CDR Representative Provisions

Last Updated: 18 November 2026

See What's Changed

This Schedule sets out the terms on which Biza, as an Accredited Data Recipient, appoints the Client as its CDR Representative to use Open Gateway. It applies whether the Client buys Open Gateway under the Master Services Agreement, through a Statement of Work, or under the Consolidated Services Agreement, through an Order Form.

1. Definitions and application

1.1 This Schedule applies when the Client's Applicable Agreement provides for the Client to act as Biza's CDR Representative for one or more Client Software Products. It forms part of that Applicable Agreement. If this Schedule is inconsistent with the Applicable Agreement, the order of precedence set out in the Applicable Agreement applies.

1.2 Terms defined in the Applicable Agreement have the same meaning in this Schedule. The following definitions also apply:

Applicable Agreement
: means either the Master Services Agreement between Biza and the Client together with the Statement of Work or other ordering document that provides for the CDR Representative arrangement, or the Consolidated Services Agreement together with the Order Form that selects the CDR Representative option.

Applicable Laws
: means all laws and regulations that apply to the provision of the OG Services, including the CDR Legislation and the CDR Rules.

Appointment
: has the meaning given in clause 1.3.

Biza CDR Policy
: means the Consumer Data Right Policy published by Biza.

CASASAA
: means the CDR Accreditation Sponsored Accreditation Self-Assessment and Attestation form, as updated from time to time and available from https://www.cdr.gov.au/resources/forms-and-templates.

CDR Legislation
: means Part IVD of the *Competition and Consumer Act 2010* (Cth) and any regulations made under it.

CDR Privacy Safeguards
: means the privacy safeguards in Division 5 of Part IVD of the *Competition and Consumer Act 2010* (Cth).

CDR Regulator
: means a regulator of the Consumer Data Right, including the ACCC and the Office of the Australian Information Commissioner.

CDR Representative
: has the meaning given in the CDR Rules.

CDR Requirements
: means the requirements of the Consumer Data Right that apply to the Client from time to time, including under the CDR Legislation, the CDR Rules and the Data Standards, as introduced or amended from

time to time.

CDR Rules
means the *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth), as amended from time to time.

Client Software Product
means each software product of the Client, as identified on the CDR Register, for which the Applicable Agreement provides the CDR Representative arrangement.

Data Standards
means the consumer data standards made for the purposes of the Consumer Data Right and published at consumerdatastandards.gov.au, as amended from time to time.

DR+ Sharing Arrangement V1 and **DR+ Sharing Arrangement V2**
have the meanings given in the table in clause 3.1.

DSB Implementation Guidance
means the Data Standards Body's implementation guidance, as published at https://consumerdatastandardsaustralia.github.io.

Government Agency
means any government, or any governmental, semi-governmental or judicial entity or authority, other than a CDR Regulator.

OAIC Privacy Safeguard Guidelines
means the CDR Privacy Safeguard Guidelines for the Consumer Data Right published by the Office of the Australian Information Commissioner at https://www.oaic.gov.au/consumer-data-right.

OG Services
means Open Gateway and the services that Biza provides with it under the Applicable Agreement, used by the Client as Biza's CDR Representative.

Register of Accredited Persons
has the meaning given in rule 1.7 of the CDR Rules.

1.3 Biza, as CDR representative principal, appoints the Client to act as its CDR Representative for each Client Software Product (**Appointment**), and the Client accepts the Appointment. The Appointment is exclusive to Biza, and the Client must not be appointed as a CDR Representative of, or enter into any similar arrangement with, any other Accredited Data Recipient.

1.4 As CDR representative principal, Biza will:

(a) facilitate the secure and compliant execution of the consent types permitted in clause 3.4, as defined by the CDR Rules;

(b) provide access to permitted CDR Data on behalf of the Client;

(c) ensure that all CDR Data retrieval occurs in compliance with the CDR Rules;

(d) provide reasonable support and guidance to the Client to help it meet its CDR obligations and industry best practice; and

(e) cooperate with the Client in any regulatory audit or inquiry related to the OG Services.

2. Performance as CDR Representative

2.1 Without limiting its other obligations in this Schedule, the Client must take the steps in Schedule 2 of the CDR Rules to protect the CDR Data as if it were the CDR representative principal, including:

(a) establishing a formal governance framework for managing information security risks related to CDR Data;

(b) having and maintaining an information security capability;

(c) establishing and implementing a testing program to review and assess the effectiveness of that information security capability; and

(d) having procedures and practices in place to detect, record and respond to information security events as soon as practicable.

