GILBERT
+TOBIN

OPEN BANKING – WHAT YOU NEED TO KNOW

NOVEMBER 2019

GTLAW.COM.AU

INTRODUCTION

The Consumer Data Right (**CDR**) provides consumers (both individuals and businesses) with a right to access specified data that businesses hold about them. Consumers will be able to consent to this information being provided to certain accredited third parties.

Australia has taken significant steps towards establishing a CDR regime and implementing it in the banking sector (**Open Banking**) in the second half of this year, with the Government having stated that it is committed to extending the CDR regime to the energy and telecommunications sectors before it is rolled out economy wide.

The purpose of this publication is to provide an overview of the legal and regulatory framework, key aspects of the timing for implementing Open Banking and the high-level obligations imposed on relevant CDR participants.

LEGAL AND REGULATORY FRAMEWORK

LEGISLATION ESTABLISHING THE CDR FRAMEWORK

In August 2019, *Treasury Laws Amendment (Consumer Data Right) Act 2019* (Cth) (**CDR Act**) came into effect establishing the overarching framework of the CDR regime. The CDR Act inserted Part IVD into the *Competition and Consumer Act 2010* (Cth) (**CCA**) and made amendments to the *Privacy Act 1988* (Cth) and the *Australian Information Commissioner Act 2010* (Cth) (**AIC Act**).

The ACCC is the lead regulator of the CDR regime and will be supported by the Office of the Australian Information Commissioner (**OAIC**) and CSIRO as the Data Standards Body. The Australian Financial Complaints Authority (**AFCA**) was designated as the external dispute resolution scheme for Open Banking on 3 October 2019.

BANKING DESIGNATION INSTRUMENT

The CDR applies to economic sectors designated by the Minister (section 56AC(2) of the CCA).

On 7 September 2019, the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019 designated the banking industry as the first sector subject to the CDR regime.

CDR RULES

The ACCC has the power to make CDR rules for designated sectors (section 56BA of the CCA).

On 2 September 2019, the ACCC published a locked-down version of the Competition and Consumer (Consumer Data Right) Rules 2019 (**CDR Rules**) which established rules that will apply to Open Banking and the CDR regime more generally, pending Treasury consent.

It is intended that the CDR Rules will "progressively apply to a broader range of data holders and products" over time.

TECHNICAL DATA STANDARDS

The Data Standards Chair has the power to make data standards for designated sectors (section 56FA of the CCA). They are assisted by the Data Standards Body, CSIRO's Data61, which is responsible for designing the common technical standards that will apply to Open Banking.

On 30 September 2019, the Data Standards Body released the Consumer Data Standards v1.1.0 (**Data Standards**) which is expected to become the initial binding technical standard for data sharing in Open Banking.

DATA CAPTURED BY OPEN BANKING

CDR DATA CAPTURED BY OPEN BANKING

There are four classes of data and information captured by the Open Banking regime. These fall within 2 broad categories of Consumer Data (data that relates to a CDR consumer) and Product Data (that doesn't relate to a CDR consumer).

CONSUMER DATA (RELATES TO A CDR CONSUMER)

CUSTOMER DATA: Information that identifies or is **about the consumer**.

For individuals: includes the person's name, contact details and other information provided when acquiring the product or relating to their eligibility, but not an individual's date of birth.

For businesses: it also includes a name, ABN, ACN, date of registration etc.

ACCOUNT DATA: Information that identifies or is **about the operation of the account**.

Includes the account number, account name, opening, current and closing balance, available funds and authorisations (i.e. direct debits, scheduled payments and payee details).

TRANSACTION DATA: Information that identifies or describes **the transaction**.

Includes the date of the transaction, identifier for the counter-party, information provided by the merchant, amount debited/credited, description of the transaction and the "simple categorisation" (e.g. whether the transaction is a fee or interest).

PRODUCT SPECIFIC DATA: Information that identifies or describes **the product**.

Includes the product type, name, price (including fees, charges and interest rates), features and benefits (including discounts and bundles), terms and conditions and customer eligibility.

Product prices or features that are negotiated individually with a CDR consumer are Consumer Data.

PRODUCT DATA (DOESN'T RELATE TO A CDR CONSUMER)

PRODUCT SPECIFIC DATA: Information that identifies or describes **the product**.

