Australian Government

Consumer Data Right

# Frequently asked questions (FAQs) – Consumer Data Right

## 1 General

### 1.1 What is Consumer Data Right?

Consumer Data Right is an economy-wide reform that will apply sector by sector, starting with banking. Consumer Data Right's objective is to enable individual and small business consumers (**consumers**) to efficiently and conveniently access specified data about them held by businesses (**data holders**), and to authorise the secure disclosure of that data to third parties (**accredited data recipients**) or to themselves.

The right is designed to give consumers more control over their data. Consumers' improved data control will support the development of better and more convenient products and services, customised to individual needs, and consumer privacy.

Consumer Data Right also requires businesses to publish information about their standard products. Better price comparison services, which consider consumers' actual usage and circumstances, will help consumers save money by securing personalised, cost-effective services.

Privacy protection and robust information security are a core feature of the system.

### 1.2 What is the background to Consumer Data Right? Where did the idea come from?

Several government reviews, including the Murray, Harper, Coleman and Finkel inquiries, recommended that Australia develop a right and standards for consumers to access and transfer their information in a usable format.

Also, in May 2017, the Australian Government received the Productivity Commission's report on its Inquiry into Data Availability and Use. The report made 41 recommendations, including for the creation of a new economy-wide 'comprehensive data right'.

On 20 July 2017, the then Treasurer, the Hon. Scott Morrison MP, commissioned the Review into Open Banking in Australia (**the review**) to identify the most appropriate model for open banking in Australia. Following the review, the government decided to legislate a Consumer Data Right. The Treasurer will lead its development. Before making final decisions on implementation, the government released the report of the Review into Open Banking in Australia on 9 February 2018 for public comment on its recommendations.

On 9 May 2018, the government agreed to the recommendations of the review, both for the framework of the overarching Consumer Data Right and for the application of the right

to the banking sector, with a phased implementation from July 2019, starting with the publication of product reference data by the big four banks.

## 1.3 Who is implementing Consumer Data Right and making sure it functions as intended?

Consumer Data Right is regulated by the Australian Competition and Consumer Commission (**ACCC**) and the Office of the Australian Information Commission (**OAIC**), as it concerns both competition and consumer matters as well as the privacy and confidentiality of consumer data.

The ACCC leads on developing the Consumer Data Right Rules and which additional sectors of the economy will come under Consumer Data Right. Monitoring compliance with and enforcement of the Consumer Data Right Rules is also a key feature of the ACCC's role.

The ACCC is also the Data Recipient Accreditor and the Accreditation Registrar. This means the ACCC is responsible for building, testing and managing the Consumer Data Right Register, which is essential to ensure that data sharing is safe and secure.

The OAIC leads on matters relating to the protection of individual and small business consumers' privacy and confidentiality, and compliance with the Consumer Data Right Privacy Safeguard Guidelines (Privacy Safeguard Guidelines).

A Data Standards Body (**DSB**) helps the Data Standards Chair in making data standards for Consumer Data Right. The data standards prescribe the format and process by which Consumer Data Right data is to be shared with consumers and accredited data recipients within the Consumer Data Right system.

## 1.4 When will Consumer Data Right launch?

Consumer Data Right is being implemented in phases.

From July 2019, Australia and New Zealand Banking Group Limited (**ANZ**), Commonwealth Bank of Australia (**CBA**), National Australia Bank Limited (**NAB**), and Westpac Banking Corporation **(Westpac)** (collectively the 'four major banks') published their 'product reference data' (**PRD**)[1], which is general information for which there are no specific Consumer Data Right consumers, such as interest rates, fees and charges, discounts and other features for their standard products, such as transaction accounts, term deposits, and credit card and debit card accounts. From February 2020, the four major banks must also publish mortgage and personal loan PRD.

At this stage, PRD is most useful to business end users, such as comparison websites. It is an important step in enabling comparison of banking products in a meaningful like-for-like manner.

From July 2020, consumers of the four major banks will be able to share their banking data. The following is an overview of the data that the four major banks must make available from:

[1] Detailed descriptions of the PRD API payloads are available from the Consumer Data Standards website: https://consumerdatastandardsaustralia.github.io/standards/#get-products

- July 2020: savings and transaction accounts, call accounts, term deposit accounts, current accounts, cheque accounts, debit, credit or charge card accounts, personal basic accounts and GST or tax accounts (not all personal accounts which may fit these descriptions will be available from July).
- November 2020: home loans, personal loans and mortgage offset accounts. Joint accounts, closed accounts, direct debits, scheduled payments and payees will also become available.