2.2 The Appointment does not give the Client any express, implied or other authority to act in any capacity for Biza, other than as expressly set out in the Applicable Agreement.

2.3 In performing as a CDR Representative, the Client must:

(a) act as a CDR Representative in good faith and with all reasonable care and skill;

(b) comply with Biza's reasonable written directions, instructions, codes, manuals, policies and procedures, including the Biza CDR Policy;

(c) comply, and ensure its personnel comply, with all Applicable Laws, including the CDR Rules;

(d) ensure that its representatives are appropriately trained to deliver the OG Services, and comply with Biza's directions at all times;

(e) ensure that its end-user agreements and related policies are aligned with the Biza CDR Policy and meet the requirements of the Applicable Laws;

(f) not delegate, subcontract or outsource any of its duties or authority under the Applicable Agreement to any other person without Biza's prior written consent;

(g) not engage in any CDR outsourcing arrangement, as defined in rule 1.10 of the CDR Rules;

(h) at Biza's request, assist Biza to comply with the Applicable Laws, including the CDR Rules, and with any act that Biza is compelled by law, by a court or by a CDR Regulator to perform;

(i) cooperate with Biza's monitoring and reporting activities, as required under the CDR Rules or requested by a CDR Regulator;

(j) comply with Division 4.3A of the CDR Rules as it applies to CDR Representatives; and

(k) notify Biza immediately on becoming aware of any breach of this Schedule or of any Applicable Law.

2.4 In managing data as a CDR Representative, the Client must:

(a) comply with the CDR Privacy Safeguards, including Privacy Safeguards 2, 4, 8, 9, 11, 12 and 13 (anonymity and pseudonymity, unsolicited data, overseas disclosure, government identifiers, quality of data, security of data and redundant data, and correction of data);

(b) comply with any direction from Biza to return to Biza, or delete, redundant data as identified under Privacy Safeguard 12, together with any data derived from it, and notify Biza of the deletion;

(c) not use, access, store or disclose the CDR Data other than in accordance with the CDR Rules, and for no purpose other than providing the OG Services; and

(d) provide the OG Services as Biza's CDR Representative only with the relevant CDR Consumer's explicit and informed consent, and in accordance with the CDR Requirements.

3. Supported action, consent and operating mode types

3.1 In addition to the CDR Rules, the DSB Implementation Guidance, the CDR Requirements and the OAIC Privacy Safeguard Guidelines, this clause 3 uses the following references:

Name	Description	Detailed information
DR+ Sharing Arrangement V1	A like-for-like technical specification reproducing a CDR Arrangement.	DataRight+ Sharing Arrangement V1

Name	Description	Detailed information
DR+ Sharing Arrangement V2	An extended version of DR+ Sharing Arrangement V1 enabling consent status polling.	DataRight+ Sharing Arrangement V2

3.2 The following action types are supported under the Applicable Agreement:

Action type	Primary references	Supported
CDR Arrangement	CDR Rules; DSB Implementation Guidance; OAIC Privacy Safeguard Guidelines	Yes
DR+ Sharing Arrangement	CDR Rules; DSB Implementation Guidance; OAIC Privacy Safeguard Guidelines; DR+ Sharing Arrangement V1; DR+ Sharing Arrangement V2	Yes

3.3 For the avoidance of doubt, the Client must ensure that any CDR Requirements reasonably expected to be delivered while executing an action type are delivered, in compliance with the CDR Rules, the OAIC Privacy Safeguard Guidelines and the DSB Implementation Guidance.

3.4 The following consent types are permitted under the Applicable Agreement:

Consent	Operating mode	Primary references	Permitted
Collection	Unrestricted Recipient; Representative; By Sponsor; By Affiliate	CDR Rules 1.10A(1)(a); CDR Rules 4.3	Yes
Amendment	Unrestricted Recipient; Representative; Holder; By Sponsor; By Affiliate	CDR Rules 4.3	Yes
Use	Unrestricted Recipient; Representative	CDR Rules 1.10A(1)(b)	Yes
Holder Disclosure; TA Disclosure	Holder	CDR Rules 1.10A(1)(c); CDR Rules 1.13; CDR Rules 4.2.3	No
Direct Marketing	Unrestricted Recipient; Representative	CDR Rules 1.10A(1)(d)	No
De-Identification	Unrestricted Recipient; Representative	CDR Rules 1.10A(1)(e)	No
Insight Disclosure	Unrestricted Recipient	CDR Rules 1.10A(3)	No
Business Consumer Disclosure	Unrestricted Recipient; Representative	CDR Rules 1.10A(11)	No

3.5 For the avoidance of doubt, the Client must ensure that any CDR Requirements reasonably expected to be delivered while executing a consent type are delivered, in compliance with the CDR Rules, the OAIC Privacy Safeguard Guidelines and the DSB Implementation Guidance.

