Australian Government
The Treasury

Exposure draft legislation to enable action initiation in the Consumer Data Right

Summary of proposed changes

September 2022

treasury.gov.au

Manager
Media Unit
The Treasury
Langton Crescent
Parkes ACT 2600
Email: media@treasury.gov.au

Contents

Making submissions

Interested parties are invited to comment on this draft legislation.

All information (including name and address details) contained in submissions will be made available to the public on the Treasury website unless you indicate that you would like all or part of your submission to remain in confidence. Automatically generated confidentiality statements in emails do not suffice for this purpose. Respondents who would like part of their submission to remain confidential should provide this information marked as such in a separate attachment.

The consultation period closes on 24 October 2022. Submissions may be sent to data@treasury.gov.au. For accessibility reasons, please submit responses sent via email in a Word or RTF format. An additional PDF version may also be submitted.

Purpose of this paper

This paper sets out a summary of the proposed amendments to the *Competition and Consumer Act 2010* that would expand the Consumer Data Right (CDR) to enable action initiation. It explains how the proposed amendments would build on CDR data-sharing to enable consumers to initiate actions safely and securely in the CDR.

The Government welcomes views on the exposure draft legislation via submissions to inform the final bill.

This document is not a legal description of the bill. Separate explanatory material will be prepared to expand on the information provided in this paper.

Action initiation in the CDR

The *Inquiry into the Future Directions for the Consumer Data Right* recommended strengthening and deepening the CDR's functionality and use through the implementation of third-party action initiation reforms.[1] The proposed bill would enable action initiation in the CDR.

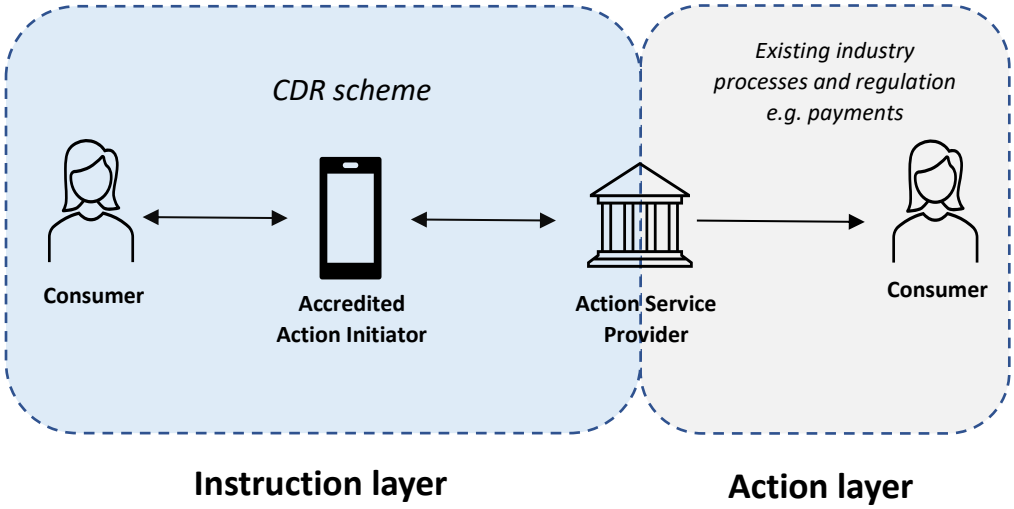
As envisaged by the inquiry, action initiation would create a new channel for consumers to instruct a business to initiate actions on their behalf and with their consent. These actions could include making a payment, opening and closing an account, switching providers and updating personal details (such as address) across providers.

Action initiation would expand the CDR from a data-sharing scheme to a scheme that allows consumers to act on insights they receive. The CDR gives consumers control over their data, helping Australians make better use of their money by making it safe to use transaction data to simplify complex financial decisions and take advantage of data-enabled innovations. Increasing functionality of the scheme to include action initiation would empower consumers to authorise, manage and facilitate actions securely in the digital economy.

Action initiation is made up of two parts: the instruction layer and the action layer. The instruction layer would sit within the CDR scheme and enable a consumer to give consent for a third party, known as an Accredited Action Initiator, to send an action initiation request to an Action Service Provider (refer to 'Key features of the legislation' for an explanation of the different entities). The Action Service Provider would then authenticate the consumer and carry out the action as they would if the request came directly from the consumer. The Action Service Provider would carry out the action in the action layer, which would be outside the scope of the CDR.

1 https://treasury.gov.au/publication/inquiry-future-directions-consumer-data-right-final-report

Figure: Action initiation in the CDR



Some potential use cases indicated by industry include allowing consumers to send instructions to:

- make a payment
- update their contacts details across multiple accounts
- compare electricity tariffs and then switch services, and
- automatically move funds between accounts to optimise interest or minimise fees.

These use cases are an example of how introducing action initiation into the CDR will unlock new business models and drive consumer benefits and digital innovation. There are several key benefits action initiation will bring to the Australian digital economy. They include:

- reducing complexity, time and cost for consumers
- increasing functionality of services
- creating a secure and standardised instruction layer linking to the broader data ecosystem, and
- helping boost competition.

The benefits of action initiation are apparent in the success of payment initiation in the UK's Open banking scheme, which has over 6 million regular active users.[2] There are several other jurisdictions pursuing or considering payment initiation.

2 Open Banking Implementation Entity (OBIE): New Impact Report shows cloud accounting allowing SMEs to run businesses more efficiently. Accessed 16 September 2022.

