Data Standards Body

Technical Working Group

Decision Proposal 225: Data Recipient Security Standards

Contact: Mark Verstege
Publish Date: November 16th 2021
Feedback Conclusion Date: February 18th 2022

Context

The recent release of the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021* introduced amendments that:

(a) increased the ways businesses can participate in the CDR and the range of services by which consumers can derive benefit from their data through new access pathways including: trusted advisers, representatives and sponsored affiliates.
(b) permitted, or where necessary, made clear, that the Data Standards Chair may seek to define data standards in relation to the disclosure of CDR data including by data recipients.
- Repeals 4.10(2)
- Includes a substituted 7.5(2)

Whilst data standards are defined for the secure transfer of data between data holders and the primary collecting data recipient, to-date, the data standards have not defined standards for the secure transfer of CDR data beyond the primary data recipient. With the changes to the rules to permit, where necessary, data standards to be defined in conjunction with the new access arrangements being permitted, the DSB is seeking input whether security standards should be considered for the transfer of CDR data beyond the primary data recipient. And if so, the nature of any possible security data standards.

The rules permit data standards to be made covering matters beyond the primary data recipient in several areas. This includes:

Schedule 2, clause 2.2 (1)(i)

> Encryption in transit
>
> Implement robust network security controls to help protect data in transit, including: encrypting data in transit and authenticating access to data in accordance with the data standards (if any) and industry best practice, implementing processes to audit data access and use, and implementing processes to verify the identity of communications.

Subrule 7.5(2)

However:

(a) a disclosure is not a ***permitted use or disclosure*** unless it is done in accordance with the data standards; and

(b) none of the uses or disclosures of CDR data referred to in subrule 4.12(3) is a ***permitted use or disclosure***.

8.11 Data standards that must be made

(c) the disclosure and security of CDR data, including:

(i) authentication of CDR consumers to a standard which meets, in the opinion of the Chair, best practice security requirements; and

(ii) seeking authorisations to disclose CDR data in response to consumer data requests; and

(iii) consumer experience data standards for disclosure of CDR data to accredited persons; and

(iv) consumer experience data standards for disclosure of CDR data to trusted advisers;

(v) consumer experience data standards for disclosure of CDR insights;

Access arrangements for disclosing CDR data

The CDR allows multiple pathways for organisations to collect and disclose CDR data and insights, with consumer consent. Each of these arrangements has different considerations in relation to secure data transfer and data use.

