

Data Standards Body

Consumer Experience Working Group

Decision Proposal 222: Insight and TA Disclosure Consents

Contact: Michael Palmyre

Publish Date: 16 November 2021

Feedback Conclusion Date: 30 November 2021

Context

This decision proposal relates to Consumer Experience (CX) Standards for insight and trusted adviser (TA) disclosure consents. The options in this paper progress from [Noting Paper 207](#) to reflect the [v3 Rules](#), which were made on 30 September 2021.

This paper identifies a range of options for CX standards to support intuitive, informed, and trustworthy data sharing experiences relating to insight and trusted adviser disclosures. DP222 does not contain any recommended options. This initial consultation is being conducted to collect feedback from the community before a subsequent decision proposal is published and consulted on from December 2021 to January 2022, in which the DSB's final recommendations will be proposed. Phasing DP222 consultation in two stages will allow the DSB to iterate on options if required based on community feedback and the findings of CX research currently being conducted.

The options in this paper cover:

- [Insight descriptions](#)
- [Disclosure notifications](#)
- [Existing disclosure consent standards](#)
- [Existing disclosure consent withdrawal standards](#)

As per Rule 7.5A, insight and trusted adviser disclosure consents are not permitted until the earlier of 1 February 2022 or the day the Data Standards Chair makes the standards referred to in 8.11(1A) and 8.11(1)(c)(iv). These standards relate to:

- obtaining authorisations and consents, and withdrawal of authorisations and consents;
- CX standards specifically for insight and TA disclosures;
- specific CX standards for how accredited persons can meet the requirement to make clear what a CDR insight would reveal or describe; and
- specific CX standards to inform consumers that their data will leave the CDR ecosystem when it is disclosed

Rule 7.5A also specifies that an insight disclosure consent is not permitted if the CDR insight includes or reveals sensitive information within the meaning of the Privacy Act 1988.

Rule 1.10A(3) notes that accredited data recipients ('ADRs') are authorised to use insight disclosure consents for one or more of the following purposes:

- verifying a consumer's identity;
- verify a consumer's account balance;
- verifying the details of credits to or debits from the consumer's account;

However, where the CDR data relates to more than one transaction, the ADR must not disclose an amount or date in relation to any individual transaction.

Rule 1.10C outlines that ADRs may invite a CDR consumer to nominate one or more persons as trusted advisers of the CDR consumer. Trusted advisers must belong to one of the following classes:

- qualified accountants within the meaning of the Corporations Act 2001;
- persons who are admitted to the legal profession (however described) and hold a current practising certificate under a law of a State or Territory that regulates the legal profession;
- registered tax agents, BAS agents and tax (financial) advisers within the meaning of the Tax Agent Services Act 2009;
- financial counselling agencies within the meaning of the ASIC Corporations (Financial Counselling Agencies) Instrument 2017/792;
- relevant providers within the meaning of the Corporations Act 2001 other than:
- provisional relevant providers under section 910A of that Act; and (ii) limited-service time-sharing advisers under section 910A of that Act;
- mortgage brokers within the meaning of the National Consumer Credit Protection Act 2009

This proposal seeks to help consumers remain informed about what information they are consenting to be disclosed. This work is guided by the Data Standards Body's [principles](#), particularly the following:

Outcome Principle 3: Data sharing provides a positive consumer experience

The standards will ensure that CDR consumers have simple, informed, and trustworthy data sharing experiences that provide them with positive outcomes over the short and long term.

CX Principle 2: The CDR is Accessible and Inclusive

A diverse range of people are able to access, use, and comprehend the CDR ecosystem regardless of their background, situation, experience, or personal characteristics.

CX Principle 3: The CDR is Comprehensible

When interacting with the CDR, consumers are able to understand the following:

- **who** their data is shared with;
- **what** information is shared;
- **when** sharing begins and ceases;
- **where** data is shared to and from;
- **why** their data is being requested; and
- **how** they can manage and control the sharing and use of their data

CX Principle 4: The CDR is Simple and Empowering

Consumer interactions with the CDR are as simple as possible, but not at the expense of informed consent, consumer control, transparency, privacy, or comprehension. Consumers should be encouraged to be privacy conscious without experiencing cognitive loads that lead to disengagement. Consumers should also be empowered by the CDR without interactive burdens being placed on them.

This decision proposal has been informed by consultation and research conducted in 2020 and 2021, including the following:

1. [Noting Paper 207 consultation](#)
2. [Draft v2 Rules consultation](#) (see concepts [5.1: TA disclosures](#) and [5.2: Insight disclosures](#))
3. [Draft v3 Rules consultation](#)
4. CX research (see [research brief](#) and [summary of preliminary research](#) on draft v2 rules)
5. Consumer Policy Research Centre (CPRC) report: [Vulnerability, capability, opportunity](#)

Decision to be Made

1. Decide requirements for ADRs to make clear what an insight would reveal or describe
2. Decide requirements for ADRs to notify consumers when disclosing data from the CDR environment

Identified Options

The DSB CX Working Group is currently conducting consumer research on insight and TA disclosure consent. This research will test several options outlined in this paper based on the current working hypotheses:

Hypothesis 1

For insight descriptions, if ADRs articulate the below details in relation to insights and data clusters, and data handling statements, then consumers will have the necessary information to provide informed insight disclosure consents:

- **What** the insight will reveal or describe to the non-accredited person ('non-AP'), with a realistic and easy to understand example
- **When** the insight will be generated, and the period the insight will refer to
- **Why** the insight will be generated and disclosed, if known
- **How** the insight will be generated

Hypothesis 2

For disclosure notifications, if ADRs provide the below details when consumers are about to provide an insight or TA disclosure consent, then consumers will be informed about disclosed data risks, controls, and recourse:

- **What** regulations and protections do or do not apply to disclosed data
- **Where** insights can be reviewed and accessed
- **Where** to go for help if there's a problem

For an overview of the research being conducted by the CX working group on insight and TA disclosures, see [Miro](#) | [PDF](#)

Insight Descriptions

This section outlines options for insight description requirements. These proposals seek to support ADRs in meeting the requirement to make clear what an insight would reveal or describe. The options listed in this section are not mutually exclusive. Any supported options will be articulated in the standards in a way that is specific to insight disclosure consents to be applied in the consent process. These options would also apply to insight descriptions in dashboards.

For design illustrations of how and where options 1, 2, 3, and 4 might apply, see [Miro](#) | [PDF](#) (p.6)

Option 1: Insight Example

This option proposes that ADRs provide an easy to understand example that demonstrates what they will reveal or describe to the non-AP using the insight. This example could be used to demonstrate other options in this section.

This option can be articulated in the standards as follows:

ADRs **MUST** provide an easy to understand example that demonstrates what they will reveal or describe to the non-accredited person using the insight. This example **SHOULD** be articulated conversationally and in a way that realistically portrays the specific insight being requested.

Option 2: Time of Insight Generation

This option proposes that ADRs explain the period the insight refers to and when the insight will be generated.

This option can be articulated in the standards as follows:

ADRs **MUST** specify the period the insight will refer to and **SHOULD** note when the insight will or is expected to be generated.

Option 3: Purpose of Insight

This option proposes that ADRs describe the purpose of generating the insight.

This option can be articulated in the standards as follows:

ADRs **SHOULD** explain why the non-accredited person requires the insight.

Option 4: Insight Readability

This option proposes that ADRs achieve a specified readability level when describing insights. A grade 10 readability level is considered appropriate, flexible, and achievable. This is not specified in the proposed standard at this time, and the DSB welcomes feedback on an appropriate grade to specify.

This option can be articulated in the standards as follows:

ADRs **MUST** describe insights in a way that achieves grade **(x)** readability using the Flesch-Kincaid formula or the Automated Readability Index.

Option 5: Actual Insights

This option proposes that ADRs display the actual insight to the consumer prior to disclosing the insight to the non-AP. This will not be workable for certain use cases, such as insight consents with an ongoing duration, or scenarios where the insight cannot be generated until after the consumer has granted consent(s), such as a collection and use consent.

This option can be articulated in the standards as follows:

ADRs **MAY** display the actual insight(s) to the consumer prior to disclosing the insight to a non-accredited person.

Disclosure Notifications

This section outlines options for disclosure notification requirements. The options listed in this section are not mutually exclusive. Any supported options will be articulated in the standards in a way that is specific to the process of seeking consent to disclose data to a non-AP as part of an insight or TA disclosure consent.

For design illustrations of how and where options 1, 2, 3, and 7 might apply, see [Miro](#) | [PDF](#) (p.6)

Option 1: CDR Protections

This option proposes that ADRs specify that non-APs, including TAs, will not be regulated as part of CDR.

This option can be articulated in the standards as follows:

ADRs **MUST** state that data disclosed to non-accredited persons, including trusted advisers, will not be regulated as part of the Consumer Data Right. ADRs **SHOULD** also include information on the Consumer Data Right.

Option 2: Non-AP Handling

This option proposes that ADRs advise consumers to check how non-APs will handle their disclosed data.

This option can be articulated in the standards as follows:

ADRs **MUST** advise the consumer to review how the non-accredited person will handle their data.

Option 3: Non-AP – Known Regulations

This option proposes that ADRs explain what regulations and protections apply to the non-AP's handling of the disclosed data.

This option can be articulated in the standards as follows:

ADRs **SHOULD** state what regulations and protections apply to the non-accredited person's handling of the disclosed data. This **MAY**, for example, provide a link to or summary of the non-accredited person's data handling policy, such as their Privacy Policy.

Option 4: Non-AP – Unknown Regulation

This option proposes that, if the ADR does not know how the non-AP will be regulated, the ADR state that the non-AP may not be subject to the Privacy Act.

This option can be articulated in the standards as follows:

If the ADR does not know how a non-accredited person's handling of disclosed data will be regulated, the ADR **MUST** state that the non-accredited person may not be subject to regulations such as the Privacy Act.

