

[122] 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 the CDR Rules, rule 7.9 and Chapter 10 (Privacy Safeguard 10) of the CDR Privacy Safeguard Guidelines.

[123] CDR Rules, rule 4.27.

        - the requester, where relevant account holder(s) have not given approval for disclosure within the relevant timeframe, or have withdrawn an approval.[124]
    - The data holder must provide the approval notification as soon as practicable after the relevant event occurs, unless the joint account holder has selected an alternative schedule of notifications.[125] The notification must be given through the data holder's ordinary means of contacting the joint account holder(s).[126]
- **Additional notification obligation – 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.[127]

Liability for third-party service providers

- In certain circumstances, a data holder may be accountable under the CDR system 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.[128]
- The CDR system 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 system 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 system 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).[129] The CDR system also regulates CDR representative arrangements to which an accredited data recipient is a party, and an accredited data recipient is liable for the conduct of its CDR representatives under that arrangement.[130]

---

[124] CDR Rules, subrule 4A.14(1). The approval notification must be given in accordance with the Consumer Experience Standards.

[125] CDR Rules, paragraph 4A.14(2)(a). The reference to an 'alternative schedule of notifications' in this paragraph relates to CDR Rules, subrule 4A.14(3), which provides that the data holder must (in accordance with any relevant data standards)provide for alternative notification schedules (including reducing the frequency of notifications or not receiving notifications), and give each joint account holder a means of selecting such an alternative, and of changing a selection. See the Consumer Experience Standards for a non-exhaustive list of options that data holders may implement to support their compliance with these rules.

[126] CDR Rules, paragraph 4A.14(2)(b).

[127] CDR Rules, rule 4.28. Notification must be provided through the data holder's ordinary means of contacting the account holder: CDR Rules, subrule 4.28(2).

[128] 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 section 56AU(1), which provides that the conduct of agents of a CDR entity are attributable to the CDR entity, and section 84.

[129] See CDR Rules, rule 1.10. For further information on outsourced service providers, see Chapter B (Key concepts) in the CDR Privacy Safeguard Guidelines.

[130] See CDR Rules, rule 1.10AA. For further information on CDR representatives, see Chapter B (Key concepts) in the CDR Privacy Safeguard Guidelines.

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.[131]
- Data holders are required to keep and maintain these and other records under the CDR Rules.[132]
- 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.[133]
- In adopting a timetable that is 'as soon as practicable', a data holder can take technical and resource considerations into account.
- 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 ACCC.

Reporting requirements

- A data holder must prepare and submit a report for each reporting period to the OAIC and the ACCC, under rule 9.4 of the CDR Rules. Data holders are required to complete and submit their reports by entering information into the CDR Participant Portal.
- For information on these reporting requirements and using CDR Participant Portal, see the ACCC's website (on 'reporting forms (Rule 9.4)') and ACCC's Participant Portal User Guide.

[131] CDR Rules, subrule 9.5(1). CDR complaint data is defined in the CDR Rules, rule 1.7.

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

[133] CDR Rules, subrule 9.5(4).

Appendix A – primary data holder obligations in relation to SR (shared responsibility) data

- This appendix outlines key privacy obligations for primary data holders in relation to SR (shared responsibility) data.[134] As the energy sector is currently the only CDR sector with primary data holders, this appendix focuses on the energy sector.
- Primary data holders should read this appendix in conjunction with the body of this Guide (which covers obligations in relation to non-SR data) and the CDR Privacy Safeguard Guidelines.[135] For further guidance on primary and secondary data holders, including information about AEMO, data holders should refer to Chapter B (Key concepts) of the CDR Privacy Safeguard Guidelines.

What is SR data?

- SR data is a type of CDR data.[136] CDR data may be specified as SR data where it is held by one data holder (the secondary data holder), but it would be more practical for consumer data requests for the data to be directed to a different data holder (the primary data holder).[137]
- Under current arrangements, the only CDR sector with SR data is the energy sector. In the energy sector, certain NMI (national metering identifier) standing data, metering data and DER (distributed energy resource) register data is specified as SR data.[138]

Who is a primary data holder for SR data?

- Certain data holders will be 'primary' or 'secondary' data holders under the CDR Rules. A person will be a primary data holder for SR data if:
  - the person is a data holder (according to the criteria in section 56AJ of the Competition and Consumer Act), and
  - the person is specified as a primary data holder for the SR data in a sector schedule to the CDR Rules.[139]
- In the energy sector, retailers are specified as primary data holders for SR data.[140]

---

[134] The privacy obligations of secondary data holders are not covered in this appendix. This is because the Australian Energy Market Operator Limited (AEMO) is currently the only secondary data holder in the CDR system, and AEMO is exempt from most privacy obligations usually applicable to data holders.

