Product Schedule

CDR Services

V1.2 effective from 4 November 2026

Table of contents

Part 1 – CDR Services general terms

1 What is this document? 1
2 How are the Services provided? 1
3 What are your obligations? 1
4 How do we manage intellectual property? 3
5 Additional CDR Services general terms 4

Part 2 –Service-specific terms

6 Experian as Accredited Data Recipient terms 4
7 Experian as Accredited Requestor service terms 5
8 Transaction Risk Score service terms 6

Part 1 – CDR Services general terms

Part 1 applies to all CDR Services

1 What is this document?

1.1 It applies to all CDR Services

This Product Schedule only applies to Services involving CDR Data that we collect to provide to you, as an Accredited Data Recipient (where the Location is Australia) or as an Accredited Requestor (where the Location is New Zealand). All references to Services in this Product Schedule refer to CDR Services in the Location.

1.2 Definitions

Capitalised terms used in this Product Schedule have the meaning given to them in:

a. the Work Order;
b. the Experian Dictionary accessible at www.experian.com.au/terms; or
c. the following terms have the meaning given to them in the CDR Laws:
   i. where the Location is Australia: Accredited Data Recipient and CDR Representative; and
   ii. where the Location is New Zealand: Accredited Requestor.

2 How are the Services provided?

2.1 We operate under applicable Laws

Our ability to provide the Services is subject to Law (including CDR Laws).

2.2 We use our Related Bodies Corporate

The Services are provided by:

a. Experian Open Data Solutions Pty Ltd (ADRBNK000017) where the Location is Australia; and
b. Experian Open Data Solutions (NZ) Limited (Co. No. 9388757) where the Location is New Zealand (**Experian, we, our, us**).

3 What are your obligations?

3.1 Using the Services

You must:

a. only use the Services for the Authorised Use and in line with their intended purpose and applicable Laws;
b. implement and maintain industry best practice security measures and safeguards in relation to your computer systems, network and internet connectivity to access the Services;
c. use the Services on up to date and secured hardware, networks, systems and software;
d. comply with all applicable technical safeguards and access restrictions designed to protect the integrity and security of the Services;
e. keep all Credentials secure and confidential. If there is any unauthorised use of Credentials, you must promptly notify us, change the affected Credentials (if you can), and follow our reasonable instructions;
f. ensure that the Services or Experian Data are not resupplied, resold, or repackaged;

g. protect the Services from unauthorised access, use, modification, reproduction, publication, or distribution, including through reverse engineering, automated tools or processes, or harmful code;
h. restrict access to the Services to you and your Authorised Users only; and
i. if you use any third-party systems, platforms or service providers in connection with your use of the Services, ensure that those third-party service providers comply with the obligations under this clause 3.1.

Unless required by Law, you must not voluntarily produce any Experian Data in legal proceedings or identify us, our Related Bodies Corporate, the Services, or our Confidential Information as a source of reference.

3.2 Use of AI Technology

a. You must not use (or allow any third party to use) Experian Data to develop, improve, train, validate, or benchmark any artificial intelligence, machine learning or similar technologies, systems or agents (**AI Technologies**). Any technology, information, data or materials created using Experian Data in a way that does not comply with this clause are owned by us, treated as our Confidential Information, and you assign all IP Rights in them to us.
b. For clarity, you may use Experian Data in AI Technologies solely to produce individual results within the Authorised Use, provided that no Experian Data (including any subset or derived data) is retained by any third party (including AI Technology providers).

3.3 You are responsible for Authorised Users

a. If Authorised Users access the Services, you:
   i. must maintain a list of Authorised Users and share it with us on request;
   ii. must ensure that your Authorised Users comply with the Agreement and our reasonable directions to use the Services;
   iii. are responsible for your Authorised Users' use of the Services; and
   iv. acknowledge that we may disable Authorised Users that are deemed inactive or we reasonably suspect have breached the Agreement.
b. If an Authorised User no longer needs access to the Services, you must remove their access. Anyone with access will be considered authorised by you.
c. We may monitor your Authorised Users use of the Service to ensure your compliance with the Agreement, our security standards and to prevent fraud and unauthorised use. You are responsible for obtaining any necessary consents from your Personnel and Authorised Users in relation to this clause.

3.4 You are responsible for how you use the Services

The Services aren't designed or intended to be relied upon as the sole basis for any business decision. You are solely responsible for any decisions made (or not made) by you or your Authorised Users in relation to the use of the Services.

3.5 The way we provide the Services

You acknowledge that we:

a. do not determine your purpose for requesting CDR Data of the End User;
b. rely on your instructions and representations regarding your compliance with these terms and any applicable Laws, and that these terms are reasonably necessary to enable us to comply with the CDR Laws and to maintain our accreditation; and
c. we will attempt to collect End User data using CDR Services, but;
   i. if the CDR Service cannot be completed because the End User consent is not obtained or a CDR open banking connection is unsuccessful; then
   ii. we will attempt to collect the relevant data using our digital data capture (**DDC**) service, provided you have access to the DDC service, the applicable financial institution is available, and the End User gives consent. The terms applicable to that DDC service will apply.

