Australian Government

Consumer Data Right

# Consumer Data Right Rules

## Update 1 to Privacy Impact Assessment

### Agency response

October 2020

# ACCC response to Privacy Impact Assessment

As required by the Competition and Consumer Act, the Australian Competition and Consumer Commission (ACCC) considers and seeks to balance a range of matters when developing and making the Competition and Consumer (Consumer Data Right)(CDR) Rules (CDR Rules):

- the interests of consumers
- the efficiency of relevant markets
- the privacy or confidentiality of consumers' information
- promoting competition
- promoting data-driven innovation
- any intellectual property in the information to be covered by the instrument
- the public interest.

In making the Competition and Consumer (CDR) Amendment Rules (No. 2) 2020 (the Amending Instrument), the ACCC engaged Maddocks to conduct an independent Privacy Impact Assessment (PIA) of the proposed changes to the CDR Rules.

This PIA was conducted on the basis that it was an update to the PIA report for the CDR Rules dated March 2019, published by the Treasury. A draft of the PIA report was released for consultation alongside the draft Rules on 22 June 2020, for a period of 28 days.

The final PIA report made 10 recommendations in relation to the proposed changes to the CDR Rules. That report is based on the development of the Rules as at 4 September 2020. Subsequent to the report, and prior to finalising the Amending Instrument, the ACCC made changes in response to some of those recommendations. The table below outlines the ACCC's consideration of the recommendations, and the ACCC's response to each.

| | Recommendation | Response |
|---|---|---|
| 1 | We **recommend** that the ACCC clarify:<br>• whether the Provider is liable for its collection of CDR Data from the Data Holder (not the Principal on whose behalf it is making that collection);<br>• which obligations in the CDR Rules apply to the Principal and/or the Provider (noting that both will be accredited persons); and<br>• the intention of the proposed amendments to Rule 7.6(2)(b)(ii), and specify whether it is intended to apply to further CDR Outsourcing Arrangements of the Provider in relation to that CDR Consumer, or additional CDR Outsourcing Arrangements of the Provider for other CDR Consumers. | **Accepted.**<br>The Amending Instrument and accompanying explanatory material clarify the matters identified in this recommendation.<br>• Rule 1.7(5) clarifies 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.<br>• Rule 1.16(2) clarifies the operation of Privacy Safeguards 5, 10 and 11.<br>• Rule 7.5(1)(f) provides that disclosure by a provider to a principal under an outsourcing arrangement is permitted for the purposes of Privacy Safeguard 6.<br>• The explanatory statement to the Amending Instrument further details the liability framework that applies to CDR outsourcing arrangements including that:<br>  ○ Privacy Safeguards 3 and 4 apply to collection by a provider and a principal<br>  ○ s 84(2) of the Competition and Consumer Act may apply in relation to a provider collecting on behalf of a principal<br>  ○ the Rules retain the position that, where a CDR outsourcing arrangement is in place, use or disclosure by the provider of data that is the subject of that arrangement is also taken to be by the principal (rule 7.6). This is intended to encompass any use or disclosure of that data under a further outsourcing arrangement as referred to in rule 1.10(2)(b)(v). |
| 2 | We **recommend** that the CDR Outsourcing Arrangements be expressly required to contain an obligation:<br>• upon the Principal to accurately communicate the CDR Consumer's consent to the Provider; | **Not accepted.**<br>The ACCC considers that the inclusion of express obligations in relation to communications about consent and authorisation would not provide material additional protections for consumers as to how their data may be collected, used or disclosed. |