The ACCC consulted with the major and non-major banks to make sure the implementation timetable is achievable.

In light of the COVID-19 pandemic, the ACCC granted three-month exemptions to financial services providers that are required to share product reference data by 1 July 2020 under the Consumer Data Right. These temporary exemptions until 1 October, will apply to non-major ADIs, non-major banks, building societies and credit unions, and to non-primary brand products offered by the major banks.

## 1.5 Who are the key parties involved in Consumer Data Right?

**Consumers**

Consumer Data Right focuses on giving value to consumers. Its success depends on consumer trust in, and ability to use, Consumer Data Right products and services. The Consumer Data Right system is designed for consumers and includes strong privacy protections and requirements around consent.

All eligible customers—individuals or businesses—will be entitled to exercise the right to access and share their Consumer Data Right data.[2] Consumer Data Right will therefore benefit some customers who may not be considered 'consumers' under other laws.

The Consumer Data Right Rules provide that a 'Consumer Data Right consumer' for the banking sector must:

- be 18 years or older if the Consumer Data Right consumer is an individual (this requirement does not apply to Consumer Data Right consumers who are businesses)
- have an account with the data holder that is open and can be accessed online.

The Consumer Data Right Rules will progressively apply to a broader range of consumers, such as those who hold closed accounts. From November 2020, the Consumer Data Right Rules will also apply to joint accounts held in the name of two consumers.

**Data holders**

Data holders, the businesses who hold specific data that Consumer Data Right enables consumers to access, are the second group of key participants in the Consumer Data Right system. At a consumer's direction, a data holder will be obliged to share a consumer's data with either:

a) an accredited data recipient to whom the consumer has provided their consent, or

b) the consumer themselves, subject to the commencement schedule.

---

[2] For the full definition of eligible consumer, see clause 21 of Schedule 3 of the *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth).

In the case of banking, the initial data holders are the four major banks. This will expand to include most authorised deposit-taking institutions (ADIs), with some exceptions, such as foreign ADIs.

An ADI is a body corporate that the Australian Prudential Regulation Authority (**APRA**) has authorised to carry on 'banking business' in Australia. APRA maintains a register of ADIs on its website.

**Accredited data recipients**

Accredited data recipients are the third key group of participants in the Consumer Data Right system. Consumers can transfer their own Consumer Data Right data to themselves or to accredited data recipients.

Accreditation criteria, including privacy and information security requirements, are set by the ACCC in consultation with the government, Consumer Data Right agencies and industry.

Initially, there will be one level of accreditation: the 'unrestricted level'. To be accredited at the unrestricted level, applicants must satisfy certain requirements, including information security obligations to ensure the security of Consumer Data Right data. Subject to ongoing obligations, unrestricted accredited data recipients will be able to receive all Consumer Data Right data within scope for banking.

If an accredited data recipient breaches its obligations under the Consumer Data Right regime, this may lead to the revocation or suspension of its accreditation, or imposition of conditions on its accreditation.

The nature and number of accredited data recipients in the Consumer Data Right regime will grow and change over time but will initially include businesses such as 'fintechs' (financial technology firms) and other ADIs. Fintechs use the internet, mobile devices, software technology or cloud services to perform or connect with financial services. Many fintech products are designed to connect consumers' finances with technology for ease of use, although the term is also applied to business-to-business technologies. In the context of Consumer Data Right, fintechs will offer consumers innovative products and services, including budgeting, comparison and forecasting services.

The ACCC has worked with the initial testing participants who are expected to be the first ADRs in the Consumer Data Right ecosystem. The ACCC will advise other businesses on when they can apply to become accredited.

## 1.6 How will the government decide the next sectors for Consumer Data Right implementation?

After banking, application of Consumer Data Right in energy and telecommunications is expected to follow. Future sectors of the economy which will become part of Consumer Data Right will be identified through sectoral assessments by the ACCC. The ACCC may conduct a sectoral assessment on its own initiative or at the request of the Treasurer.

Following an assessment, the ACCC advises the Treasurer on whether to designate a sector. The OAIC aids in assessments and also advises the Treasurer regarding the privacy impact of designating a sector. The Treasurer then determines whether the benefits of designating a sector outweigh the costs and then designates that sector.