Includes the product type, name, price (including fees, charges and interest rates), features and benefits (including discounts and bundles), terms and conditions and customer eligibility.

Product prices or features that are not negotiated individually with a CDR consumer are Product Data.

VOLUNTARY VS REQUIRED DATA

Open Banking also distinguishes between voluntary and required data. Data Holders cannot charge a fee for disclosing required data but can charge a fee for disclosing voluntary data.

Required Consumer Data

Consists of the following data where it **relates to a CDR consumer** and is held in **digital form**:

+ **Customer Data**;
+ **Account Data** for single or joint accounts of at least one CDR consumer - whether open, closed, online or offline (together, **Relevant Accounts**), with some exceptions relating to old direct debits.
+ **Transaction Data** for transactions on Relevant Accounts, with some exceptions for old transactions.
+ **Product Specific Data** for products the CDR consumer uses.

Voluntary Consumer Data

Data that falls outside the scope of Required Consumer Data but still relates to a CDR consumer.

Required Product Data

Consists of the following data where it **does not relate to any CDR consumer** and is **held in digital form**:

+ Eligibility criteria, terms and conditions, price of a product;
+ Availability or performance of a product where publicly available; and
+ Product Specific Data.

Voluntary Product Data

Data that falls outside the scope of Required Product Data but is still Product Specific Data and doesn't relate to a CDR consumer.

DATA NOT CAPTURED BY OPEN BANKING

Materially Enhanced Information only in relation to the use of a product by a customer

"Materially enhanced information" is information derived from source data that was wholly or partly derived through the application of insight or analysis by the Data Holder to make the information significantly more valuable than the source material in terms of usefulness, usability or commercial value. For example, the outcome of an income expense or asset verification assessment or categorisation of transactions. For other examples, see our Insight "Open Banking - where are we up to?".

Certain Credit Information

Includes court proceedings, personal insolvency and serious credit infringement information.

Data that is not CDR data - accounts of minors and accounts with multiple authorisations

Account Data, Transaction Data and Product Specific Data in relation to persons under 18 years of age (or for joint accounts where one account holder is under 18). Account Data, Transaction Data and Product Specific Data in relation to individual accounts where more than 1 person is authorised to make transactions (or joint accounts where more than 2 people are authorised to make transactions).

SHARING DATA IN OPEN BANKING

KEY PARTIES IN OPEN BANKING

The key participants in Open Banking are shown in the table below.

CDR CONSUMER

Only **Eligible** CDR consumers can receive Consumer Data or authorise an ADR to request Consumer Data on their behalf. To be an Eligible CDR consumer, the consumer must be over 18 (if an individual) and have an open account that can be accessed online.

DATA HOLDER

In Open Banking, a Data Holder is an entity that holds original data about a CDR consumer. The obligation to share CDR data will first apply to Initial Data Holders (the four major banks in relation to products branded with their main brands).

Later, the obligation to share data will apply to Subsequent Data Holders.

ACCREDITED DATA RECIPIENT (ADR)

An **ADR** is an Accredited Person with whom the Data Holder shares CDR data.

To become an **Accredited Person**, a person applies to the Data Recipient Accreditor. There is currently only one level of accreditation – the 'unrestricted' level – and no fee is required.

SHARING PRODUCT AND CONSUMER DATA

HOW PRODUCT DATA IS SHARED IN OPEN BANKING

STEP 1: PRODUCT DATA REQUEST

A person may request Product Data from a Data Holder that relates to product(s) offered by the Data Holder using the Data Holder's Product Data Request Service.

STEP 2: DATA SHARING

The Data Holder: (a) must disclose the requested Required Product Data and (b) may disclose the requested Voluntary Product Data to the person using the Data Holder's Product Data Request Service.

HOW CONSUMER DATA IS SHARED IN OPEN BANKING

Consumer Data requests can only be made by CDR consumers. They can request the data directly from a Data Holder; or have an ADR make the request on their behalf.

How does a CDR consumer request Consumer Data directly?