3.6 The following operating models are permitted, or not, under the Applicable Agreement:

Operating model	Primary references	Permitted
CDR Representative	CDR Rules 1.10AA; CDR Rules Part 4, Division 4.3A; CDR Rules Parts 5 to 7	Yes
Unrestricted Recipient; CDR Principal; Sponsor	CDR Rules Part 4, Division 4.2; CDR Rules Part 4, Division 4.3A; CDR Rules Parts 5 to 7	No
Affiliate	CDR Rules Part 4, Division 4.3A; CDR Rules Parts 5 to 7	No

Operating model	Primary references	Permitted
Holder	CDR Rules Part 4, Division 4.4	No

3.7 For the avoidance of doubt, the Client must ensure that any CDR Requirements reasonably expected to be delivered within the context of its operating model are delivered, in compliance with the CDR Rules, the OAIC Privacy Safeguard Guidelines and the DSB Implementation Guidance.

4. Security obligations

Security practices

4.1 Biza and the Client will each comply with the information security and privacy standards appropriate for handling confidential information.

4.2 Biza will maintain its certification to, and materially adhere to, ISO/IEC 27001:2022.

4.3 Biza will document, and the Client will attest to the completion, validation and verification of, the CASASAA form provided by the CDR Regulator.

4.4 Biza will document, maintain and follow industry best practice for security incident notification and response plans.

4.5 Biza and the Client will each, at their own expense, conduct comprehensive background checks on all employees and contractors who have access to, and make decisions on the handling of, CDR Data. A person whose check results do not meet the fit and proper person requirements for CDR delivery must not perform material aspects of the OG Services.

4.6 Biza will comply with the Information Security Requirements.

Security reviews by Biza

4.7 At least annually, Biza and one or more independent and appropriately qualified organisations will audit the services used to deliver the OG Services.

4.8 On request, Biza will give the Client a summary of the results of Biza's independent security audits (ISO/IEC 27001, SOC 2 Type 2 or equivalent), as they relate to the OG Services.

Security reviews by the Client

4.9 No more than once a year, Biza will permit the Client to:

(a) conduct an on-site security audit, at mutually agreed times of day; and

(b) review relevant information about Biza's security architecture, systems and procedures.

4.10 Biza will remediate any identified and mutually agreed material deficiency within a reasonable period, not exceeding 20 Business Days.

Client security obligations

4.11 The Client will notify Biza of any material security breach of the Client within 24 hours of discovering it.

4.12 The Client will cooperate with Biza during the investigation of a security breach. It will provide access to the information Biza requires, and make its personnel available to the extent necessary, to help Biza determine any impact on Biza.

4.13 Biza may suspend the OG Services on written notice to the Client in the event of a security breach, until Biza has determined that the incident does not pose a security or reputational risk to Biza.

4.14 If Biza asks, the Client will provide:

(a) a summary of any security audit report by an independent organisation, detailing the scope and results of the assessment; and

(b) a letter on the Client's letterhead, signed by a duly authorised officer, asserting the Client's ongoing compliance with the security requirements of the CDR Rules and this Schedule.

5. Ecosystem registration

5.1 Biza and the Client will take all steps reasonably necessary for the Appointment to take effect, including submitting registration information to the CDR Regulator and to the Register of Accredited Persons.

5.2 The Client will bear any costs directly associated with making applications and giving notifications to the CDR Regulator under this Schedule and, when Biza asks, will reimburse Biza for any reasonable costs Biza incurs in making any such application or notification.

6. Records and reporting

6.1 For as long as it operates as Biza's CDR Representative, including any later term, and after the Appointment ends, the Client will keep all accounts, books, records and data relating to the Client, its CDR Consumers and the OG Services that may reasonably be required for it to meet its obligations as a CDR Representative.

6.2 The Client agrees that Biza, and any other person Biza nominates from time to time (including a CDR Regulator or Government Agency), may request access to all relevant information and records held by or under the control of the Client, and the Client will provide copies of those records.

6.3 When Biza reasonably asks, the Client will provide a report for each reporting period required by the CDR Rules, including details of CDR complaints, the services the Client offers as part of the OG Services, and any material changes made to the OG Services.