This involves consideration of the likely:

- effects on consumers
- effects on relevant markets, including market efficiency, integrity and safety
- effects on privacy for individuals and confidentiality for businesses
- regulatory effect of consumer data rules
- effects on intellectual property rights
- any other relevant matters.

## 1.7 What data will be shared under Consumer Data Right?

In the banking sector, there are four categories of data that consumers will be able to request a data holder share:

- **customer data** including a customer's:
  - name
  - contact details
  - information provided when acquiring or relating to their eligibility to acquiring that product
  - details if they operate a business (such as business name, ABN and ACN, the type of business, date of establishment, and organisation type)
- **account data** including:
  - account number and name
  - the opening and closing balances for the account
  - authorisations on the account, including direct debit deductions, scheduled payments and payee details stored with the account
- **transaction data** including:
  - the transaction date
  - any identifier for the counter-party to the transaction
  - if the counter-party is a merchant, any information provided by the merchant pursuant to the transaction
  - the amount debited or credited pursuant to the transaction
  - the opening and closing balances for the account including a current balance and available funds
  - any description in relation to the transaction
  - the categorisation of the transaction (for example, whether the transaction is a debit, a credit, a fee or interest)
- **product-specific data** including:
  - product type and product name
  - its price, including fees, charges and interest rates associated with the product, and the circumstances in which these apply
  - features and benefits, including discounts and bundles
  - terms and conditions
  - customer eligibility criteria.

As noted above, Consumer Data Right data about different categories of banking products will be made available at different times.

The Australian Government, in consultation with interested parties, will determine the scope of the data to be made available under Consumer Data Right in the energy sector.

# 2 Data sharing, security and privacy

## 2.1 How does the Consumer Data Right system help consumers to share their data safely?

Data holders must share Consumer Data Right data with ACCC-accredited data recipients of the consumer's choosing after the consumer has explicitly consented to this. Rigorous consent requirements apply to both the collection of Consumer Data Right data and subsequent use of Consumer Data Right data under the Consumer Data Right Rules.

The focus of consent to collect and use Consumer Data Right data should be on transparency and ensuring consumers understand what they are agreeing to. The consent rules aim to ensure that consent is:

- voluntary
- express
- informed
- specific as to purpose
- time limited
- easily withdrawn.

To make sure that the consent process meets this objective, the Consumer Data Right Rules set out several obligations on accredited persons, including that an accredited person must:

- only ask a consumer for their consent to collect data and with a time period that is reasonably needed to provide the good or service they are offering
- not bundle consent with other directions, permissions, consents or agreements
- not include or refer to other documents during the consent process
- give the consumer an active choice to give consent, for example consent must not be the result of default settings.

The consumer must be able to select or indicate their consent for:

- the types of data to be collected
- the specific uses of that data
- a period over which that data is to be collected and used, up to a maximum of 12 months, including whether Consumer Data Right data may be:
    - collected on a single occasion and used over a specified period of time, or
    - collected and used over a specified period of time.

A request for consent must be presented to a consumer using concise, easily understood language and/or visual aids.

An accredited data recipient must offer consumers a straightforward process to withdraw consent and inform each consumer about that process before receiving their consent. This must include how their data is treated once consent is withdrawn, for example if it is to be deleted or de-identified.

When giving consent, using the accredited data recipient's dashboard, the consumer has the right to elect their Consumer Data Right data be deleted, at any time, once it is no longer needed. This can only happen before data is de-identified.

Transferring customer data using the Consumer Data Right ecosystem is safer and more secure than traditional data sharing practices, such as screen scraping.

## 2.2 After a consumer has consented, how can they be sure their privacy will be protected in the Consumer Data Right system?

Privacy and security are core features of Consumer Data Right. To protect and strengthen the privacy of consumers' data, the legislation and Rules tailor privacy protections to reflect the needs of Consumer Data Right and each sector. These privacy protections include:

- the mandatory accreditation of data recipients
- requirements that data can only be transferred to accredited data recipients at the consumer's direction
- requirements for greater transparency and choice so that consumers control how their information will be used
- obligations regarding deletion or de-identification of data
- the introduction of data standards for the transfer of Consumer Data Right data
- extending the *Privacy Act 1988* obligations to bind all accredited data recipients in their handling of data other than Consumer Data Right data, including small to medium sized enterprises
- avenues for consumers to seek meaningful remedies for breaches, including external dispute resolution and direct rights of action.