3.6 End User Authorisation

a. You must only use and disclose CDR Data provided to you for the purposes expressly authorised by the End User (**Authorised Use**).
b. You must obtain and maintain all necessary consents and provide all notices which are necessary for your use and disclosure of any CDR Data that we provide to you.
c. The End User authorise us to provide the relevant Service on a one-off basis or on an ongoing basis for a defined period. We will only provide CDR Data to you in accordance with the End User's consent or authorisation from time to time and the CDR Laws.

d. If the End User asks you to change or withdraw a consent managed by us, or requests that the shared CDR Data no longer be used, or you no longer require an ongoing consent to provide your services to an End User, you must:
   i. direct the End User to their consumer dashboard or other method we specify for the End User to make that change;
   ii. not represent to the End User that you can make the change on our behalf;
   iii. stop requesting the CDR Data from us and terminate the relevant data request arrangement; and
   iv. cease or restrict, and ensure your authorised recipients cease or restrict, further use and disclosure of the affected CDR Data as required by Law.

   You must notify us (within one Business Day) if the End User insists that you pass the request to us, or the request is in connection with fraud, or threat of physical or mental harm, or misuse of CDR Data, or makes a complaint about us, the Services or a consent managed by us. Your notice does not, by itself, establish that the consent has been changed or withdrawn.

e. We may use and disclose de-identified CDR Data to our Related Bodies Corporate for the improvement of products and services if the End User gives consent.

3.7 Your use of the CDR Data

a. You are solely responsible for:
   i. the lawfulness of each data request; and
   ii. your collection, use, storage, disclosure and handling of any CDR Data received through the Services, including compliance with all applicable Laws.

b. You must comply with any reasonable direction we give in relation to an End User authorisation including ceasing to access or use affected CDR Data.

c. You must not make any representations on our behalf without our prior written consent.

d. You must notify us promptly (within one Business Day) and keep us updated:
   i. if you receive any complaints in relation to the Service or CDR Data from any Regulator, End User or third parties. To the extent permitted by Law, you must not respond to any complaints without first consulting with us and must cooperate with us to resolve the complaint; and
   ii. of any matter that could reasonably be expected to affect our compliance with the CDR Laws or our accreditation.

e. You agree to provide us with all reasonable assistance and information if a Regulator, End User or a third party makes an inquiry or complaint about the Services.

4 How do we manage intellectual property?

4.1 Ownership and licensing of Existing IP

You and we each own and continue to own all of our respective Existing IP. If any of your Existing IP forms part of any of our Services, you grant us a non-exclusive, perpetual, irrevocable, royalty-free licence to use and modify that Existing IP to the extent required to deliver the Experian Services.

4.2 We don’t transfer any IP Rights in the Services

We retain (and don’t, at any time, transfer) any ownership rights, including IP Rights, in the Services and we reserve all rights not expressly granted.

4.3 IP created during Service provision

All right, title and interest, including IP Rights, in any Enhancements or Joint IP vests in us on creation. If you acquire any IP Rights in any of our Services, Enhancements, or Joint IP, you:

a. assign those IP Rights to us (or our licensor) with effect from acquisition; and
b. agree to do all things reasonably required by us to give effect to such assignment.

4.4 We may use your IP

To the extent required to provide the Services, you grant us a non-exclusive, non-transferable, royalty-free licence to use your IP Rights for the Service Term for the exclusive purpose of providing the Services and to integrate your trade names, trademarks or other intellectual property into any software interface.

5 Additional CDR Services general terms

5.1 We may immediately suspend or stop providing CDR Data to you (without liability to you) if an End User's consent expires, is withdrawn or we reasonably believe it may no longer be valid, or is necessary to comply with Law, our accreditation conditions or a Regulator's direction.

5.2 We may (acting reasonably) immediately suspend or terminate the Services (in whole or in part) by notice to you if we reasonably believe that the continued provision of the Services would cause or result in us or any of our Related Bodies Corporate breaching the CDR Laws or any conditions of our accreditation.

Part 2 – Service-specific terms

Each set of service-specific terms applies only to the Services described in each section below.

6 Experian as Accredited Data Recipient terms

6.1 When this section applies

This section applies when the Location is Australia and we act in our capacity as an Accredited Data Recipient, for purposes of providing the following CDR Services: Insights, Business Disclosure, Categorisation and/or Experian Open Data Suite.

6.2 Our obligations

a. We will act in our capacity as an Accredited Data Recipient in providing the Services, including the collection of End User consent.

b. We will only provide the Services to you on the condition that you are not a CDR Representative.

c. We will collect, use, and disclose CDR Data of the End User in accordance with the consent provided by the End User and the CDR Laws, including disclosing it to the specified recipient nominated by the End User.

d. Any CDR Data that we collect will be handled in accordance with the Experian Australia CDR Policy available at https://www.experian.com.au/privacy-policy-terms-conditions.