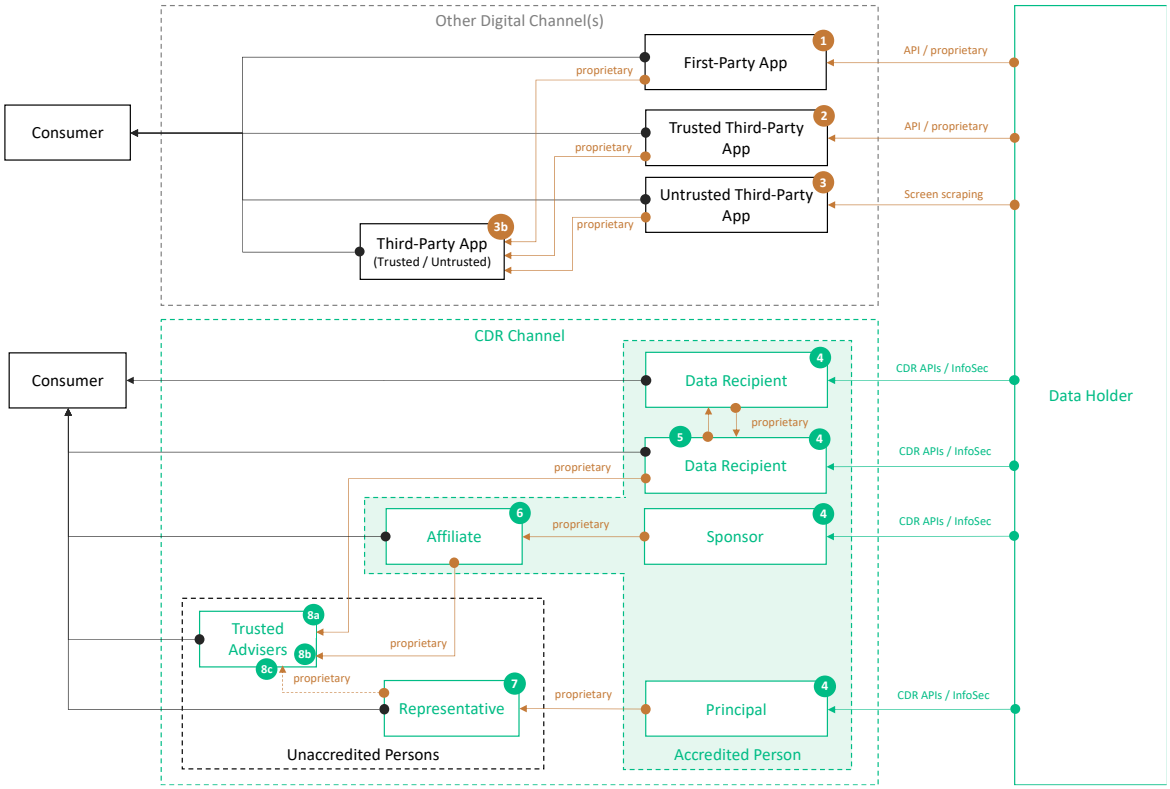

Figure 1: CDR and non-CDR data access pathways

Whilst the CDR defines data recipient access arrangements, in many respects, existing commercial arrangements exist in the market for the transfer of data including data platforms and marketplaces. Where organisations are seeking to expand their data services to the collection and disclosure of CDR data, many may seek to leverage their existing platforms to the extent that is possible or offer a separate standalone solution. For the purposes of this decision proposal the common pathways as well as the CDR access arrangements have been summarised below.

Interface 1 (non-CDR): Data Holder connected to first-party applications
A data-holding organisation connects to its own first-party applications. For example, a bank using REST APIs to connect to its iOS and Android mobile banking apps. Security standards are defined and controlled within a closed wall system defined by the Data Holder.

Interface 2 (non-CDR): Data Holder connected to trusted commercial third-party applications
A data-holding organisation connects to a controlled ecosystem of third-party apps approved by the Data Holder. For example, a bank that offers an app marketplace to use its bank-as-a-service APIs. Security standards are defined and controlled by the Data Holder for approved third-party integrations. They may involve common or bespoke integration solutions.

Interface 3 (non-CDR): Untrusted third-party apps connect to Data Holders using customer credentials
A data-holding organisation is connected to untrusted third-party applications that commonly use customer credentials to connect and scrape customer data. For example, a bank account aggregator or online accounting provider. No formal security standards are defined, and third-party apps impersonate end-users. This permits third-party apps to perform any operations offered to the customer but commonly are limited to screen scraping data such as banking transaction history.

Interface 3b (non-CDR): Connected third-party apps connect to first- and third-party apps
A data-holding organisation is connected to untrusted third-party applications that commonly use customer credentials to connect and scrape customer data. For example, a bank account aggregator or online accounting provider. No formal security standards are defined, and third-party apps impersonate end-users. This permits third-party apps to perform any operations offered to the customer but commonly are limited to screen scraping data such as banking transaction history.

Interface 4 (CDR): ADR collects CDR data from a Data Holder
Accredited data recipients collect data with a consumer's consent from a Data Holder using CDR APIs. Security standards are defined by the Consumer Data Standards.

Security standards already exist.

Interface 5 (CDR): ADR collects CDR data from another ADR
Accredited data recipients collect data with a consumer's consent from another accredited data recipient.

No security-related data standards exist. How data is transferred between the two data recipients is not defined by the consumer data standards and the security requirements of the solution vary depending on the commercial agreement and technical integration between the two recipients.

Interface 6 (CDR): Sponsor and affiliate relationship
The sponsor agrees to disclose to the affiliate, in response to a consumer data request made by the affiliate to the sponsor[1], CDR data that it holds as an accredited data recipient. The affiliate undertakes to provide the sponsor with such information and access to its operations as is needed for the sponsor to fulfil its obligations as a sponsor. The affiliate may also collect data from another accredited person who is not their sponsor, relying on the CDR disclosure rules.

No security-related data standards exist. How data is transferred between the affiliate and their sponsors or disclosing data recipients is not defined by the consumer data standards and the security requirements of the solution vary depending on the sponsor having regard to the liability and accreditation requirements defined in the CDR rules.

Interface 7 (CDR): Unaccredited representative and principal relationship
The CDR representative model enables unaccredited persons to provide goods and services to consumers using CDR data in circumstances where they are in a CDR representative arrangement with an unrestricted accredited person who is liable for them. These relationships may involve a variety of solutions including where data does not leave the systems hosted by the principal ADR.

No security-related data standards exist. How data is transferred between the representative and their principal is not defined by the consumer data standards and the security requirements of the solution vary depending on the technical arrangement with the principal whilst having regard to the liability and accreditation requirements defined in the CDR rules.

Interface 8a/ 8b / 8c (CDR): Trusted advisers
A consumer consents to disclose CDR data or insights to an unaccredited trusted adviser that uses the platform services of an accredited data recipient and is a member of one of the classes listed in r 1.10C (e.g., financial counselling agencies, certain qualified accountants etc. in accordance with a trusted adviser disclosure consent. How the trusted adviser interfaces with the accredited data recipient is not defined by the data standards. This may involve API integrations, but it may also involve delegated use of a data recipient application on behalf of the consumer who is present with the consumer to fulfil a service.

Note (interface 8c): CDR representatives can disclose data to Trusted Advisers. They can also make insight disclosures. Whilst the CDR representative makes these disclosures, in practice it may do so through their principal (the accredited data recipient).

No security-related data standards exist for the disclosure of CDR data and insights to Trusted Advisors.