The OAIC will advise on and enforce privacy safeguards under Consumer Data Right including the requirement for a Consumer Data Right policy. Data holders and accredited data recipients must have a 'Consumer Data Right policy' which provides consumers with clear information and guidance about how they will manage Consumer Data Right data and how consumers can access their dispute resolution process if they have a complaint, including complaints about how their Consumer Data Right data has been managed.

Data holders and accredited data recipients must make it easy for consumers to access their Consumer Data Right policy on their website.

## 2.3 If a consumer decides to share their Consumer Data Right data with an accredited data recipient, how do they keep track of their data sharing arrangements?

Accredited data recipients must provide consumers with a consumer dashboard that enables them to see and manage their consents for the collection and use of their Consumer Data Right data.

Data holders must also provide consumers with a consumer dashboard that enables them to manage and see their authorisations for the disclosure of their Consumer Data Right data. These dashboards must be an online service and can be built into existing online banking or mobile apps.

The consumer dashboard must contain functionality that allows a Consumer Data Right consumer, at any time, to withdraw authorisations to disclose Consumer Data Right data. This functionality must:

- be simple and straightforward to use
- be prominently displayed
- be no more complicated than the process for giving the authorisation to disclose the Consumer Data Right data

- as part of the withdrawal process, display a message relating to the consequence of the withdrawal.

Withdrawing authorisation[3] on the dashboard will also require the accredited data recipient to stop using the Consumer Data Right data they have already collected, as well as delete or de-identify the previously collected Consumer Data Right data, in line with a consumer's election and the accredited data recipient's Consumer Data Right policy.

The consumer dashboard provided by an accredited data recipient must contain a functionality that allows a Consumer Data Right consumer, at any time, to:

- withdraw consents to collect and use Consumer Data Right data
- elect that redundant data be deleted and withdraw such an election.

These functionalities must be simple and straightforward to use, and prominently displayed.

Accredited data recipients' dashboards must include information to help a consumer identify what data was being shared, for how long, and from which data holder, while the data holder's dashboard should identify which accredited data recipient Consumer Data Right data is being shared with.

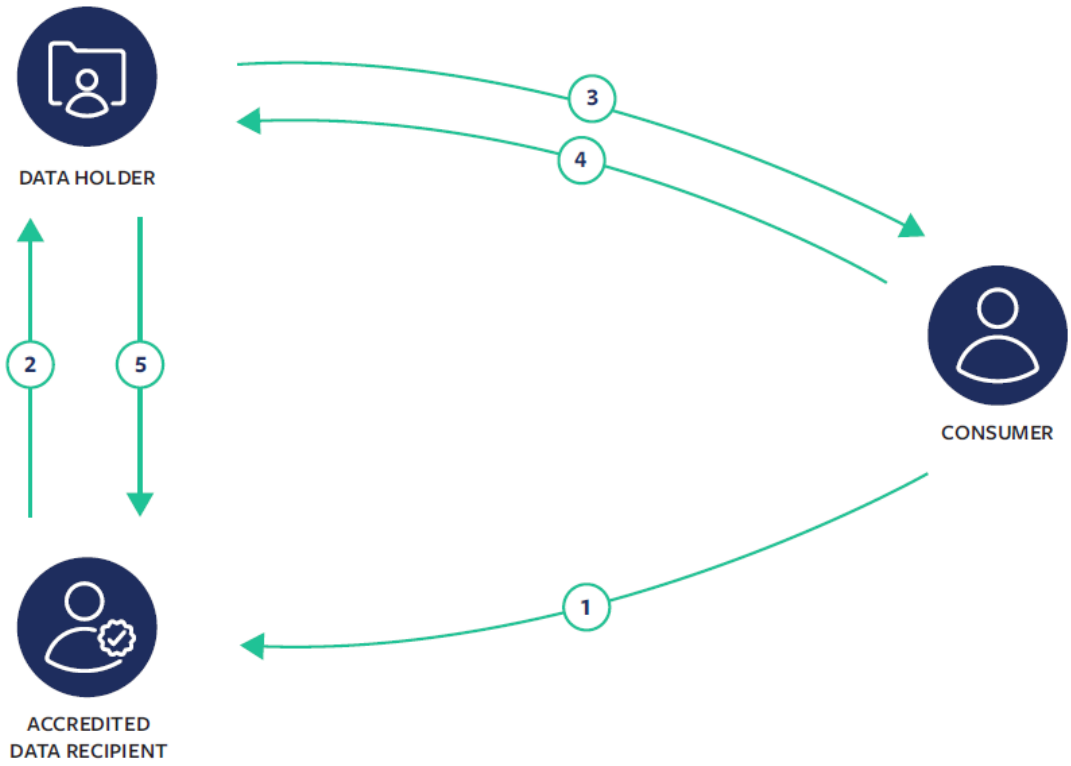
## 2.4 What is the purpose of the consent process? How will this affect my use of the Consumer Data Right system?