| | | |
|---|---|---|
| | • upon the Provider to collect CDR Data from the Data Holder in accordance with the consent provided by the CDR Consumer, and communicated by the Principal; and<br>• upon the Principal to notify the Provider if a CDR Consumer withdraws their consent or authorisation, so that the Provider does not inadvertently continue to use or disclose CDR Data without an appropriate consent and authorisation.<br>Further, we **recommend** that the ACCC should consider whether the legislative framework should contain specific technical requirements for any communications that occur between the Principal and the Provider for information that is not CDR Data (such as information about a CDR Consumer's consent, or their contact information). These requirements could be specified in the proposed amendments to the CDR Rules regarding the content of CDR Outsourcing Arrangements. This would further assist to ensure that the information is appropriately protected. | In particular, because both the principal and provider are required to be accredited, they are subject to a range of obligations under the CDR regime.<br>The Rules govern the circumstances under which CDR data may be collected, used or disclosed, as well as when CDR data must be deleted or de-identified, all of which must be in accordance with a consumer's consent. Rule 1.16(1) further imposes an express obligation on the principal to ensure the provider complies with an outsourcing arrangement that in turn can only permit collection, use and disclosure that accord with a current consent.<br>The ACCC notes the recommendation in relation to specifying technical requirements for communications between the principal and provider. The ACCC will continue to consider the issue of when the Minimum Information Security Controls should apply as part of future rule amendments processes, including as part of the current consultation on proposed changes to the CDR Rules (commenced 30 September 2020). |
| **3** | As an alternative to **Recommendation 2** in relation to containing an obligation in the CDR Outsourcing Arrangements for communication of consent, we recommend the ACCC consider whether the CDR Rules could be amended to include an express obligation on the Principal to the CDR Outsourcing Arrangement to notify the Provider of the withdrawal or expiry of a consent. This would strengthen the privacy protections by not simply relying on the Accredited Data Recipients complying with, and enforcing, contractual obligations. | **Noted.**<br>As discussed above, the ACCC considers that the inclusion of express obligations in relation to communications about consent would not provide material additional protections for consumers as to how their data may be collected, used or disclosed. In particular the principal's liability for the conduct of the provider is set out in rule 1.16(1) and rules 7.6 and 7.7, which operate alongside section 84(2) of the Competition and Consumer Act. |
| **4** | We **recommend** that:<br>• the ACCC clarify whether the references to 'the accredited person's CDR Policy' in Rule 4.11(3)(f)(ii) and (iii) are meant to refer to the Principal, the Provider if they are an accredited person, or both;<br>• Rule 4.11(3)(f)(iii) is amended to specify that the CDR Consumer can obtain further information about the specific Provider's *collections*, *uses* and disclosures from the Principal's CDR Policy; and | **Accepted in part.**<br>The Amending Instrument and accompanying explanatory material clarify the matters identified in this recommendation. These changes, as they relate to CDR Policy obligations, are consistent with the approach to outsourced service providers generally, whether they are collecting, using or disclosing CDR data, on behalf of the principal. The CDR Rules, as amended, 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). |

| | | |
|---|---|---|
| | • the CDR Consumer is informed that their CDR Data may be collected by, disclosed to, or *used by*, the specific Provider. | • Rule 1.7(5) clarifies 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.<br>• Amendments to rule 4.11(3) expand the operation of that Rule to include collections, in addition to uses and disclosures.<br>• The explanatory statement to the Amending Instrument describes the obligations of the parties in the context of CDR outsourcing arrangements. |
| **5** | We **recommend** that the ACCC consider whether, through the Principal's Consumer Dashboard, CDR Consumers should be provided with more granular information (e.g. Provider "X" will be used to collect CDR Data from Data Holder "X"). | **Not accepted.**<br>In finalising the Amending Instrument, the ACCC considered whether, and through what mechanism, consumers should be provided with granular information about a provider.<br>The CDR Rules, as amended, 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). Taking into account the build impacts for data holders and the relative benefits of doing so, the ACCC considers that the CDR Rules should not require more granular information about outsourced service providers to be displayed on the principal's consumer dashboard. |
| **6** | If use of the Principal's ICT credentials (i.e., ICT security certificates) by the Provider is to be permitted, we **recommend** that the ACCC consider amending the CDR Rules to require CDR Outsourcing Arrangements to contain strict obligations in relation to the use of the Principal's credentials by the Provider. If it is not intended that the Provider can use the Principal's credentials, we recommend that the CDR Rules expressly prohibit this use. | **Not accepted.**<br>It is intended that the provider will use the credentials of the principal to collect CDR data. In finalising the Amending Instrument, the ACCC considered whether the CDR Rules should contain obligations in relation to that use.<br>The ACCC considers that additional obligations in the CDR Rules would not provide material additional protections, as these matters will be addressed through the technical requirements that will apply in the Accreditation Register to support the use of the collection arrangements and associated obligations in relation to the use of PKI certificates issued to principals. The ACCC has released technical guidance relating to these issues on 14 October 2020. |