STEP 01	**CONSUMER DATA REQUEST** A CDR consumer requests Consumer Data from the Data Holder using the Data Holder's Direct Request Service.
STEP 02	**DATA HOLDER DETERMINES VALIDITY OF REQUEST** The Data Holder reviews the request to determine if it is valid (the CDR consumer must be Eligible at the time of the request) and whether it is a request for: (a) Voluntary Consumer Data; or (b) Required Consumer Data.
STEP 03	**DATA HOLDER DETERMINES IF AN EXCEPTION APPLIES AND IF SO, NOTIFIES CDR CONSUMER** The Data Holder may refuse to disclose Required Consumer Data if: (a) it considers this necessary to prevent physical or financial harm or abuse; or (b) an exception in the Data Standards applies. The Data Holder must inform the CDR consumer of a refusal.
STEP 04	**DATA SHARING** The Data Holder: (a) must disclose the requested Required Consumer Data and (b) may disclose the requested Voluntary Consumer Data to the CDR Consumer using the Data Holder's Direct Request Service.

How does an ADR request Consumer Data on behalf of a CDR consumer?

STEP 01	**REQUEST AND CONSENT** A CDR consumer gives consent to an ADR to obtain their Consumer Data. For example, where an ADR provides the CDR consumer with goods or services which requires the use of the CDR consumer's data and the CDR consumer consents to the collection and use.
STEP 02	**CONSUMER DATA REQUEST** ADR requests Consumer Data from the Data Holder (on behalf of the CDR consumer) using the Data Holder's Accredited Person Request Service.
STEP 03	**AUTHORISATION** Data Holder checks if there is authorisation. If no existing authorisation, and the Data Holder reasonably believes the Consumer Data request was made by an ADR on behalf of a CDR consumer that is Eligible, it must ask the CDR consumer to authorise disclosure.
STEP 04	**DATA SHARING** The Data Holder: (a) must disclose the requested Required Consumer Data and (b) may disclose the requested Voluntary Consumer Data to the CDR consumer using the Data Holder's Accredited Person Request Service.

IMPLEMENTATION DEADLINES FOR KEY DATA HOLDERS IN OPEN BANKING

A staggered approach has been taken for Data Holders to implement Open Banking.

Initially, Open Banking will only apply to **Initial Data Holders**, and ADIs that elect to voluntarily participate early, in relation to Phase 1 products first (defined below), before applying in relation to more complex Phase 2 and Phase 3 products.

The obligation to share CDR data will then extend to **Subsequent Data Holders**:

+ ADIs that have accreditation and are not foreign ADIs or foreign branches of domestic banks (**Accredited ADIs**) and accredited persons that are not an ADI (**Accredited non ADI**) such as Fintechs;
+ the other brands of Initial Data Holders (including for the four major banks' related brands, for example, St George, Bank of Melbourne, BankSA and RAMS for Westpac, BankWest for CBA and UBank for NAB); and
+ any other ADI that is not one of the other Data Holders listed above and is not a foreign bank, foreign branch of a domestic bank or a restricted ADI (**Any other relevant ADIs**).

The relevant timeframes are set out in the diagrams on page 9 which show when Data Holders are required to share particular types of CDR data. There are other circumstances in which requests can be made to Data Holders but they are not required to disclose CDR data.

LEGEND

PDR	Product Data request
CDR-AP	Consumer Data requests made by Accredited Persons
CDR-C	Consumer Data requests made by Eligible CDR consumers
P1 Product*	Limited to certain Phase 1 Products that are held in the name of an individual CDR consumer and relate to open accounts

Initial Data Holders (CBA, ANZ, NAB & Westpac) – Implementation Deadlines

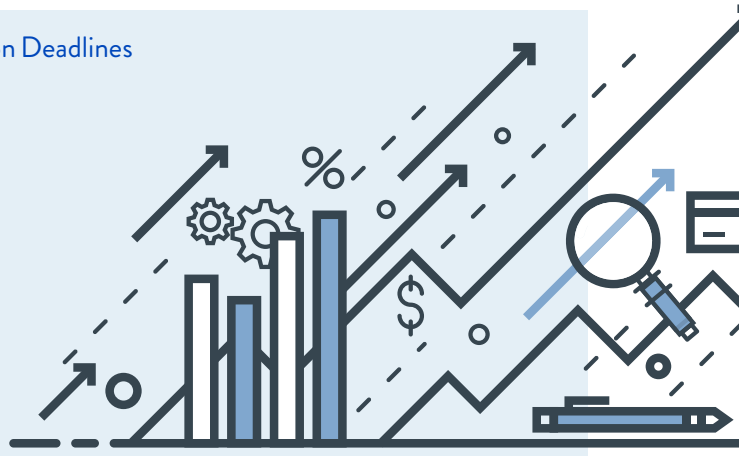
DATA DISCLOSURE COMMENCEMENT DATE – 31 JAN 2020	1 FEB 2020 – 30 JUN 2020	1 JUL 2020 – 31 JAN 2021	1 FEB 2021 ONWARDS
P1 Product	P1 Product	P1 Product	P1 Product
	P2 Product	P2 Product	P2 Product
		P3 Product	P3 Product
	P1 Product	P1 Product	P1 Product
		P2 Product	P2 Product
			P3 Product
		P1 Product	P1 Product
		P2 Product	P2 Product
			P3 Product