Consumer Data Right places a high threshold on consent, so consumers know what they are agreeing to when they consent to their data being collected and used. The focus of consent to collect and use consumer data is on transparency and making sure consumers understand the benefits and any potential consequences of what they are agreeing to.

Once consumers have provided explicit consent for their data to be collected and used to an accredited data recipient, using the Consumer Data Right system will be straightforward. Consumers can view any activities relating to their data using their own consumer dashboard provided by the accredited data recipient. Consumers can also use this database to withdraw their consent, at any time.

The DSB has published Consumer Experience (**CX**) Guidelines, which will provide accredited data recipients and data holders with standards and guidance for seeking and receiving consent from consumers, the process for which is shown in the diagram below.

[3] **NB**: **Authorisation** is used to refer to the consumer permitting the data holder to share their data with the accredited data recipient that has requested it. **Authorisation** also has a technical meaning that relates to a process by which the accredited data recipient's application obtains access to the consumer's data via the data holder's API. **Authentication** is the process by which the data holder verifies the identity of the consumer directing the sharing of their data, and the identity of the accredited data recipient seeking to collect the consumer's data. Authentication occurs as part of the authorisation process.




1. The consumer consents to the accredited data recipient obtaining their data
2. The accredited data recipient seeks to access the consumer's data and their identity and accreditation status is authenticated by the data holder
3. The data holder authenticates the identity of the consumer
4. The consumer authorises the data holder to disclose their data to the accredited data recipient
5. The consumer's data is shared between the data holder and the accredited data recipient

A successful consumer experience will be fostered by an evidence-based consent process and a trusted Consumer Data Right ecosystem that can help consumers:

- understand what they are consenting to and why their data is being requested
- understand what they are sharing and how it will be used
- understand and trust who will have access to their data and the duration of that access
- understand how to manage and withdraw consents and authorisations
- understand the implications of withdrawing consents and authorisations
- feel confident and informed about the sharing of their data
- understand how to navigate the consent process.

# 3 Breaches of Consumer Data Right

## 3.1 What happens if there is a breach of Consumer Data Right?

The ACCC's approach to compliance and enforcement is underpinned by the objective of ensuring that consumers can trust the security and integrity of the Consumer Data Right regime. The Consumer Data Right regulatory framework, which covers the *Competition*

*and Consumer Act 2010* (Cth) (**the Act**) and the Consumer Data Right Rules, establishes clear principles of liability to ensure that data holders and accredited data recipients act appropriately.

Under the Act, individual consumers also have a right of action against persons who fail to comply with a binding data standard.

The Consumer Data Right regulatory framework specifies that Consumer Data Right enforcement will be a co-regulatory effort between the ACCC and the OAIC.

The OAIC will be primarily responsible for complaint handling and for strategic enforcement relating to the protection of privacy and confidentiality. The OAIC will also receive and handle notifications of eligible data breaches relating to Consumer Data Right data.

The ACCC will be responsible for compliance and enforcement of the Rules, data standards, participant-to-participant conduct and taking strategic enforcement action. The ACCC will focus on addressing conduct that has broader industry detriment.

Prevention of a breach through the ACCC's and OAIC's compliance activities is preferable to taking action after the breach has occurred. However, where we believe a breach has occurred, we will take regulatory action proportionate with the seriousness of the breach and the level of harm or potential harm. We have several enforcement options (remedies) available to us to respond to and resolve breaches of the Consumer Data Right legislation, including: infringement notices, court enforceable undertakings, suspension or revocation of accreditation, and court proceedings. The court may make a range of orders including civil penalties and injunctions.