| | | |
|---|---|---|
| **7** | We **recommend** that the ACCC consider whether Data Holders should know whether the Accredited Data Recipient is acting in the role of a Provider or a Principal.<br>The Data Holder could then be required to:<br>• check the accreditation for both the Provider and the Principal, including whether each accreditation has been surrendered, suspended or revoked; and<br>• notify the Principal and the Provider if the CDR Consumer's authorisation is withdrawn or expires. | **Accepted in part.**<br>In finalising the Amending Instrument, the ACCC considered whether the CDR Rules should specify what information will be shown to data holders about the roles of a Provider and a principal.<br>The ACCC considers that the outsourcing arrangement rules clarify that the provider, as an outsourced service provider, acts on behalf of the principal. The ACCC has released technical guidance on this matter which is consistent with the outsourcing rules. That documentation clarifies that the data holder will check the status of the principal's software product, which will be coupled to the accreditation status of both the principal and the provider. |
| **8** | We **recommend** that the ACCC consider whether it would be appropriate for the CDR Rules to contain requirements for the Provider, before disclosing any CDR Data, to check:<br>• the accreditation of the Principal; and<br>• that the technical details it is going to use for the disclosure of the CDR Data match up with the Principal on whose behalf it collected the CDR Data from the Data Holder, or the Principal who disclosed the CDR Data to it. | **Accepted in part.**<br>In finalising the Amending Instrument, the ACCC considered whether the CDR Rules should contain the requirements for the provider to perform certain checks before disclosing CDR data.<br>These matters will be facilitated through the technical requirements that will apply in the Accreditation Register to support the use of the collection arrangements. The provider will be able, but not required, to check the status of the principal via the Register. |
| **9** | We **recommend** that the ACCC consider whether the CDR Rules should clearly provide further protections for CDR Consumers, which could include:<br>• requiring, if either the Principal's, or the Provider's, accreditation is suspended, revoked or surrendered (previously-accredited data recipient):<br>  • the previously-accredited data recipient must notify the other Accredited Data Recipient (i.e. the Principal or the Provider, as relevant) of the fact that it is no longer accredited; and<br>  • the CDR Consumer must be notified of that fact by either:<br>  • the previously-accredited data recipient; or<br>  • the other Accredited Data Recipient,<br>as agreed in the CDR Outsourcing Arrangement; and | **Not accepted.**<br>In finalising the Amending Instrument, the ACCC considered whether and what further protections for consumers should be included in the CDR Rules, in the event that either the principal or provider's accreditation is revoked.<br>The ACCC considers that the CDR Rules, as amended, adequately address and mitigate the identified risk, noting in particular that the CDR Rules require:<br>• accredited persons to take certain steps in the event that its accreditation is surrendered, suspended or revoked — including giving a direction to its outsourced service providers (rules 5.23, 7.12).<br>• the Data Recipient Accreditor to notify the Accreditation Registrar about information relating to accreditation status of accredited data recipients, including of any surrender, suspension or |

| | | |
|---|---|---|
| | • broadening the obligations in the CDR Rules so that, if a party to a CDR Outsourcing Arrangement is notified regarding the other party (i.e. the previously-accredited data recipient is no longer accredited), they must not continue to collect or use CDR Data and clarifying the requirements to treat that CDR Data as redundant data.<br>If the ACCC intends to implement systems (e.g. through the ACCC CDR ICT system), which will ensure anyone using the Principal's credentials (including a Provider) is notified of a suspension, revocation or surrender of the Principal's accreditation, this functionality should be clearly communicated to CDR Consumers. | revocation (rule 5.15), and the Accreditation Registrar to update the Accreditation Register to reflect these details (rule 5.24).<br>This matter is also addressed in the technical guidance relating to the Register. |
| **10** | We **recommend** that the ACCC consider whether it should explicitly clarify that, if the Principal uses a Provider to collect CDR Data from a Data Holder on its behalf, the Principal only collects the CDR Data when the Provider discloses that CDR Data to the Principal (rather than when the Provider collects that CDR Data from the Data Holder).<br>We also **recommend** that the ACCC consider:<br>• providing additional guidance for CDR participants about the distinction between CDR Data and service data, and how the CDR Rules apply to each category; and<br>• ensuring there are no overlaps or gaps that occur in the application of the CDR Rules to CDR Data and service data. | **Accepted in part.**<br>In finalising the Amending Instrument, the ACCC considered that the recommended clarification about when the principal is considered to have collected CDR data, was not necessary, given that the term 'collect' is defined in the governing legislation (the Competition and Consumer Act) .<br>The explanatory statement to the Amending Instrument provides additional guidance on the distinction between CDR data and service data. In finalising the rule amendments, the ACCC has sought to address any gaps or overlaps in the application of the CDR Rules to CDR data and service data. |