Related brands of Initial Data Holders and any other relevant ADIs - Implementation Deadlines

1 JUL 2020 – 31 JAN 2021	1 FEB 2021 – 30 JUN 2021	1 JUL 2021 – 31 JAN 2022	1 FEB 2022 ONWARDS
P1 Product	P1 Product	P1 Product	P1 Product
	P2 Product	P2 Product	P2 Product
		P3 Product	P3 Product
	P1 Product*	P1 Product	P1 Product
		P2 Product	P2 Product
			P3 Product
		P1 Product	P1 Product
		P2 Product	P2 Product
			P3 Product

Accredited ADIs and accredited non-ADIs - Implementation Deadlines

1 JUL 2020 – 31 JAN 2021	1 FEB 2021 ONWARDS
P1 Product	P1 Product
P2 Product	P2 Product
P3 Product	P3 Product
P1 Product	P1 Product
P2 Product	P2 Product
	P3 Product
	P1 Product
	P2 Product
	P3 Product



Update: On 20 December 2019, the ACCC announced that the launch of Open Banking would be delayed to 1 July 2020. We are awaiting a new version of the CDR Rules that reflects this.

DATA HOLDER OBLIGATIONS THAT ATTRACT CIVIL PENALTIES

The CDR Rules have introduced civil penalties where Data Holders or Accredited Persons fail to comply with certain obligations in Open Banking.

LEGEND

- $ Maximum civil penalty for non-compliance (per contravention)
  - For **corporations** is the greater of: $10 million, 3x the benefit received or 10% of the company's annual turnover
  - For **individuals** is $ 500,000.
- $ Maximum civil penalty for non-compliance (per contravention)
  - For **corporations** is $250,000
  - For **individuals** is $50,000

PRODUCT DATA REQUESTS

Data Holders must disclose Product Data in accordance with the implementation deadlines set out on page 9.

Managing Product Data requests

Data Holders must provide an online **Product Data Request Service** that complies with Data Standards which: $

- can be used by any person to make Product Data requests; $
- is used by the Data Holder to disclose Product Data in machine-readable form. $

Sharing Product Data

Following a Product Data request, a Data Holder must use its **Product Data Request Service** to disclose: $

- all **Required Product Data** requested, in compliance with Data Standards: $
  - including that contained on the Data Holder's website or product disclosure statement; $
  - without charging a fee , imposing conditions, restrictions or limitations on use; $
  - unless an exception applies and the Data Holder has informed the person who made the request. $
- any **Voluntary Product Data** it chooses to disclose.

CONSUMER DATA REQUESTS FROM ELIGIBLE CDR CONSUMERS

Data Holders must make certain Consumer Data available on request by eligible CDR consumers in accordance with the implementation deadlines set out on page 9.

Managing Consumer Data requests from CDR consumers

Data Holders must provide an online **Direct Request Service** that complies with Data Standards and that: $

- can be used by CDR consumers to make Consumer Data requests in a timely, efficient and convenient way; $
- is used by the Data Holder to disclose Consumer Data in human-readable form; $ and
- sets out any fees for the disclosure of Voluntary Consumer Data. $

Sharing Consumer Data with Eligible CDR Consumers

A Data Holder must use its **Direct Request Service** to disclose:

- all **Required Consumer Data** requested in compliance with Data Standards: $
  - without charging a fee; $
  - having taken reasonable steps to ensure data is accurate, up-to-date and complete; $
  - unless an exception applies and the Data Holder has informed the CDR Consumer. $
- any **Voluntary Consumer Data** it chooses to disclose.

