Australian Government

Consumer Data Right

# Your privacy rights

November 2020

Consumer Data Right gives you control over information businesses have about you. It allows you to give access to this information to a business, accredited by the Australian Competition and Consumer Commission as a data recipient, so they can offer products and services tailored to your needs.

Consumer Data Right is an opt-in system and strict privacy safeguards are in place to protect your data.

You have the choice to give consent to an accredited data recipient accessing your data and you can withdraw your consent at any time. You also control what data is transferred and what it can be used for, and you can ask for your data to be deleted if it is no longer needed.

The Consumer Data Right privacy safeguards set out your privacy rights and the strict obligations on businesses collecting and handling your data. There are 13 legally binding privacy safeguards.

## 1: Open and transparent management of data

Businesses must have procedures and systems in place to ensure they meet their privacy obligations under Consumer Data Right. This includes having a clearly expressed and up-to-date Consumer Data Right policy about how they manage your data.

## 2: Anonymity and pseudonymity

An accredited data recipient must provide you with the option to not identify yourself or allow you to use a pseudonym. There are some exceptions to this. For example, when it is not practical for the business to deal with a consumer who has not identified themselves or has used a pseudonym, or if a law or a court order requires that they deal with an identified consumer.

## 3: Seeking to collect data

An accredited data recipient can only try to collect your data from another business if they have your express consent. They must not seek to collect data beyond what they need to provide the product or service to you.

## 4: Dealing with unsolicited data from Consumer Data Right providers

An accredited data recipient must delete any Consumer Data Right data where consent has not been received to collect it, unless a law or court order requires it to be retained.

## 5: Notification of collection

An accredited data recipient must notify you through your consumer dashboard when they collect your data. A consumer dashboard is an online service that enables you to see and manage your consents for the collection, use and disclosure of your data. It can be built into existing online portals or mobile apps and must be provided by all businesses participating in Consumer Data Right.

## 6: Use or disclosure of data

Businesses can use or disclose your data only where required or authorised under Consumer Data Right and only with your consent, unless otherwise required by a law or a court order. For example, a business can use or disclose your data to provide you with the product and service you requested.

## 7: Direct marketing

Your data cannot be used for direct marketing unless you consent and it is allowed under the Consumer Data Right Rules. For example, a business can provide information about an upgraded or alternate product or service to you, if you have consented to this.

## 8: Overseas disclosure of data

An accredited data recipient must not send your data overseas, unless an exception applies. For example, if the business receiving your data overseas is also accredited under the Consumer Data Right system.

## 9: Adoption or disclosure of government identifiers

An accredited data recipient cannot adopt, use or disclose a government-related identifier, such as a Medicare or Australian passport number, unless required or authorised under another law, court order or privacy regulations.

## 10: Notification of disclosure

When a business discloses your data to an accredited data recipient, they must notify you by updating your consumer dashboard.

## 11: Quality of data

Businesses must ensure the quality of your data. They must inform you if incorrect data is disclosed and they must provide the corrected data to the accredited data recipient on your request.

## 12: Security of data and the handling of redundant data

An accredited data recipient must meet strict information security requirements. This includes ensuring your data is protected from misuse, interference and loss, as well as from unauthorised access, modification or disclosure. Any data that is no longer needed for a permitted purpose must be deleted or de-identified, unless an exception applies.

## 13: Correction of data

Businesses must respond to data correction requests and take steps to correct or add a qualifying statement to the data to ensure the data will not be misinterpreted. They must notify you when they have done so or explain why a correction or statement is unnecessary or inappropriate.

## What if you have a complaint?

If your data is mishandled or you believe your privacy has been breached, you can make a formal complaint about it to the business.

If the business does not respond to your complaint within a reasonable period (usually 30 days) or you are not satisfied with the response, you can lodge your complaint with the Office of the Australian Information Commissioner (OAIC).

If you have a question about your privacy rights or how to make a complaint, you can visit www.oaic.gov.au or call the OAIC on 1300 363 992.

## More information

More information on Consumer Data Right can be found on www.cdr.gov.au. Alternatively, if you are unable to find the information you are looking for, you can also contact the Consumer Data Right team using the contact us page.


ACCC 11/20_20-64 www.accc.gov.au