Option 5: Non-AP Data Handling Summary

Option 4 suggests that ADRs explain, in simple and summarised terms, how the non-AP will handle their data.

This option can be articulated in the standards as follows:

If known, ADRs **MAY** provide a simple summary of how a non-accredited person will handle disclosed data. This **MAY**, for example, list key and meaningful elements of a non-accredited person's Privacy Policy.

Option 6: Complaint Handling

This option proposes that ADRs display information on or instructions for how to make a complaint or resolve a dispute, such as through OAIC's [CDR complaints](#) portal.

This option can be articulated in the standards as follows:

ADRs **MUST** provide information on making a complaint and dispute resolution. This **MAY** include a direct link to the [CDR complaints portal](#) or information on how to lodge a complaint with another dispute resolution body.

Option 7: Record Access

This option outlines a proposal for ADRs to explain how a consumer can request further records on insights as per Rules 1.14 and 9.5.

This option can be articulated in the standards as follows:

ADRs **MUST** provide instructions for how the consumer can access records pertaining to insights via their consumer dashboard (as per Rules 1.14 and 9.5).

Option 8: Notification Record

This option proposes that ADRs provide information relating to the disclosure notification requirements otherwise than in the consent flow, such as in the consumer's CDR Receipt and dashboard. Providing this information elsewhere will help consumers retain and access this information if required. The relevant information would depend on the supported options in this section.

This option can be articulated in the standards as follows:

ADRs **MUST** provide the information contained in the disclosure notification otherwise than in the consent flow. This **SHOULD** be contained in the consumer's CDR Receipt. This **SHOULD** also be accessible in the consumer dashboard as part of the data sharing arrangement details.

Existing Disclosure Consent Standards

[Existing CX standards on consent](#) would apply to insight and TA disclosure consents, depending on the scenario. The below standards already apply to AP disclosure consents and were developed in a way that they could apply to disclosure consents regardless of their specific type.

The existing CX standard would support the 'How' attribute in Hypothesis 1:

Disclosure Consent: Collection Source

In the course of seeking a consumer's consent to disclose data as part of a disclosure consent:

1. Data Recipients **MUST** specify which CDR Participant(s) they collected the associated CDR data from
2. Data Recipients **SHOULD** specify the sector(s) the data was collected from or associated with

Note:

- Point (1) only requires the Data Recipient to refer to the CDR Participant(s) immediately preceding them in the disclosure chain, which may not always include a consumer's Data Holder(s)
- This standard is proposed to apply to all data to be disclosed by a Data Recipient, including unmodified, aggregated, derived, and transformed CDR data
- Where applicable, the existing data language standards apply to descriptions of CDR data that have not been modified

This existing CX standard supports insight comprehension. Point 2 would apply to insight and TA disclosure:

Disclosure Consent: Descriptions of Data to be Collected and Disclosed

If:

1. An accredited person is seeking a collection consent to collect CDR data from a particular accredited data recipient; or
2. An accredited data recipient is seeking a disclosure consent from a consumer to disclose CDR data;

and the data subject to the disclosure or collection is not within the data language standards as it does not relate to a relevant data cluster, then that data **MUST** be described in language that is as easy to understand as practicable.

Existing Disclosure Consent Standards: Withdrawal

The [existing withdrawal standards](#) for disclosure consents would apply to insight and TA disclosure consents, specifically the following standard:

Withdrawal: Disclosure Consent

As part of the disclosure consent withdrawal process, Data Recipients **MUST** advise the consumer to review, with the recipient that the data was disclosed to:

1. How their data will be handled; and
2. The consequences of withdrawing the disclosure consent

Note: The precise wording of the withdrawal message is at the discretion of the ADR

Current Recommendation

As noted in the beginning of this paper, this decision proposal makes no recommendations.

This initial consultation is being conducted to collect feedback from the community on the options listed in this paper, and any other identified options, before a subsequent decision proposal is published that indicates the final recommendations to be considered.

For design illustrations of how and where **Insight Descriptions**: Options 1, 2, 3, and 4 might apply, see [Miro](#) | [PDF](#) (p.6)

For design illustrations of how and where **Disclosure Notifications**: Options 1, 2, 3, and 7 might apply, see [Miro](#) | [PDF](#) (p.6)

CX research is currently underway to test several options in this paper. These include options 1, 2, 3, and 4 in the **Insight Descriptions** section, and options 1, 2, 3, and 7 in the **Disclosure Notifications** section. For an overview of the research being conducted by the CX working group on insight and TA disclosures, see [Miro](#) | [PDF](#)

Implementation Considerations

As insight and trusted adviser disclosure consents are not currently permitted in the rules, no existing implementations will be impacted. A follow up DP222 consultation will outline final recommendations in which the DSB will seek views on implementation considerations.

When reviewing this proposal and formulating feedback, please consider the following questions:

1. Which options outlined in this paper do you support?
2. What requirements should be considered to facilitate insight comprehension, such as readability level or details to be included?
3. What requirements should be considered to ensure consumers are informed about the disclosure of their data outside of the CDR environment?
4. What alternative requirements should be considered for insight descriptions and disclosure notifications?