CONSUMER DATA REQUESTS FROM ACCREDITED PERSONS (ON BEHALF OF ELIGIBLE CDR CONSUMER)

Data Holders must make certain Consumer Data available on request by Accredited Persons in accordance with the implementation deadlines set out on page 9.

Receiving Consumer Data Requests from Accredited Persons

An Accredited Person can request that a Data Holder disclose Consumer Data on behalf of a CDR consumer by using the Data Holder's Accredited Person Request Service in compliance with Data Standards. $

Managing Consumer Data requests from Accredited Persons

Data Holders must provide an online **Accredited Person Request Service** that complies with Data Standards and that: $

+ can be used by Accredited Persons to make Consumer Data requests; and $
+ is used by the Data Holder to disclose Consumer Data in machine-readable form. $

Obtaining authorisation from CDR consumer

Following a Consumer Data request from an Accredited Person, the Data Holder must check that there is a current authorisation from an Eligible CDR Consumer. If no current authorisation exists, the Data Holder must seek authorisation for:

+ all **Required Consumer Data** requested, $ unless an exception applies and the Data Holder has informed the Accredited Person; $
+ any **Voluntary Consumer Data** it is considering disclosing.

When asking for authorisation, the Data Holder must:

+ comply with the Data Standards and information requirements in Rule 4.23 of the CDR Rules; $
+ not add additional requirements, provide/request additional information or offer additional services. $

Managing Authorisation from CDR Consumer

Data Holders must provide an online **Consumer Dashboard** that:

+ can be used by CDR consumers to manage disclosure authorisations (including withdrawals with immediate effect); $
+ contain details of each authorisation (including period and information disclosed); $
+ has all of the functionalities listed in Rule 1.15 of the CDR Rules. $

Sharing Consumer Data with Accredited Person

The Data Holder must use its **Accredited Person Request Service** to disclose in compliance with Data Standards: $

+ all **Required Consumer Data** requested: $
  - without charging a fee; $
  - having taken reasonable steps to ensure data is accurate, up-to-date and complete; $
  - unless an exception exists and the Data Holder has informed the Accredited Person; $
+ any **Voluntary Consumer Data** it chooses to, and is authorised to, disclose.

Where the Data Holder discloses the requested Consumer Data, it must notify the CDR consumer. $

ACCREDITED PERSON'S OBLIGATIONS

CONSUMER DATA REQUESTS FROM ACCREDITED PERSONS (ON BEHALF OF ELIGIBLE CDR CONSUMER)

Consumer Data Requests can be made by an Accredited Person where a CDR consumer has given their consent. For example, where the Accredited Person provides goods or services to the consumer and needs to access their CDR data in order to do this.

Requests for consent from the CDR consumer

An Accredited Person must seek consent (in the form of a "valid" request) from a CDR consumer to collect and use their Consumer Data[$]. To be valid, in accordance with subdivision 4.3.2 of the CDR Rules the request: must, amongst other things:

+ allow the CDR consumer to choose the types of and uses for CDR data collected and period of collection; [$]
+ seek express consent including for any direct marketing; [$]
+ provide the information required by CDR Rule 4.11(3), e.g. how consent can be withdrawn and redundant data is treated, [$]

must not:

× include/refer to other documents, bundle consents or present pre-selected options; [$]
× request consent to sell CDR data unless it is de-identified; or [$]
× generally, request consent to identify, compile insights or build a profile about someone other than the CDR consumer. [$]

The request must also comply with the Data Standards and the data minimisation principle outlined in rule 1.8 of the CDR Rules. [$]

Managing CDR consumer consent - Using the Consumer Dashboard

An Accredited Person must provide an online **Consumer Dashboard** that: [$]

+ can be used by the CDR consumer to manage their consents (including withdrawal), and elect that redundant data be deleted; [$]
+ contains details of each consent to collect and use CDR data (including what CDR data the consent relates to, specified uses, date and expiry of consent and information collected); [$]
+ is updated by the Accredited Person as soon as practicable. [$]

CDR consumer withdrawing consent

A CDR consumer can withdraw consent (a) immediately using the **Consumer Dashboard** or (b) by giving written notice to the Accredited Person.