# 4 Accreditation

## 4.1 Why would a business apply for accreditation?

Accredited data recipients may receive a Consumer Data Right consumer's data from a data holder at the request and consent of the consumer.

Any person, in Australia or overseas, who wishes to receive Consumer Data Right data to offer products or services to consumers must be accredited.

To become accredited, a person must apply to the Data Recipient Accreditor (the ACCC). The ACCC will only accredit a person if it is satisfied that the person meets the criteria for accreditation.

## 4.2 What are the criteria for accreditation?

An applicant must satisfy certain requirements to be accredited at the 'unrestricted' level, which include:

- being a fit and proper person to manage Consumer Data Right data
- undertaking information security measures to protect Consumer Data Right data from misuse, interference, loss, unauthorised access, modification or disclosure
- ensuring internal dispute resolution processes are in place
- holding membership with a recognised external dispute resolution scheme in relation to Consumer Data Right consumer complaints

- having adequate insurance, or comparable guarantee, relevant to the nature and extent of their management of Consumer Data Right data.

There are ongoing obligations under Part 5 of the Consumer Data Right Rules that must be met, once applicants become accredited.

For more detailed information about the accreditation criteria, please see the ACCC's draft Consumer Data Right Accreditation Guidelines.

## 4.3 Are there different levels of accreditation?

Currently there is only an unrestricted level of accreditation. We expect that additional levels of accreditation will be included in the future as Consumer Data Right develops and other sectors are introduced to the Consumer Data Right regime. There are no fees to apply for accreditation.

Once accredited, an accredited data recipient must meet ongoing obligations to maintain accreditation.

For the banking sector, ADIs (other than restricted ADIs) meet the criteria for the streamlined (unrestricted) accreditation process and may complete a streamlined version of the approved form. However, once accredited, ADIs must still comply with the ongoing obligations of a person accredited at the unrestricted level (excluding the insurance obligation).

## 4.4 How can a consumer identify someone as an accredited person?

If it accredits an applicant, the Data Recipient Accreditor (the ACCC) must give the applicant a unique number that identifies them as an accredited person. This number is known as an accredited person's accreditation number. Accreditation takes effect once the applicant is included on the Register of Accredited Persons (the Register). Any person can check the Register at any time to confirm whether a business they are considering is an accredited person.

The ACCC is registering the Consumer Data Right logo as a trade mark. The Consumer Data Right logo will be present during the consent process to indicate to consumers that the provider they are looking to share their data with is an ACCC-accredited data recipient.

## 4.5 What happens if an accredited person does something wrong?

As the Data Recipient Accreditor, the ACCC may suspend or revoke an accredited data recipient's accreditation where:

- the accredited data recipient obtained its accreditation through false or misleading statements or other irregular means
- the ACCC believes, on reasonable grounds, that the accredited data recipient has contravened, or the accredited person has been found to have contravened, a law relevant to the management of Consumer Data Right data or a civil penalty provision of the CCA or Rules or the data standards or a condition of its accreditation (where applicable)
- civil or criminal proceedings are commenced against the accredited data recipient, or a director of the accredited data recipient, by a public agency in Australia alleging a contravention of the CCA (including the Australian Consumer Law), the ASIC Act, the Privacy Act or a serious offence or an offence of dishonesty

- the accredited data recipient becomes insolvent (in the case of an individual, the individual becomes bankrupt or enters into a personal insolvency agreement; in the case of a company, the company enters into liquidation, administration or receivership)
- the ACCC considers it necessary for consumer protection, or to protect the security, integrity, stability of or trust in the Consumer Data Right regime
- in the case of ADIs that have been registered as accredited data recipients, the ADI has its ADI status suspended or revoked
- the ACCC is no longer satisfied that the accredited person is a fit and proper person to manage Consumer Data Right data, in line with the fit and proper persons criteria, or
- a current contract between the accredited data recipient and a Consumer Data Right consumer has been found to have an unfair term.

Where the ACCC intends to suspend, vary or revoke an accredited data recipient's accreditation, it must provide written notice of the proposed decision and reasons to the accredited data recipient and provide an opportunity for the accredited data recipient to respond.

# 5 Further information

## 5.1 How can people stay informed about Consumer Data Right developments?

For further general information about Consumer Data Right, please sign up to the ACCC's Consumer Data Right newsletter here, and refer to the ACCC's website, the OAIC's website, the Consumer Data Standards website and the Treasury website.