Explanatory Statement

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

Prepared by the Australian Competition and Consumer Commission

Contents

Explanatory Statement: *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 2) 2020*

Background

1. This Explanatory Statement accompanies the *Competition and Consumer (Consumer Data Right) Amendment Rules (No.2) 2020* (**Amending Instrument**) which amends the *Competition and Consumer (Consumer Data Right) Rules 2020* (**Rules**).

2. The Rules are a critical component of the Consumer Data Right (**CDR**) regime, an economy-wide reform that gives consumers the ability to safely, efficiently and conveniently access specified data held about them. This data is held by businesses (data holders) and consumers may request that data be disclosed to accredited data recipients.

Purpose

3. The primary purpose of the Amending Instrument is to permit the use of accredited intermediaries to collect CDR data, through an expansion of the rules relating to CDR outsourcing arrangements.

4. When consulting on proposed rules in June (see paragraphs 31-33 below), the draft amendments were described as the 'Combined Accredited Person' rules. Having regard to the feedback received during consultation, the Amended Rules take the approach of making provision for collection of CDR data on behalf of an accredited person in the existing CDR outsourcing rules.

Changes to CDR outsourcing arrangements to include collection arrangements

5. A CDR outsourcing arrangement is an arrangement where a consumer-facing accredited data recipient (**the principal**) engages the services of another party (**the provider**), to enable or assist in the delivery of a good or service to a CDR consumer.

6. Prior to these amendments, the rules permitted CDR outsourcing arrangements to cover disclosure of CDR data by the principal to the provider; and use or disclosure of CDR data by the provider on behalf of the principal.

7. The Amending Instrument expand CDR outsourcing arrangements to include the collection of CDR data on behalf of an accredited data recipient (the principal). Where the CDR outsourcing arrangement encompasses collection, the collecting provider must be accredited at the unrestricted level.

Transparency for consumers

8. The Rules as amended (**Amended Rules**) maintain the requirement for consumers to be given information during the consent process about the use of outsourced service providers (via the principal's Privacy Safeguard 1 Policy, rule 7.2). This includes the name and, if applicable, the accreditation number of the outsourced service providers who may collect data or to whom data may be disclosed. As such, when consent is given to the principal, that consent encompasses the principal's use of outsourced service providers.

9. As the customer-facing entity, the principal is responsible for providing the dashboard and complying with the dashboard requirements for accredited data recipients, which remain unchanged.

10. A provider who is also an accredited data recipient is also required to have its own Privacy Safeguard 1 policy.

Obligations of the parties

11. As accredited persons, both the principal and provider have certain obligations imposed under the rules in relation to CDR data.

12. However, some obligations are modified in the context of CDR outsourcing arrangements. The amendment to rule 1.7(5) clarifies that certain obligations in relation to making consumer data requests, collecting consumer data, obtaining consents, providing consumer dashboards, and using or disclosing CDR data do not apply to the provider, even if the provider is accredited. The purpose of this amendment is to clarify that these are the obligations of the principal in a CDR outsourcing arrangement. In addition, the amendment to rule 1.16(1) imposes an obligation on the principal to ensure that a provider complies with the provider's requirements under an outsourcing arrangement including in relation to collection.

13. As accredited persons, both the principal and provider are subject to the Privacy Safeguards set out in the *Competition and Consumer Act 2010* (Cth) (**Competition and Consumer Act**) sections 56ED-56EO. In particular, as Privacy Safeguard 3 (soliciting CDR data from CDR participants) and Privacy Safeguard 4 (dealing with unsolicited CDR data from CDR participants) apply to accredited persons, they will apply to both the principal and the provider.

14. The Amending Instrument clarifies the operation of certain Privacy Safeguards in the context of CDR outsourcing arrangements where both parties are accredited. Notably, the amendment to rule 1.16(2) clarifies the operation of Privacy Safeguards 5, 10 and 11. The rules relating to Privacy Safeguard 12 (rules 7.11-7.13) remain unchanged, as they already accommodate outsourced service providers. However, as noted in paragraph 16 below, two new minimum information security controls are added to the requirements in Schedule 2.

Liability

15. The Amended Rules retain the position that, where a CDR outsourcing arrangement is in place, use or disclosure of CDR data by the provider, whether or not in accordance with the arrangement, is also taken to be by the principal (rule 7.6).