The Accredited Person must:

+ give effect to written withdrawals of consent within 2 business days of receipt; [$]
+ provide the CDR consumer with a **CDR receipt**; [$]
+ notify the Data Holder in accordance with Data Standards. [$]

If a CDR consumer's consent is still current and 90 days has elapsed since (a) consent was given; (b) the CDR consumer used the Consumer Dashboard or (c) the Accredited Person sent the CDR consumer a notification – the Accredited Person must notify the CDR consumer that their consent is still current. [$]

Requesting Consumer Data from Data Holder

Provided there is valid consent, the Accredited Person can request the Consumer Data from the Data Holder by using the Data Holder's **Accredited Person Request Service** in accordance with the Data Standards. [$]

+ **Using Consumer Data:** An ADR must not use or disclose the Consumer Data, or CDR data directly or indirectly derived from it, other than for a permitted use or disclosure (see rule 7.5 of the CDR Rules). [$]
+ **Redundant data** (i.e. data that is no longer needed for a permitted use or disclosure) that is not required by law or for legal proceedings must be destroyed or de-identified. [$]

OTHER OBLIGATIONS OF DATA HOLDERS AND ADRs

OBLIGATIONS THAT APPLY TO BOTH DATA HOLDERS AND ADRS

Obligation to correct

If a CDR consumer requests correction of CDR data, Data Holders or ADRs (as applicable) must make the correction within 10 business days $ without charge. $

CDR Policy

Data Holders and ADRs must have a clearly expressed up-to-date policy about management of CDR data that is in an approved form and separate from its privacy policies. $ It must include information specified in section 56ED of the CCA and rule 7.2 of the CDR Rules such as outsourced service providers, whether data is stored off-shore and how the ADR deletes redundant data and uses de-identified data. $

The CDR policy must be available through each online service used to deal with CDR consumers, $ without charge. An electronic or hardcopy must be provided where requested by a CDR consumer. $

Record Keeping

Data Holders and Accredited Persons (including ADRs) have various record-keeping and reporting obligations. $

Audits

Data Holders and Accredited Persons (including ADRs) must comply with requests for information from relevant regulators. $

OBLIGATIONS THAT ONLY APPLY TO DATA HOLDERS

Internal Dispute Resolution

For Open Banking, Data Holders must have internal dispute resolution processes that for banking, comply with ASIC Guide 165. $

External Dispute Resolution

Data Holders must be a member of AFCA. $

Joint Account Management Service

Data Holder must provide a **Joint Account Management Service** for joint account holders to jointly elect to either make Consumer Data requests directly, authorise disclosure of joint account Consumer Data to an Accredited Person, withdraw consent or revoke election. $ If an election is made, the Data Holder must give effect to it as soon as possible. $

OBLIGATIONS THAT ONLY APPLY TO ADRS

Accredited Person obligations

Accredited Persons (including ADRs) must comply with the obligations required for Accredited Persons at the 'unrestricted level' (see rule 5.12 of the CDR Rules), $ conditions of their accreditation $ and other notification requirements. $

Outsourcing

If an Accredited Person (including an ADR) discloses CDR data to another person under an outsourcing arrangement, it must ensure they comply with its requirements. $

PRIVACY SAFEGUARDS

The CDR Act establishes 13 privacy safeguards to protect the privacy or confidentiality of CDR consumers (**Privacy Safeguards**). This is supplemented by the CDR Rules which outline what is needed to comply with each Privacy Safeguard. It is intended that the privacy protection under the CDR regime is stronger than that available under the Australian Privacy Principles (**APPs**). The table below demonstrates the strength of each Privacy Safeguard relative to the equivalent APP.

The Privacy Safeguards, taken collectively, are intended to be an expansion of APP 12 and are designed to make gaining access to data easier for both individuals and businesses.

Role of the OAIC

The OAIC will lead on matters concerning the protection of privacy and confidentiality of individuals and small businesses participating in the CDR regime and compliance with the Privacy Safeguards. The OAIC will be the primary complaints handler under the CDR regime, with a range of investigative and enforcement powers and will work closely with the ACCC to address any systemic breaches.

The OAIC has developed a set of Privacy Safeguard Guidelines, based on the structure of the existing APP Guidelines, that are currently under consultation. These Guidelines set out the OAIC's current understanding and interpretation of the Privacy Safeguards and accompanying CDR Rules.

