

CDR Data Management Policy

MOGOPLUS (Mogo Holdings Pty Ltd)

1. About this Policy

Mogo Holdings Pty Ltd ("**Mogo**", "**MOGOPLUS**", "**we**", "**us**" or "**our**") provides data, analytics and insight solutions to organisations. In some cases, the organisations we work with are Accredited Data Recipients ("**ADR**") under the Consumer Data Right ("**CDR**") regime established under Part IVD of the Competition and Consumer Act 2010 (Cth) and the Competition and Consumer (Consumer Data Right) Rules 2020 (Cth) ("**CDR Rules**").

Mogo is not an Accredited Data Recipient and does not hold CDR accreditation. We act solely as an **Outsourced Service Provider ("OSP")** engaged by ADRs to whom this Policy refers as our "**OSP Principal(s)**".

This Policy explains how we handle CDR data in our capacity as an OSP, under the terms of the relevant CDR outsourcing arrangement(s) we have in place with our OSP Principal(s). It should be read together with our [Privacy Policy](#), which covers our broader handling of personal information under the Privacy Act 1988 (Cth).

Because we are not an accredited person or CDR representative, we are not required to hold a CDR Policy under Privacy Safeguard 1 of the Competition and Consumer Act 2010 (Cth) (section 56ED); the content requirements for a CDR policy are separately set out in rule 7.2 of the CDR Rules. We publish this Policy voluntarily, for transparency, so that consumers and our OSP Principals understand how we handle CDR data that is disclosed to us.

2. Our role as an Outsourced Service Provider

When an ADR engages us to provide our Service, CDR data may pass through our systems as part of that Service. Under the CDR Rules, this data is treated as "**service data**" — data we handle on behalf of, and under the direction of, our OSP Principal.

We operate on a pass-through basis and do not retain CDR data beyond the transient processing necessary to perform the Service. CDR data is processed transiently as it moves through our systems, for the sole purpose of performing the Service, and is not held by us in any persistent database, file store or backup once that processing step is complete.

We do not collect CDR data directly as we are not accredited. Any handling of CDR data by us occurs strictly within the scope of:

- (a) the consumer's consent obtained by our OSP Principal;
- (b) the CDR Rules and the applicable Privacy Safeguards, which our OSP Principal remains responsible and liable for ensuring we comply with.

Our OSP Principal is responsible for identifying us (and any other direct or indirect OSPs it engages) in its own CDR Policy, including our accreditation status (unaccredited), whether we are based overseas, the nature of the services we provide, and that we do not store CDR data.

3. How we handle CDR data

Under our CDR outsourcing arrangement(s), we:

- (a) only process service data for the purposes set out in the relevant CDR outsourcing arrangement and as directed by our OSP Principal, and do so on a **transient, pass-through basis only** – data is not retained by us beyond the transient processing necessary to perform the Service, and is not stored or indexed by us, once it has been passed to our OSP Principal or the intended recipient system;
- (b) do not use service data for our own independent research, marketing, or any purpose outside the scope of the services we have been engaged to provide;
- (c) do not disclose service data to any other party except where permitted under the CDR outsourcing arrangement (for example, to a further OSP engaged by us to assist in providing the Service, in which case that further OSP is bound by equivalent obligations and equivalent no-storage/pass-through requirements, where applicable); and
- (d) take the steps required under Schedule 2 of the CDR Rules to protect service data while it is in our systems — including in transit and during processing — as if we were an accredited data recipient, notwithstanding that the data is not stored by us.

4. Overseas access to CDR data

Mogo's systems used to provide the Service are located in Australia. No CDR service data is processed by, routed through, or accessible from systems or personnel located outside Australia.

Our OSP Principal is responsible for disclosing our location (including whether we are based overseas) and that of any other direct or indirect OSPs it engages, in its own CDR Policy, in accordance with the CDR Rules.

5. Security of CDR data in transit and during processing

Because we do not retain CDR data beyond the transient processing necessary to perform the Service, our security controls are focused on protecting data **while it is in transit and being processed**, consistent with the information security requirements of Schedule 2 to the CDR

Rules. This includes encryption in transit, access controls, and monitoring, with access restricted to systems that are required to perform the Service.

No bank account login credentials (including passwords) are retained by us at any point, consistent with our Privacy Policy.

6. Retention, deletion and de-identification of CDR data

As we do not retain CDR data beyond the transient processing necessary to perform the Service, we do not hold "redundant" CDR data of the kind that would ordinarily require deletion or de-identification under Privacy Safeguard 12 and the CDR Rules. CDR data passing through our systems is not retained beyond the point necessary to complete the relevant processing step in providing the Service to our OSP Principal.

Where our OSP Principal's CDR Policy sets out requirements for the deletion or de-identification of CDR data (including redundant data), those requirements are directed at data that is stored — which, in our case, is not ordinarily applicable, as we do not persist such data in the ordinary course. We remain bound by, and will comply with, any relevant instructions from our OSP Principal regarding the treatment of CDR data that passes through our systems.

Notwithstanding the above, where requested by our OSP Principal, we will return or delete service data (including any transient copies held in caches, message queues, error logs, temporary files or backups) in accordance with the applicable CDR outsourcing arrangement, and will provide confirmation or evidence of that deletion on request.

7. Data breaches and security incidents

We have procedures in place to detect, respond to and report data breaches or security incidents affecting CDR data. Where an incident affects, or may affect, service data, we will notify our affected OSP Principal(s) promptly in accordance with our CDR outsourcing arrangement, so that they can meet their own notification obligations to consumers and regulators.

8. Your rights as a consumer

Because we act as an OSP and not as the ADR you have a direct relationship or consent arrangement with, **we are generally not the appropriate party to action CDR consumer rights** such as requests to access, correct or withdraw consent regarding your CDR data. These rights sit with the ADR that obtained your consent.

If you have a question or concern about how your CDR data has been handled, we recommend you contact the ADR or organisation you dealt with directly, and refer to their CDR Policy. You are also welcome to contact us using the details below and we will assist where we are able to, including by directing your enquiry to the relevant OSP Principal.

9. Complaints

If you believe we have not handled CDR data in accordance with our obligations under a CDR outsourcing arrangement, you can contact us using the details in section 10 below. We will investigate and respond within a reasonable timeframe.

You may also be able to raise a complaint with the relevant ADR, or with the Office of the Australian Information Commissioner (OAIC) on 1300 363 992 or at www.oaic.gov.au.

10. Contact us

If you have any questions about this CDR Data Management Policy, please contact us at:

support-AU@mogoplus.com

11. Changes to this Policy

We may update this Policy from time to time to reflect changes in our services, our CDR outsourcing arrangements, or the CDR Rules. The current version will always be available on our website.

Last updated: 06 Aug 2026