HERBERT SMITH FREEHILLS

CONSUMER DATA RIGHT: INCREASED ROLE FOR INTERMEDIARIES

28 October 2020 | Insight
Legal Briefings – By **Julian Lincoln, David J. Ryan and Siobhan Lane**

The *Competition and Consumer (Consumer Data Right) Rules 2020* (**the Rules**) were recently amended to allow accredited third party service providers to provide additional services within the Consumer Data Right (**CDR**) ecosystem.[1] Subject to consumer consent, the amendments permit accredited intermediaries to collect CDR data from data holders (in addition to using or disclosing CDR data) on behalf of accredited data recipients (**ADRs**).

WHAT ARE THE CHANGES?

ACCREDITED INTERMEDIARIES

The role of intermediaries in facilitating the implementation of the CDR regime has been an ongoing area of focus, including in public consultations undertaken by the Australian Competition and Consumer Commission (**ACCC**) earlier this year. This reflects the "*important role of intermediaries in facilitating the efficient and secure collection of data*."[2]

Before the recent amendments were implemented, the Rules already provided for CDR outsourcing arrangements which allow an ADR to disclose CDR data to an outsourced service provider (**OSP**), who can then use or disclose that CDR data on the ADR's behalf. Such data sharing benefits ADRs by enabling OSP-provided capability and capacity such as data infrastructure and tools to derive novel insights.

Under the amended Rules, the scope of CDR outsourcing arrangements has been expanded to allow an intermediary accredited to the 'unrestricted' level (the **Provider**) to not only use and disclose, but also *collect* CDR data on behalf of an ADR (the **Principal**), with the consent of a CDR consumer. This type of outsourcing structure is called a Combined Accredited Person (**CAP**) arrangement.

The amendments seek to:

- further encourage the use of outsourced IT infrastructure and software, rather than requiring ADRs to build their own;
- increase fintech participation in the CDR ecosystem; and
- make it easier for businesses more generally to engage in the CDR regime by reducing the time and costs associated with developing internal capabilities.

JOINT RESPONSIBILITY

As both Principals and Providers are accredited persons, they must comply with all of the obligations for accredited persons under the Rules. However, for certain obligations in relation to CDR data, the two parties to a CAP arrangement can determine who is best placed to fulfil the relevant obligation on behalf of both entities. For example, either the Principal or Provider can provide the CDR consumer with a CDR receipt to satisfy this requirement under the Rules for both entities. This said, each party must still fulfil certain ongoing accreditation requirements (e.g. regarding insurance and information security) on their own accord.

DATA PROTECTION

The amended Rules also apply strengthened measures to promote data security and transparency. In the process of giving consent to a Principal, CDR consumers must be provided with the relevant Provider's name and accreditation number. Accordingly, although a Principal will remain the consumer-facing entity, the Provider's role will always be known to the CDR consumer, promoting transparency within the CDR ecosystem.

The amendments also impose two new minimum information security controls for CDR outsourcing arrangements:

- **Encryption of data in transit:** data in transit, including from a Principal to the Provider, must be protected by robust security controls. Such controls may include encryption or audits for, and authentication of, data access and use.
- **Data segregation:** CDR data held by a Provider on behalf of a particular Principal must be effectively segregated from data held for other Principals.

These additional protections are intended to ensure that CDR data remains protected at all points in the CDR ecosystem.

LIABILITY

While both Principals and Providers are subject to normal CDR privacy safeguards and general accreditation requirements, the amendments also make clear that ultimate responsibility for fulfilling key CDR obligations rests with Principals. Accordingly, Principals are liable for any acts and omissions of Providers (as is the case when ADRs outsource services to OSPs), even if Providers act beyond the scope of their engagement. Including contractual controls may help to reduce this risk, but it does not completely mitigate regulatory or reputational risk for Principals. Accordingly before entering into CDR outsourcing arrangements with Providers, Principals should consider:

- whether the relevant Provider has appropriate controls (both at present and in future) in place to govern the handling of CDR data;
- how to define and control the relevant Provider's role and the terms on which they can operate; and
- if frameworks can be implemented (e.g. security questionnaires and third party information security audits) and information security governance policies and controls aligned.

LOOKING FORWARD

The amendments to the Rules (which entered into force on 2 October 2020) are an important step towards facilitating greater participation of intermediaries in the CDR ecosystem, while still maintaining high standards for accreditation and security. Allowing entities to participate in the CDR ecosystem at lower accreditation levels is likely the next critical step to further opening up the CDR ecosystem and promoting more innovative service offerings that will benefit CDR consumers.

The ACCC are currently consulting on an expansion of the Rules, including to address this next step, and is hoping to further amend the Rules to address this issue in December this year. Accordingly it is more important than ever for interested entities to proactively consider what functions they want to play in the CDR ecosystem and what actions they may need to take to achieve that role.

For more information on the CDR, visit our dedicated hub.

ENDNOTES

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

2. ACCC *CDR Consultation Paper – Participation of Third Party Service Providers* (23 December 2019).

Please click here to return to our CDR showcase page

RELATED TOPICS

Data and privacy

FEATURED INSIGHTS

FEATURED INSIGHTS

HELPING YOU STAY AHEAD OF THE BIG ISSUES

BROWSE BY:

- TECH, DIGITAL & DATA

- GEOPOLITICS AND BUSINESS

- NEW BUSINESS LANDSCAPE

RELATED ARTICLES

UPDATED: UK NATIONAL SECURITY ACT 2021 - WHAT INVESTORS NEED TO KNOW

Foreign investment: Rising tides of politics in regulation

Comply or Explain to climate-related reporting – A cross-industry roadmap

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

JULIAN LINCOLN
PARTNER, HEAD OF TMT & DIGITAL AUSTRALIA, MELBOURNE
+61 3 9288 1694
Julian.Lincoln@hsf.com

PETER JONES
PARTNER, SYDNEY
+61 2 9225 5588
peter.jones@hsf.com

KAMAN TSOI
SPECIAL COUNSEL, MELBOURNE
+61 3 9288 1336
kaman.tsoi@hsf.com

DAVID J RYAN
SENIOR ASSOCIATE, MELBOURNE
+61 3 9288 1831
david.j.ryan@hsf.com