16. In addition, section 84(2) of the Competition and Consumer Act may also apply such that conduct engaged in by the provider on behalf of the principal may be deemed to be conduct engaged in by the principal.

Changes to minimum information security controls

17. The Amending Instrument inserts two new minimum information security controls relating to encryption in transit and data segregation and which are relevant to CDR outsourcing arrangements generally. The encryption in transit control requires accredited data recipients to implement robust network security controls to protect data in transit, including for CDR data that is disclosed to an outsourced service provider (and then by that provider). The data segregation control requires CDR data that is held by providers on behalf of a principal to be segregated, such as through physical or logical segregation, from data held on behalf of others.

Authority for making the Amending Instrument

18. The Amending Instrument was made under section 56BA of the Competition and Consumer Act which enables the ACCC to make consumer data rules and, relying on subsection 33(3) of the *Acts Interpretation Act 1901* includes the power to amend the rules.

19. The Minister consented to the ACCC making the Amending Instrument in accordance with section 56BR of the Competition and Consumer Act.

20. Before making consumer data rules, section 56BP of the Competition and Consumer Act requires the ACCC to have regard to certain matters outlined in section 56AD. These include the likely effect of the rules on the interests of consumers, the efficiency of relevant markets, the privacy and confidentiality of consumers' information, and the regulatory impact of the rules. The process for making the Amending Instrument involved consideration of the matters outlined in section 56AD, including through public consultation on draft amendments.

Statement of compatibility with human rights

21. This statement is prepared in accordance with Part 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011* (Cth).

22. The Amending Instrument is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the Human Rights (Parliamentary Scrutiny) Act 2011.

Human right implications

23. The Amending Instrument is consistent with the right to protection from unlawful or arbitrary interference with privacy under Article 17 of the International Covenant on Civil and Political Rights (**ICCPR**).

24. Amended Rules 1.10 and 1.16 set out the framework of obligations and responsibilities of accredited persons in CDR outsourcing arrangements. These provisions protect against unlawful or arbitrary interference with privacy.

25. Amended Rules 1.6(11), 1.7(1), 1.7(4), 1.7(5), 1.16, 1.18(c), 4.11(3)(f), 7.2(4)(b), 7.4, 7.5(1)(d), 7.5(1)(e), 7.5(3)(c), 7.6(2) and (3), 7.9, 7.10(1), 7.12(2)(b), 9.3(2)(i)(i) and 9.8(e) are intended to bring the operation of those provisions in line with the broader purpose of the Amending Instrument. As such, the effect of these Amended Rules is to ensure that the overall operation of the rules remains in line with the protections afforded by Article 17.

26. Amendments to clause 2.2 of Schedule 2 add to the existing framework for minimum information security controls and as such provide additional protections in relation to privacy.

Conclusion

27. The Amending Instrument is compatible with human rights and freedoms.

Privacy impact assessment

28. An independently prepared draft of the Privacy Impact Assessment report was released for consultation alongside the draft rules on 22 June 2020. This was prepared as an update to the Privacy Impact Assessment dated March 2019, published by The Treasury.

29. A final Privacy Impact Assessment report will be published on the ACCC's website

Regulatory impact analysis

30. The Amending Instrument falls within the scope of the regulation impact assessment undertaken at the time of making the Rules. The Amended Rules do not depart significantly from the original consideration. On this basis, the Office of Best Practice Regulation advised that a Regulation Impact Statement was not required (OBPR reference ID 24996).

Consultation

31. Draft rules were released for consultation on 22 June 2020, for a period of 28 days. In addition, the ACCC held an online workshop on 14 July 2020 about the design and technical implementation of the draft rules.

32. The ACCC also consulted with the Information Commissioner.

33. This satisfies the consultation requirements specified in section 56BQ of the Competition and Consumer Act.

Explanatory Notes

Clauses 1 to 4

1. Clauses 1, 3 and 4 of the Amending Instrument provide for the name and authority for the making of the instrument and the amendments to be made (as set out in Schedule 1).

2. Clause 2 provide for the Amended Rules to commence the day after the Amending Instrument is registered on the Federal Register of Legislation. The Amended Rules will require technical implementation in the Register of Accredited Persons (the **Register**) that the ACCC maintains in its capacity as the Accreditation Registrar. The ACCC expects that the Amended Rules will be implemented and supported in the Register by early November 2020 and will publish details about this via the ACCC's CDR newsletters.