Consequences of breach

The CDR regime provides for a direct right of action for both individuals and businesses to recover for loss or damage that arises from a breach of the Privacy Safeguards under the CCA. No such right currently exists under the Privacy Act. We note that this direct right of action applies to a broader range of information than under the Privacy Act since CDR data is not confined to personal information.

Further, the penalty regime for breach of a Privacy Safeguard is much higher than that currently available under the Privacy Act. The current maximum penalty available under the Privacy Act (for serious or repeated breaches of privacy) in respect of corporations is $2.1 million. In contrast, a breach of a Privacy Safeguard may result in a maximum civil penalty under the CCA regime (with no requirement for breaches to be serious or repeated), being the greater of $10 million; three times the total value of the benefits that have been obtained from the breach; or 10% of the annual domestic turnover of the entity that committed the breach.

LEGEND

APP Privacy Safeguard is as onerous as equivalent APP

APP Privacy Safeguard is more onerous than equivalent APP

ADR ADRs are to comply

DH Data Holders are to comply

PRIVACY SAFEGUARD		COMPARED TO EQUIVALENT APP
PS 1 - Open and transparent management of CDR Consumer Data	ADR DH APP 1	
PS 2 - Anonymity and pseudonymity	ADR DH APP 2	
PS 3 - Soliciting CDR Consumer Data from CDR participants	ADR APP 3	PS 3 sets out that collection of CDR data is not permitted unless the CDR consumer has requested the collection occur. APP 3 requires that the information collected must be reasonably necessary for the functions of the collecting entity.
PS 4 - Dealing with unsolicited CDR Consumer Data from CDR participants	ADR APP 4	If CDR data is collected otherwise than in accordance with PS 3 then it must be destroyed as soon as practicable Under APP 4 if the data could have been collected under APP 3 then it is a valid collection.
PS 5 - Notifying the collection of CDR Consumer Data	ADR APP 5	Notification under PS 5 must be at or before the point of collection while APP 5 allows for subsequent notification.
PS 6 - Use or disclosure of CDR Consumer Data by ADRs or designated gateways	ADR APP 6	CDR data under PS 6 may only be used in response to a valid request. APP 6 allows for use of personal information for a purpose other than the primary purpose, provided an exception applies, including where the alternative purpose would be reasonably expected.
PS 7 - Use or disclosure of CDR Consumer Data for direct marketing by ADRs	ADR APP 7	CDR data must not be used for direct marketing unless it is in response to a valid request or the disclosure is expressly consented to. Direct marketing is allowed under APP 7 where the individual would reasonably expect such use.
PS 8 - Overseas disclosure of CDR Consumer Data by ADRs	ADR APP 8	
PS 9 - Adoption or disclosure of government related identifiers by ADRs	ADR APP 9	If CDR data includes a government related identifier of a CDR consumer, the ADR must not adopt it as the personal identifier of the CDR consumer, unless authorised by law. APP 9 provides for a broader set of acceptable circumstances.
PS 10 - Notifying of the disclosure of CDR Consumer Data	ADR DH	No equivalent APP
PS 11 - Quality of CDR Consumer Data	ADR DH APP 10	
PS 12 - Security of CDR Consumer Data	ADR DH APP 11	
PS 13 - Correction of CDR Consumer Data	ADR DH APP 13	

AUTHORS

ELIZABETH AVERY
Partner, Competition + Regulation
T +61 2 9263 4362
M +61 411 314 505
E eavery@gtlaw.com.au

MELISSA FAI
Partner, Technology + Digital
T +61 2 9263 4685
M +61 404 873 252
E mfai@gtlaw.com.au

CHERRIE FUNG
Lawyer, Competition + Regulation
T +61 2 9263 4727
M +61 410 539 646
E fung@gtlaw.com.au

NICOLA JACKSON
Lawyer, Competition + Regulation
T +61 3 8656 3314
M +61 457 808 078
E njackson@gtlaw.com.au

DILYS TENG
Knowledge Lawyer,
Knowledge + Practice Innovation
T +61 3 8656 3388
M +61 402 511 541
E dteng@gtlaw.com.au

REBECCA CHING
Lawyer, Competition + Regulation
T +61 2 9263 4242
M +61 429 501 976
E rching@gtlaw.com.au

MATTHEW HARGREAVES
Lawyer, Technology + Digital
T +61 3 8656 3490
E mhargreaves@gtlaw.com.au

The authors would like to thank Joy Chen for her contribution to this publication.