Brace Yourselves: Data Portability Rights Are Coming to Australia

Sophie Dawson & Ashna Taneja BIRD & BIRD

On 15 August 2018, the Australian Government released draft legislation to introduce a data portability right in Australia, to be known as the 'Consumer Data Right' (**CDR**). The new right will give consumers the power to gain access to and direct their information to accredited businesses in a particular economic sector. Transferors of information must supply the data in a format that complies with standards to be set by the forthcoming Data Standards Body.

The scope of the CDR is wider than the 'data portability' right recently introduced by the EU's General Data Protection Regulation (**GDPR**). It is also broader than the Privacy Act in key respects, because it extends beyond information *about* a reasonably identifiable individual. The new right will apply to both individual and business consumers, with no monetary limit on the size of business consumers.

The Australian Government has already confirmed that the CDR will be introduced in the banking, telecommunications and energy sectors. The Australian Competition and Consumer Commission (**ACCC**) will be responsible for advising the Minister on any further sectors to designate.

Businesses should start thinking how this new right may affect them. In particular, one should consider what benefits may accrue from becoming an 'accredited business' that can receive CDR data, and what risks and compliance issues might arise from doing so.

Why have a CDR?

The purpose of the CDR is to give consumers better control over their data and to enhance competition. The CDR is a response to the Australian Productivity Commission's recommendations in its *'Data Availability and Use'* report released on 8 May 2017 (**Report**).

Key benefits identified in the draft legislation (the *Treasury Laws Amendment (Consumer Data Right) Bill 2018* (Cth)) and the Report include:

- Benefiting consumers by enabling them to provide data to suppliers who can then tailor products and services to meet their needs;
- Reducing the costs to consumers of switching between providers of products and services;
- Lowering barriers to entry for new entrants to markets where incumbents have data that gives them market power, and thereby expanding consumer choice;
- Promoting linked services and interoperability of technology and providing a knowledge basis for innovation;
- Making markets more efficient by addressing information imbalances.

What kinds of data will be affected by the CDR?

There are 3 broad categories of data that will be the subject of the CDR:

- Data that relates to a consumer or has been provided by a consumer;
- Data that relates to a product; and
- Data that is derived from these sources.

Data that 'relates' to a consumer is broader than the definition of 'personal information' in the *Privacy Act 1988* (Cth) in at least two ways. First, it extends to businesses as well as individuals. Second, it extends beyond information 'about' an individual. In the *Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4*, the Federal Court found that 'personal information' in the Privacy Act is confined to information 'about' an individual. In that proceeding, a distinction was drawn between information 'about' an individual and, for example, information 'about' their car where it has been provided for repair. The CDR will apply to information about the car and its repair, and not just to information about the person who or that owns the car.

The most recent draft legislation recognises the broad nature of information that 'relates' to a consumer, and imposes limitations on the access and transfer rights for CDR data so that they will only apply to types of information that are specified in a designation instrument. This also has the effect of limiting the types of derived data captured by the CDR.

The CDR will also apply to data that is collected or generated outside of Australia if it has been commissioned by an Australian registered corporation, citizen or a permanent resident. In the context of banking, the right will therefore capture data generated through overseas transactions using Australian issued bank cards.

What will the CDR look like?

The draft CDR legislation is designed around 3 key players: data holders, CDR consumers, and accredited data recipients. Each of these players will be subject to a set of forthcoming Consumer Data Rules (**Rules**), which will operate as a binding contract between them. The Rules will be

drafted and enforced by the ACCC, and will likely cover:

- Disclosure, use, accuracy, storage, security and deletion of CDR data;
- Accreditation of data recipients;
- Reporting and record keeping; and
- Any other matters incidental to the CDR system.

Only accredited entities and individuals are able to receive CDR data. This process ensures that data recipients have met various security and privacy safeguards before receiving CDR data. The forthcoming Data Recipient Accreditor will be responsible for managing this accreditation process.

The Rules will include sectoral variances to account for the different attributes and needs of different economic sectors. The draft legislation also contemplates the classification of CDR data into different categories, with the view to imposing more rigorous data security standards on some categories than on others. The categories may also be used to establish fees in relation to the disclosure of certain categories of data to acknowledge the value-added nature of some data. This acknowledges the impact that free data may have on the incentives for businesses to collect value-added data.

Who will be responsible for regulating the CDR?

The ACCC and the Office of the Australian Information Commissioner (**OAIC**) will be jointly responsible for implementing and enforcing the CDR. The ACCC will have its existing enforcement tools at its disposal to enforce various CDR rights and obligations, including the enforcement of civil penalty provisions. Furthermore, the forthcoming Data Standards Body will be initially housed within CSIRO's Data61, and will be responsible for setting technical standards for the format, security and transmission of data.

How does the CDR interact with the Australian Privacy Principles (APPs)?