6.3 Experian Open Data Suite

This clause 6.3 applies only to Experian Open Data Suite.

a. We will obtain the End User's consent to collect and use the End User's CDR Data, and disclose the End User's CDR Data to the End User, only and for the purpose of providing the Experian Open Data Suite Service to the End User.

b. Following our disclosure of the CDR Data to the End User, we may provide functionality allowing the End User to choose whether to further share their own CDR Data with you.

c. If the End User independently elects to share their CDR Data with you using the Experian Open Data Suite functionality, we will facilitate the End User's sending of their CDR Data to you to the extent requested by the End User. We do not guarantee that any End User will elect to share their CDR Data with you.

d. You acknowledge that:

- **i.** any CDR Data you receive through the Experian Open Data Suite functionality is disclosed to you by the End User, and not by us (including in our capacity as an Accredited Data Recipient); and
- **ii.** you are solely responsible for the collection and any subsequent handling of CDR Data you receive through the Experian Open Data Suite functionality (including for the purposes of complying with all applicable Laws).

e. The End User may amend or cease their election to share their CDR Data at any time in accordance with the Experian Open Data Suite functionality and applicable CDR Laws.

f. We may cease facilitating any sharing of CDR Data through the Experian Open Data Suite functionality, including where the applicable consent or authorisation expires, is withdrawn, the defined sharing period ends, we reasonably consider continued sharing would breach the CDR Laws, or if we decide to no longer offer the Experian Open Data Suite functionality or we need to make changes to it.

g. We are not appointed as your agent in relation to the Experian Open Data Suite Service.

7 Experian as Accredited Requestor service terms

7.1 When this section applies

This section applies when the Location is New Zealand and we act in our capacity as an Accredited Requestor for the purpose of providing the CDR Services.

7.2 Our obligations

a. We will act as an intermediary for data services under the CDR Laws.
b. We will collect, use, and disclose CDR Data of the End User in accordance with the consent or authorisation provided by the End User and the CDR Laws.
c. Any CDR Data that we collect will be handled in accordance with the Experian New Zealand CDR Policy available at https://www.experian.co.nz/privacy-policy.

7.3 Information security

You must:

a. implement and maintain appropriate technical and organisational measures to protect CDR Data against unauthorised access, use, disclosure, alteration, loss or destruction;
b. ensure that access to CDR Data is limited to Personnel who require access for the Authorised Use and who are subject to appropriate confidentiality obligations;
c. maintain security controls that are appropriate having regard to the nature, sensitivity and volume of the CDR Data and the risks arising from its processing;
d. maintain complete and accurate records of security incidents affecting CDR Data;
e. promptly notify us (and in any event within 48 hours) of any actual or suspected security incident affecting CDR Data or any incident that could reasonably be expected to affect our compliance with the CDR Laws;
f. promptly investigate, mitigate and remediate any such incident and reasonably cooperate with us in responding to it; and
g. comply with any reasonable information security directions we give where reasonably necessary to enable us to comply with the CDR Laws.

7.4 Your obligations

a. You must comply and must ensure any third parties that you have authorised to receive or use the CDR Data comply, with the Authorised Use and the applicable Laws including the Privacy Laws.
b. You must perform your obligations under this Agreement in a manner that enables us to comply with the CDR Laws (including to maintain our accreditation) and must not do or omit to do anything that causes or contributes to our breach of the CDR Laws or any conditions of our accreditation.
c. You agree that in requesting the collection of CDR Data of an End User from us:
    i. you confirm that you are not an Accredited Requestor;
    ii. you have a contract under which you provide goods or services to that End User; and
    iii. our provision of the CDR Data of that End User to you is reasonably necessary to enable you to provide those goods or services to the End User.
d. You must not subcontract any part of your obligations without our prior written consent.
e. You must implement and maintain reasonable policies, procedures and controls to identify, prevent, detect and respond to fraud and deception risks associated with your use of the Services and the CDR Data, and must promptly notify us of any actual or suspected fraudulent or deceptive activity.
f. You must not use or permit any third party to use the CDR Data for direct marketing or promotional purposes without our prior written consent.

7.5 You indemnify us

You indemnify us and our Related Bodies Corporate against all Loss suffered or incurred, arising out of or in connection with:

a. your breach of clauses 3.6(d) 7.3, 7.4(a) and 7.4(e);
b. any act or omission of a third party authorised by you to receive or use CDR Data, that would, if done or omitted by you, constitute a breach of clause 7.4(a); and
c. any Claim, investigation, inquiry, audit, complaint or regulatory action arising out of or in connection with any of the foregoing.

Clauses 9.1 and 9.2 of the General Terms do not apply to this clause.

8 Transaction Risk Score service terms

8.1 When this section applies

This section only applies to our Transaction Risk Score Service where the Location is New Zealand.

8.2 Using the Service

a. You authorise us to act as your agent to collect, hold and use CDR Data on your behalf, for the purpose of providing the Service (and any related Services) to you.

b. We will not use the transaction risk score or any CDR Data for any purpose except to provide the Service (and any related Services) to you.

c. We may suspend, amend or terminate the Service immediately on written notice if we reasonably consider it necessary to comply with applicable Law or directions or guidance from a Regulator.