Competition and Consumer (Consumer Data Right) Amendment Rules (No. 2) 2020

The Australian Competition and Consumer Commission makes the following rules.

Dated 1 October 2020

R G Sims
The Australian Competition and Consumer Commission

Contents

1 Name

This instrument is the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 2) 2020*.

2 Commencement

(1) Each provision of this instrument specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

Commencement information

Column 1	Column 2	Column 3
Provisions	**Commencement**	**Date/Details**
1. The whole of this instrument	The day after this instrument is registered	

Note: This table relates only to the provisions of this instrument as originally made. It will not be amended to deal with any later amendments of this instrument.

(2) Any information in column 3 of the table is not part of this instrument. Information may be inserted in this column, or information in it may be edited, in any published version of this instrument.

3 Authority

This instrument is made under section 56BA of the *Competition and Consumer Act 2010*.

4 Schedules

Each instrument that is specified in a Schedule to this instrument is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this instrument has effect according to its terms.

Schedule 1—Amendments

Competition and Consumer (Consumer Data Right) Rules 2020

1 Subrule 1.6(11)

Omit "receive CDR data", substitute "hold CDR data (service data)".

2 Subrule 1.7(1)

Insert:

service data has the meaning given by rule 1.10.

3 After subrule 1.7(4)

Insert:

References to ***accredited person***

(5) In these rules, unless the contrary intention appears, a reference to an accredited person making a consumer data request, collecting consumer data, obtaining consents, providing a consumer dashboard, or using or disclosing CDR data does not include a reference to an accredited person doing those things on behalf of a principal in its capacity as the provider in an outsourced service arrangement, in accordance with the arrangement.

4 Rule 1.10

Repeal the rule, substitute:

1.10 Meaning of *outsourced service provider* and related terms

(1) For these rules, where two persons are the principal and the provider in a CDR outsourcing arrangement, the provider is an ***outsourced service provider*** of the principal.

(2) For these rules, a ***CDR outsourcing arrangement*** is a written contract between a person (the ***principal***) and another person (the ***provider***) under which:

(a) the provider will do one or both of the following:

(i) if the provider is an accredited person—collect CDR data from a CDR participant in accordance with these rules on behalf of the principal;

(ii) in any case—provide goods or services to the principal using CDR data disclosed to it by the principal; and

(b) the provider is required to comply with the following requirements in relation to any service data:

(i) the provider must take the steps in Schedule 2 to protect the service data as if it were an accredited data recipient; and

(ii) the provider must not use or disclose the service data other than in accordance with a contract with the principal; and

(iii) the provider must, when so directed by the principal, do any of the following:

(A) provide the principal with access to any service data that it holds;

(B) return to the principal CDR data that the principal disclosed to it;

(C) delete any service data that it holds in accordance with the CDR data deletion process;

(D) provide, to the principal, records of any deletion that are required to be made under the CDR data deletion process;

(E) direct any other person to which it has disclosed CDR data to take corresponding steps; and

(iv) where the provider is to collect CDR data under the contract as mentioned in subparagraph (a)(i)—the provider must not further outsource that collection; and

(v) the provider must not disclose any service data to another person, otherwise than under a further CDR outsourcing arrangement; and

(vi) if the provider does disclose such CDR data in accordance with subparagraph (v), it must ensure that the other person complies with the requirements of the further CDR outsourcing arrangement.

Note: See rule 1.18 for the definition of "CDR data deletion process".

(3) For subparagraph (2)(a)(ii), the principal is taken to disclose CDR data to the provider if the principal gives the provider permission to access or use CDR data collected by the provider on behalf of the principal.

(4) For these rules, the ***service data*** in relation to a CDR outsourcing arrangement consists of any CDR data that:

(a) was collected from a CDR participant in accordance with the arrangement; or

(b) was disclosed to the provider in the CDR outsourcing arrangement for the purposes of the arrangement; or

(c) directly or indirectly derives from such CDR data.

5 Rule 1.16

Repeal the rule, substitute:

1.16 Obligations relating to CDR outsourcing arrangements

(1) If an accredited person is the principal in a CDR outsourcing arrangement, it must ensure that the provider complies with its requirements under the arrangement.

Note: This rule is a civil penalty provision (see rule 9.8).

(2) If an accredited person collects CDR data on behalf of another accredited person (the ***principal***) under a CDR outsourcing arrangement:

(a) rule 7.4 and rule 7.9 apply only in relation to the principal; and

(b) paragraph 7.10(1)(a) requires the principal to be identified.

6 Paragraph 1.18(c)

After "disclosed that CDR data", insert ", or who has collected CDR data on its behalf,".

7 Paragraph 4.11(3)(f)

After "disclosed to", insert ", or collected by,".

8 Paragraph 4.11(3)(f)

After "(including one that is based overseas)", insert "of the accredited person".

9 Paragraph 7.2(4)(b)

After "outsourced service providers", insert "of the accredited data recipient".

10 Rule 7.4 (note)

Repeal the note, substitute:

Note 1: See paragraph 1.14(3)(h).

Note 2: See rule 1.16 for how this rule applies in the case of a CDR outsourcing arrangement in which a provider collects CDR data on behalf of a principal.

11 Paragraph 7.5(1)(d)

After "outsourced service provider", insert "of the accredited data recipient under a CDR outsourcing arrangement".

12 At the end of paragraph 7.5(1)(e)

Add:

; (f) where the accredited data recipient collected the CDR data as a provider in a CDR outsourcing arrangement—disclosing service data to the principal under the arrangement.

13 Paragraph 7.5(3)(c)

After "outsourced service provider", insert "of the accredited data recipient".

14 Subrules 7.6(2) and (3)

Repeal the subrules, substitute:

(2) For this rule:

(a) any use or disclosure of service data by the provider under a CDR outsourcing arrangement is taken to have been by the principal under the arrangement; and

(b) it is irrelevant whether the use or disclosure:

(i) is in accordance with the arrangement; or

(ii) is taken to have been by the provider by an application of this subrule to another CDR outsourcing arrangement in which it is the principal.

Note: See rule 1.10 for the definition of "service data".

15 At the end of rule 7.9

Insert:

Note 4: See rule 1.16 for how this rule applies in the case of a CDR outsourcing arrangement in which a provider collects CDR data on behalf of a principal.

16 At the end of subrule 7.10(1)

Insert:

Note 3: See rule 1.16 for how this rule applies in the case of a CDR outsourcing arrangement in which a provider collects CDR data on behalf of a principal.

17 Paragraph 7.12(2)(b)

After "any outsourced service provider", insert "of the accredited data recipient".

18 Subparagraph 9.3(2)(i)(i)

Omit "sharing CDR data with", substitute "CDR data being collected by or disclosed to".

19 Paragraph 9.8(e)

Repeal the paragraph, substitute:

(e) subrule 1.16(1);

20 Clause 2.2 of Schedule 2 (table item 1, after row relating to "Password authentication", columns headed "Minimum controls" and "Description of minimum controls")

Insert:

Encryption in transit	Implement robust network security controls to help protect data in transit, including: encrypting data in transit and authenticating access to data in accordance with the data standards (if any) and industry best practice, implementing processes to audit data access and use, and implementing processes to verify the identity of communications.

21 Clause 2.2 of Schedule 2 (table item 2, after row relating to "End-user devices", columns headed "Minimum controls" and "Description of minimum controls")

Insert:

Data Segregation	CDR data that is stored or hosted on behalf of an accredited data recipient is segregated from other CDR data to ensure it is accessible only by the accredited data recipient for whom consent was given and remains directly attributable to that accredited data recipient.