6.4 The Client will give representatives or appointees of a CDR Regulator or Government Agency access to, and if requested copies of, relevant records, files, tapes or computer systems in its possession or control that relate to the OG Services, as reasonably requested.

6.5 Each party is responsible for its own costs of regulatory audits, including preparing and submitting audit materials and compliance documentation, and auditor fees. When either party is notified of a regulatory audit, it will promptly tell the other party of the audit's scope, timing and requirements. Both parties will cooperate fully with each other and with the regulatory authorities during the audit.

7. Complaints

7.1 The Client will refer any complaint it receives about the OG Services immediately to Biza, for Biza to handle in accordance with the Applicable Laws.

7.2 The Client will give Biza any assistance needed to resolve the complaint, but will take no further action on it unless Biza expressly asks it to.

7.3 The Client will keep a record of every complaint it receives, in a readily identifiable form, for 3 years from the date it receives the complaint.

7.4 If the Client and Biza agree that the Client will manage complaints, the Client will manage them in accordance with Biza's directions and at all times in accordance with the Applicable Laws, including the CDR Rules.

8. Access

8.1 During the Applicable Agreement and for up to 7 years after it ends, the Client will:

(a) permit Biza and its representatives, at reasonable times and on reasonable prior notice, to access, inspect and take copies of the documents, books and accounts described in clause 6; and

(b) use reasonable endeavours to assist with any request by Biza to conduct interviews, investigations and audits directly with the Client (and with related parties, as the Client and Biza agree, acting reasonably), as Biza considers reasonably necessary to discharge its duties under the Applicable Laws.

8.2 During the Applicable Agreement and for up to 7 years after it ends, a CDR Regulator or Government Agency is entitled to access the Client's business premises, with or without notice, during normal business hours, to help it discharge its legal functions. The Client will, where applicable, make itself and each of its officers and employees readily available for meetings with representatives or appointees of the CDR Regulator or Government Agency, as reasonably requested.

9. Communication

9.1 The Client must immediately notify Biza in writing of any matter that affects, or could affect, its ability to act as a CDR Representative, any change in information about the Client given to Biza or the CDR Regulator, and any change in circumstances of which Biza should reasonably be made aware.

9.2 The Client must immediately notify Biza in writing of the ACCC's decision to include the Client, as Biza's CDR Representative, in the Register of Accredited Persons.

9.3 In delivering the OG Services, the Client must describe itself as a CDR Representative of Biza in all promotional material, on its website and in any dealings with CDR Consumers about the OG Services.

9.4 The Client must immediately notify Biza if a CDR Regulator or Government Agency contacts it about the Appointment or this Schedule, and must seek Biza's approval of, and reasonable input into, any communication between the Client and that CDR Regulator or Government Agency.

10. Termination

10.1 The Appointment ends automatically if:

(a) the Applicable Agreement, or the CDR Representative arrangement under it, ends or expires;

(b) Biza ceases to be permitted by the CDR Regulator to act as a CDR representative principal;

(c) the CDR Regulator directs Biza to stop providing the CDR Representative arrangement to the Client;

(d) Biza's accreditation, or any other authorisation or permission it needs, is cancelled or suspended; or

(e) Biza becomes subject to additional conditions or limitations on providing the CDR Representative arrangement, including any restriction on its ability to provide it.

10.2 Biza may end the Appointment by written notice, with effect on the date of the notice, if:

(a) it has reasonable grounds to believe that the Client has breached, or is likely to breach, any Applicable Law, including the CDR Rules; or

(b) the Client commits a material breach of the Applicable Agreement that cannot be remedied, or is not remedied within the period the Applicable Agreement allows for remedy.

10.3 Ending the Appointment may include the immediate cessation of all CDR services provided under the CDR Representative arrangement.

10.4 When the Appointment ends, the Client must immediately:

(a) stop delivering the OG Services using services provided by Biza;

(b) stop holding itself out as a CDR Representative of Biza;

(c) stop using and distributing promotional material about the OG Services;

(d) on Biza's request, provide all records kept under clause 6;

(e) cooperate as necessary so that Biza can tell CDR Consumers that the Client no longer acts as Biza's CDR Representative to deliver the OG Services;

(f) continue to meet its obligations to CDR Consumers, regulatory or otherwise, including for circumstances that arose before the Appointment ended;

(g) pay Biza all amounts due under the Applicable Agreement; and

(h) return or destroy all confidential information, subject to any retention the law requires and to copies made by automatic computer backup as part of the Client's normal archiving.

10.5 Clauses 6, 8 and 10.4 survive the end of the Appointment.