Data access models

As outlined in the Amendment Rules Explanatory Statement, the arrangements between two commercial parties either in a sponsored representative model or affiliate model may vary in complexity and integration. Potential applications of sponsored accreditation included:

- customer-facing affiliate accesses CDR data through non-customer-facing sponsor

[1] An affiliate cannot make a consumer data request directly to a data holder [Schedule 1, item 8, rule 5.1B(3)]

- affiliate relies on AP disclosures of CDR data
- data enclave
- sponsor provides white-labelled CDR infrastructure services to the affiliate

Unlike the direct API model between the data holder and primary ADR, integrations may be expansions of pre-existing solutions, they may be new API-based integrations, or they may involve, to varying degrees, a data enclave model.

Whilst the CDR introduces a new channel for alternative data access arrangements, many data platforms already exist in the market today with commercial integration solutions. For example, account aggregators offer mechanisms to connect and collect data from banks so third-parties can offer goods and services using the collected data and/ or generated insights.

Accounting platforms collect bank data and offer bespoke integrations and marketplaces for third-party applications to integrate and connect. These may utilise a data enclave of the platform or connect to externally hosted solutions.

Decision to be Made

1. Whether security standards for the transfer and use of CDR data between data recipients including those that are not accredited.
2. Where required, determine what security standards are necessary.

Identified Options

For this decision proposal specific options are not included. Instead, questions are being asked to help frame and direct feedback from the CDR community. Any feedback provided will help inform the need for future standards consultations.

When considering the questions presented below, the DSB is seeking to understand the security and implementation considerations across the myriad of solutions. Imposing standardised integration solutions may provide some advantages for consistency whilst at the same time creating other challenges for existing solutions.

Question 1 – What principles should the Data Standards Chair apply to determine if any security standards should be made for the CDR access arrangements?

- What principles should be applied to whether standards apply and to what extent?
- Do the principles apply equally to all access arrangements, or are they specific to one of the access arrangements?

Question 2 – How should the Data Standards Chair determine whether standards apply to data recipient access arrangements, or not?

- If standards are defined, is this the addition of general requirements or specific security profiles governing the disclosure of data?
- If standards are recommended, do they apply equally to all access arrangements or specifically to one or more access arrangements?

- If standards are recommended, should they be principle-based or provide detailed standards?
- If standards should not apply, why not?
- If alternative channels already exist for data collection (e.g., secure APIs or screen scraping) what reasons are security standards recommended for the CDR channel but not the alternative channels?
- Rather than apply additional security standards within the CDR, should they instead be imposed through adjacent regulations in each sector that apply universal high-grade security consistently across all digital channels for the transfer of data?

Question 3 – If standards are supported, what standards are recommended, and why?

- Should standards exist where data is in transit?
- Should standards exist where data is at rest?
- Should standards exist for how secondary data recipients authenticate with their sponsor or principal?
- Should standards exist for how two data recipients authenticate with one another for disclosure of data?
- Should standards exist for the transfer of consent where a data recipient changes its technical infrastructure or outsourced software provider?
- If standards are recommended, what impact does this have to consumer experience?

Question 4 – What concerns or considerations must be factored into pre-existing commercial data integrations and solutions?

Many access arrangements supported within the CDR replicate existing commercial arrangements for non-CDR data sharing. Defining additional security and technical requirements for pre-existing commercial solutions may therefore impact existing implementations. Are there any considerations in this regard that should be factored into making standards, or alternatively where standards should not be imposed?

Question 5 – Are security considerations limited to any given sector or do they apply to all CDR data?

As the CDR expands across sectors, data recipients will have access to data sets across different sectors. So too, Data Holders may operate in more than one sector (for example an organisation providing banking, wealth and general insurance products).

Question 6 – Should the Data Standards define customer authentication requirements for customers authenticating with accredited persons or with non-accredited persons in a CDR access arrangement?

Whilst consumers must authenticate with their data holders to authorise the disclosure of data to a data recipient, there are no standards pertaining to the authentication of the customer in the data recipient. A digital identity and/ or customer authentication is not a pre-requisite to the use a data recipient goods or service.

Question 7 – If action initiation or payment initiation are introduced into the CDR, does this raise new or additional security considerations for access arrangements?

If action initiation was adopted by Treasury, this may provide alternate pathways for consumers to initiate payments, update their data and accounts, and open new accounts. Considering the potential future enhancements to the CDR, are any additional security measures relevant for data recipients?

Question 8 – Are there any additional implementation or security considerations?

- Do these implementation considerations preclude the making of security standards or do they change or increase build considerations?
- Do these considerations impact reasonable implementation obligation dates?
- If so, where standards are recommended, what obligation dates are considered practical and reasonable?
- What key challenges would introducing security standards present?
- What key risks would introducing security standards mitigate?

Current Recommendation

This decision proposal makes no recommendations. Instead, open feedback is being sought to determine the applicability of standards being defined and where required, recommendations for future targeted consultation.

Implementation Considerations

As no specific changes are being proposed there are no direct implementation considerations that have been identified by the DSB.

Any feedback that the community may have on implementation concerns and issues with timing of implementation of any of the issues raised by this proposal are still welcome.