[135] 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.

[136] See section 56AI of the Competition and Consumer Act for the definition of CDR data. See rule 1.7 of the CDR Rules for the definition of SR data.

[137] Explanatory Statement, Competition and Consumer (Consumer Data Right) Amendment Rules (No. 2) 2021, page 5.

[138] CDR Rules, clauses 4.3 and 1.2 of Schedule 4.

[139] CDR Rules, subrule 1.7(1).

[140] Clause 4.3 of Schedule 4 of the CDR Rules. See also clause 1.4 of Schedule 4 of the CDR Rules for the definition of 'retailer'. AEMO is specified as the secondary data holder: CDR Rules, clause 4.3 of Schedule 4.

Which CDR privacy obligations apply to primary data holders in relation to SR data?

- Primary data holders will have a pre-existing relationship with the consumer, and from the consumer's perspective will be treated as the data holder for all relevant CDR data.[141] This means consumer data requests for SR data will be made to the primary data holder. The primary data holder will then seek authorisation for disclosure of requested SR data, disclose or refuse to disclose SR data, receive any complaints, and keep records relating to SR data requests.[142]
- To reflect this role, the CDR Rules apply certain existing and modified privacy obligations to primary data holders in relation to SR data. The CDR Rules also create certain additional privacy obligations for primary data holders in relation to SR data.
- At a high level, primary data holder privacy obligations include requirements related to:
  - Privacy Safeguards 1, 10 and 13
  - SR data requests and disclosing SR data in response to a consumer data request
  - asking consumers to give or amend authorisations for disclosure of SR data
  - providing consumer dashboards for SR data
  - notifying consumers of certain matters in relation to their SR data sharing arrangements, and
  - providing access to copies of records, where requested by consumers.

Does the Privacy Act apply to primary data holders?

- Where a primary data holder is an APP entity,[143] it must continue to comply with the Privacy Act.
- In the energy sector, where Privacy Safeguard 13 (correction of CDR data) applies to a primary data holder in relation to SR data (with relevant modifications),[144] APP 13 (correction of personal information) will not apply.[145]

Privacy Safeguards

- In the energy sector, primary data holders (retailers) must comply with the following privacy safeguards in relation to SR data (which will be AEMO data):[146]
  - Privacy Safeguard 1 (open and transparent management of CDR data)

---

[141] Explanatory Statement, Competition and Consumer (Consumer Data Right) Amendment Rules (No. 2) 2021, page 4.

[142] See CDR Rules. See also Explanatory Statement, Competition and Consumer (Consumer Data Right) Amendment Rules (No. 2) 2021, page 4.

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

[144] Further information about how Privacy Safeguard 13 is modified for primary data holders in relation to SR data, see Chapter 13 (Privacy Safeguard 13) of the CDR Privacy Safeguard Guidelines.

[145] Competition and Consumer Act, paragraph 56EC(4)(c). 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.

[146] Competition and Consumer Regulations 2010, sub-regulations 28RA(3)-(4).

  - Privacy Safeguard 10 (notifying of the disclosure of CDR data), and
  - Privacy Safeguard 13 (correction of CDR data), with certain modifications.
- This reflects that the secondary data holder in the energy sector (AEMO) is exempt from certain privacy safeguards that usually apply to data holders.[147]
- Information about how to comply with these privacy safeguards is available in Chapters 1, 10 and 13 of the CDR Privacy Safeguard Guidelines.

SR data requests

- An accredited person may request that a primary data holder disclose a consumer's CDR data to them (following a request from the consumer to do so).[148] Where such a request is for data that is or includes SR data, it is called an 'SR data request'.[149]
- Rule 1.13 of the CDR Rules, which relates to consumer data request services, applies to the primary data holder as if it were a data holder for the SR data. Accredited persons will use the 'accredited person request service' required by rule 1.13 to make SR data requests to the primary data holder.[150]
- Further information about rule 1.13 and consumer data request services is available in the body of this Guide.

Responding to SR data requests

- When a primary data holder receives an SR data request, it must follow the requirements in rule 4.5 of the CDR Rules as if it were a data holder for the SR data.[151] This means the primary data holder must ask the relevant eligible CDR consumer to authorise disclosure of the CDR data.[152] The

[147] In the energy sector, AEMO is exempt from privacy safeguards 1, 11 and 13, and is exempt from privacy safeguard 10 in relation to CDR data held by AEMO that AEMO discloses to an energy retailer as required or permitted by the Competition and Consumer Act: see reg 28RA(2) of the Competition and Consumer Regulations 2010.