Schedule 1 - Amendments

Items 1 and 2: Amendments to rules 1.6(11) and 1.7(1) — Add references to service data

3. Items 1 and 2 amend rules 1.6 'Overview of these rules' and 1.7 'Interpretation' to include references to 'service data', consequential to the amendments in item 4.

Item 3: After rule 1.7(4) — Clarify references to accredited persons

4. Item 3 inserts rule 1.7(5), which stipulates that certain references to 'accredited persons' throughout the rules do not apply to accredited persons acting in their capacity as a provider in a CDR outsourcing arrangement. This includes rules relating to making consumer data requests, collecting consumer data, obtaining consents, providing consumer dashboards, and using or disclosing CDR data.

Item 4: Amendment to rule 1.10 — New definitions

5. Item 4 repeals and replaces rule 1.10. This amendment replaces the meaning of 'outsourced service provider' and 'CDR outsourcing arrangement' in subrules 1.10(1) and 1.10(2) respectively. This has the effect of allowing an accredited person to enter into a CDR outsourcing arrangement as an outsourced service provider (a 'provider'), in order to collect CDR data on behalf of another accredited party (a 'principal').

6. The amendment in this item also defines the term 'service data' in subrule 1.10(4), to mean CDR data that is obtained pursuant to a CDR outsourcing arrangement. This includes CDR data collected by a provider on behalf of a principal and CDR data disclosed to a CDR provider by a principal as well as any data that is derived, indirectly or directly, from this collected or disclosed data.

Item 5: Amendment to rule 1.16 — Update and clarify obligations

7. Item 5 repeals and replaces rule 1.16, which specifies the obligations of a principal in a CDR outsourcing arrangement. The amendment preserves, in subrule 1.16(1), the position that the principal is responsible for ensuring that an outsourced service provider complies with its requirements under a CDR outsourcing arrangement.

8. The amendment also specifies in subrule 1.16(2) the intended operation of certain rules relating to the Privacy Safeguards. The intention of this amendment is to clarify that references to accredited persons in those rules are references to the principal.

Items 6, 7, 18: Amendments to rules 1.18(c), 4.11(3)(f) and 9.3(2)(i)(i) — Expand to include acts of collection

9. Items 6, 7 and 18 are amendments to rules 1.18(c), 4.11(3)(f) and 9.3(2)(i)(i), in which are consequential to the amendment in item 4. The scope of those provisions was previously limited to disclosure of CDR data to an outsourced service provider, and has been broadened to cover collection of CDR data by an outsourced service provider.

Items 8, 9, 11, 13 and 17: Amendments to rules 4.11(3)(f), 7.2(4)(b), 7.5(1)(d), 7.5(3)(c), 7.12(2)(b) — Clarify references to outsourced service providers

10. The minor amendments in items 8, 9, 11, 13 and 17 insert text to make clear that references to outsourced service providers in rules 4.11(3)(f), 7.2(4)(b), 7.5(1)(d), 7.5(3)(c) and 7.12(2)(b) are references to outsourced service providers of an accredited person.

11. This is because the definition of 'CDR outsourcing arrangement', as amended in rule 1.10 by item 4, includes arrangements where neither party is accredited.

Items 10, 15 and 16: Amendments to the notes of rules 7.4, 7.9 and 7.10(1) — Insert cross-references to rule 1.16

12. Items 10, 15 and 16 insert notes at the end of rules 7.4, 7.9 and 7.10(1) to cross-reference rule 1.16.

Item 19: Amendments to rule 9.8(e) — Update cross-reference to subrule 1.16(1)

13. Following the amendment in item 5, item 19 updates the cross-reference in this paragraph to refer to subrule 1.16(1).

Items 20 and 21: Amendments to Clause 2.2 of Schedule 2 — Insert new Minimum Information Security Controls

14. Items 20 and 21 insert two new minimum information security controls into Clause 2.2 of Schedule 2. These controls relate to encryption in transit and data segregation. The data in transit control makes provision for a data standard to be made in the future for this purpose but where there is no standard, the default requirement is to protect data in transit in accordance with industry best practice.