CDR data will be subject to its own set of privacy protections, to be known as the 'CDR Privacy Safeguards'. Generally, the APPs will continue to apply to data holders, who will be subject to additional requirements once a request for CDR data is made by a consumer. Accredited data recipients will be subject to the CDR Privacy Safeguards in substitution for the APPs. Each safeguard mirrors (but provides a higher standard than) each APP:

- ***Privacy Safeguard 1 (Open and transparent management of CDR data)*** –participants for CDR data must take steps to ensure compliance with the Consumer Data Rules, and must keep in place an up-to-date policy available free of charge on the management of CDR data;
- ***Privacy Safeguard 2 (Anonymity and pseudonymity)*** – any consumer that requests their CDR data must be given the option of using a pseudonym, or to not identify themselves when dealing with a holder of data;
- ***Privacy Safeguard 3 (Collecting solicited CDR data)*** – a person must not collect CDR data unless doing so is in response to a valid request for CDR data under the Consumer Data Rules, or is otherwise authorised by laws other than the APPs;
- ***Privacy Safeguard 4 (Dealing with unsolicited CDR data)*** – a person that received unsolicited CDR data must destroy it as soon as practicable;
- ***Privacy Safeguard 5 (Notifying the collection of CDR data)*** – any collection of CDR data must be made known to consumers;
- ***Privacy Safeguard 6 (Use or disclosure of CDR data)*** – data holders and accredited data recipients cannot use or disclose CDR data unless it is in accordance with the Consumer Data Rules, or authorised by laws other than the APPs;
- ***Privacy Safeguard 7 (Use or disclosure of CDR data for direct marketing by accredited data recipients)*** – collectors of CDR data must not use or disclose this data without the consent of the consumer unless it is in accordance with the Consumer Data Rules, or is otherwise authorised by laws other than the APPs;
- ***Privacy Safeguard 8 (Cross-border disclosure of CDR data)*** – cross-border disclosure must not be made unless the person receiving the CDR data is an accredited recipient, or meets certain requirements specified by the Consumer Data Rules;
- ***Privacy Safeguard 9 (Adoption or disclosure of government related identifiers)*** – a data holder or accredited data recipient must not adopt or disclose a government related identifier for a consumer unless doing so is required by laws other than the Consumer Data Rules or the APPs;
- ***Privacy Safeguard 10 (Quality of CDR data)*** – holders of CDR data must ensure that it is accurate, up to date, and complete when it is disclosed;
- ***Privacy Safeguard 11 (Security of CDR data)*** – holders of CDR data must take steps in accordance with the Consumer Data Rules to protect CDR data from misuse, interference, loss, and unauthorised access, modification or disclosure. It must also destroy any CDR data that becomes redundant; and
- ***Privacy Safeguard 12 (Correction of CDR data)*** – a data holder must correct CDR data if requested to do so by a consumer.

Each Privacy Safeguard (except for Privacy Safeguard 2) is a civil penalty provision.

Which sectors will be affected by the CDR?

The CDR will first be rolled out in the banking sector, with the energy and telecommunications sectors to follow. The ACCC's newly established Access to Data Unit is tasked with making recommendations to the Minister on any further sectors to implement the CDR.

The ACCC's timeline for implementation in the banking sector is as follows:

- **1 July 2019:** all major banks to have data available on credit and debit cards, transaction and deposit accounts;
- **1 February 2020:** all major banks to have data available on mortgages;
- **1 July 2020:** all major banks to have data available on all remaining products;
- **1 February 2021:** all Authorised Deposit-Taking Institutions (ADIs) to have data available for mortgages;
- **1 July 2021:** all ADIs to have data available for all remaining products.

These timeframes are subject to extension by the ACCC. All other banks are to be given an additional 12 months for each implementation stage. The timeframes for the energy and telecommunications sectors have yet to be announced.

Challenges in implementing the CDR

One of objectives of the CDR is to reduce the cost to consumers of comparing and switching between providers of products and services. This is to be achieved through the implementation of data standards, which seek to promote data interoperability.

However, the current design of the CDR does not place any obligations on businesses to either:

a) become accredited data recipients; or

b) use the data that is transferred to them by a consumer.

This raises questions as to the likely extent to which businesses will elect to become accredited so as to receive data. The usefulness of the CDR to consumers could be limited if take up is low. The ACCC's Rules Framework notes that since the CDR is consumer focused, it has not introduced any reciprocity requirements for data holders and accredited data recipients in its first version of the Rules.

It is worth noting that a consideration for some businesses in relation to whether to seek accreditation is that interoperability rules for data could affect data security risks through the standardisation of information storage and format. The current proposal for the banking sector includes a requirement for all data to be shared via a dedicated Application Programming Interface (**API**) that meets standards developed by the Data Standards Body.

Another challenge facing the CDR is its scope. The current draft legislation not only defines consumer to include businesses of any size, but captures all information that relates to an identifiable or reasonably identifiable individual arising out of a supply of goods or services to them or their associates. This could extend the CDR to individuals that do not necessarily have a direct customer relationship with the data holder. An example of this may be when a business enters into a contract with a telecommunications company for the provision of mobile phones for its employees. Any data relating to those employees held by the telecommunications company may also be subject to the CDR and potentially subject to requests for data by those employees. This has significant cost implications for businesses operating in the designated sectors in managing CDR requests.