[148] The CDR Rules also make provision for SR data request to be made directly by a CDR consumer to a primary data holder using the primary data holder's 'direct request service': CDR Rules, subrule 1.22(2). Currently, the energy sector is the only CDR sector with SR data. Part 3 of the CDR Rules (Consumer data requests made by eligible CDR consumers) does not apply to energy sector data: CDR Rules, clause 8.5 of Schedule 4. This means that currently, no CDR consumers will be able to directly make an SR data request.

[149] CDR Rules, rule 1.7. If a consumer is eligible to initiate a consumer data request to a primary data holder for SR data, the consumer is not also eligible to initiate a such a request to the secondary data holder: CDR Rules, rule 1.19.

[150] CDR Rules, subrules 1.20(1), 1.22(2) and 1.23(2).

[151] CDR Rules, subrule 1.23(3).

[152] See the body of this guide for further information about CDR Rule 4.5.

primary data holder must also provide the consumer dashboard according to rule 1.15 of the CDR Rules,[153] and follow the requirements in Division 4.4 in relation to authorisations.[154]

- If the consumer authorises the primary data holder to disclose SR data, the primary data holder must request the relevant SR data from the secondary data holder.[155] The primary data holder must do this in accordance with the data standards and using the secondary data holder's relevant online request service.[156]
- The secondary data holder will disclose the requested SR data to the primary data holder in accordance with the data standards, or will notify the primary data holder of its refusal to disclose the information.[157]
- If the secondary data holder discloses the requested SR data to the primary data holder, the primary data holder must comply with the requirements in rule 4.6 of the CDR Rules in relation to disclosing the SR data.[158] As with other CDR data, the primary data holder may refuse to disclose SR data in the circumstances outlined in rule 4.7 of the CDR Rules.[159] The primary data holder must also comply with rule 4.13 of the CDR Rules, regarding withdrawal of consent, for any relevant SR data.[160]
- Further information about the requirements in rules 4.5–4.7, rule 1.15, and Division 4.4 of the CDR Rules is available in the body of this Guide. The flow chart at page 15 also demonstrates the key information flow between a consumer, the primary and secondary data holders and an accredited person.

Additional privacy obligations related to SR data

Using SR data for other purposes

- Primary data holders must not use or disclose SR data they receive from a secondary data holder in response to an SR data request for a purpose other than responding to the SR data request.[161]

---

[153] CDR Rule 1.15 applies in relation to an SR data request as if the primary data holder were the data holder for the requested SR data: CDR Rules, subrule 1.21.

[154] Division 4.4. applies as if a reference to a data holder were a reference to the primary data holder: CDR Rules, subrule 1.23(11). CDR Rule 4.25(2) in Division 4.4 is modified so that giving effect to withdrawal includes cancelling any current requests to the secondary data holder under subrule 1.23(4). Further information about Division 4.4 is in the body of this Guide.

[155] CDR Rules, subrule 1.23(4).

[156] CDR Rules, subrule 1.23(4). While a secondary data holder is not required to provide an accredited person request service, it must provide an online service that can be used by the primary data holder to request any SR data it needs to respond to an SR data request. The service must enable the secondary data holder to disclose the data to the primary data holder in machine-readable form, and must conform with the data standards: CDR Rules, subrule 1.20(2).

[157] CDR Rules, subrules 1.23(5)-(6).

[158] CDR Rule 4.6 applies to the primary data holder as if it were the data holder for any SR data covered by the SR data request: subrule 1.23(7), subject to subrule 1.23(8).

[159] CDR Rules, subrule 1.23(9).

[160] CDR Rules, subrule 1.23(10).

[161] CDR Rules, paragraph 1.24(2)(a).

Once the primary data holder has responded to the SR data request, it must follow the CDR data deletion process in rule 1.18 of the CDR Rules.[162]

Dealing with unsolicited SR data

- Primary data holders have special obligations in relation to SR data which they collect from a secondary data holder purportedly under the CDR Rules, but not as the result of seeking to collect that SR data under the CDR Rules. For example, this could occur if SR data is disclosed to the primary data holder in error. Specifically, the primary data holder must, as soon as practicable, destroy this SR data, provided that the primary data holder is not required to retain it by or under an Australian law or court/tribunal order.[163]

Record keeping

- In addition to usual record keeping requirements in subrule 9.3(1) of the CDR Rules, the primary data holder must also keep and maintain records that record and explain any requests it makes to the secondary data holder for SR data, and disclosures of SR data or refusals to disclose SR data from secondary data holders.[164] Unlike certain other records, the primary data holder is not required to provide copies of these records to a CDR consumer upon their request.[165]

[162] CDR Rules, paragraph 1.24(2)(b).

[163] CDR Rules, rule 1.25.

[164] In other words, the records must record and explain any requests for SR data made under subrule 1.23(4) and responses received under subrule 1.23(5) or (6): CDR Rules, paragraph 9.3(1)(ca).

[165] CDR Rules, subrule 9.5(4).