Proposed legislation

The draft bill establishes the enabling provisions for action initiation, outlines key obligations and safeguards, and provides a pathway to bring individual action types into the CDR (see the following section for key features). The proposed legislation has been designed to work alongside the current data-sharing arrangements in the CDR. To date, data-sharing has been rolled out sector by sector, and is moving towards a more targeted data set approach. It is proposed that action initiation be implemented by action types. The proposed legislation for enabling action initiation in the CDR does not identify action types; this would allow the rules and standards to be tailored to different actions.

Passage of the bill would enable specific actions to be enlivened in the CDR under the following framework.

- Ministerial declaration: it is proposed that the Minister declare new action types in the CDR, similar to the current designation process for data-sharing. The Minister could declare more than one action at the same time. The declaration would specify which data holders would be obliged to accept action instructions in the CDR. Before declaring an action type, there must be a period of public consultation and the Minister would be required to consider the likely effect on:
  - the interests of consumers
  - the efficiency of relevant markets
  - the privacy or confidentiality of information
  - promoting competition
  - promoting data-driven innovation
  - any intellectual property
  - the public interest
  - the regulatory impact of the rules, and
  - any other factors the Minister considers relevant.
- Rules: Following a declaration, the Minister would be able to make rules for an action type, consistent with the current rule-making process for data-sharing. The rules would enliven the obligations for the action type set out in the declaration. The rules could include:
  - obligations on action initiation participants including recordkeeping, reporting and audit requirements
  - criteria for accreditation
  - use of CDR data
  - how instructions are delivered
  - how consent and authorisations will occur
  - application of privacy safeguards
  - rules about consumer complaints, and

- fee charging.

- Data standards and guidelines: The rules would work alongside the data standards prepared by the Data Standards Body. The Office of the Australian Information Commissioner would also prepare and publish guidelines relating to the privacy safeguards.

The proposed legislative framework does not seek to regulate the action layer. The framework would regulate the 'instruction layer', which is made up of the activities associated with consumers sending instructions for the performance of actions.

Key features of the legislation

The proposed legislation contains a number of key features to establish the framework for action initiation in the CDR.

- New entities could initiate and execute action types. The changes would create two new types of CDR entities that have a specific role in action initiation. These are:
  - Accredited Action Initiators, which would be able to instruct an Action Service Provider to carry out actions on behalf of consumers (with consent). An Accredited Action Initiator would be accredited by the Australian Competition and Consumer Commission, and it is proposed that an Accredited Action Initiator would need to be an Accredited Person for data-sharing.
  - Action Service Providers, which would be required to act on a valid instruction received from an Accredited Action Initiator. The declaration process would bring Action Service Providers into the CDR, which would need to be existing Data Holders. Action Service Providers would only be required to execute actions that they complete outside of the CDR. There would be scope for voluntary Action Service Providers to be involved in the CDR subject to approval processes. The criteria for approving voluntary Action Service Providers would be set out in the rules.

- An Action Service Provider must accept valid action requests. Action Service Providers would need to treat a valid action request they receive from Accredited Action Initiators as if it came from the consumer themselves. This does not mean they need to complete every action request, as they could still refuse an action if they would not complete the action outside the CDR. For example, a bank may decline to complete a payment if the consumer is not eligible for the particular transaction or does not have sufficient funds in their account. However, it is proposed that an Action Service Provider cannot discriminate against instructions that came through the CDR, meaning they cannot refuse to act on an instruction because the request came through the CDR framework.

- Accredited Action Initiators must act honestly, efficiently and fairly. The *Inquiry into the Future Directions for the CDR* recommended that an accredited person should be obliged to act efficiently, honestly and fairly in relation to initiating actions.[3] The proposed legislation is consistent with this recommendation. This requirement for Accredited Action Initiators is

3 Recommendation 7.6 of the Inquiry into the Future Directions for the Consumer Data Right Final Report

intended to be closely aligned with the obligation in the Australian financial services licensing regime to act efficiently, honestly and fairly.

- An Action Service Provider cannot charge a CDR premium in the action layer. This would prevent an Action Service Provider charging a consumer additional fees to complete actions just because the request came through the CDR. For example, while a bank would be able to charge a consumer a home loan application fee for a request that came through the CDR, it could not charge a higher fee than what would be applied outside the CDR.
- The rules would determine if an Action Service Provider can charge to receive an instruction. If allowed in the rules, an Action Service Provider would be able to charge an Accredited Action Initiator for receiving an action instruction from an Accredited Action Initiator. The Australian Competition and Consumer Commission would be able to intervene if it considered charges were too high.
- An action could only be initiated with the consent of a consumer. An Accredited Action Initiator would only be able to initiate a CDR action on the consumer's behalf with the consent of that consumer. It is proposed that the rules would outline the specific consent requirements for actions.
- The existing privacy safeguards would be extended to apply to CDR data being shared in action initiation. The 13 existing privacy safeguards would be extended to apply to Accredited Action Initiators, and some privacy safeguards would be extended to apply to Action Service Providers with a focus on the instruction layer to provide protection against CDR specific risks. The appendix includes a detailed explanation of the proposed extension of the privacy safeguards.

Existing provisions to be extended to action initiation

- Protection from liability if certain conditions are met. Participants that act in good faith and comply with CDR laws and rules would be protected from liability. However, the legislation would enable regulations to specify other laws that the liability protection would not apply to. For example, this may include the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*.
- CDR action participants cannot hold out to be accredited if they are not. As is the case in data-sharing in the CDR, a person would have committed an offence if they mislead or deceive a consumer into believing they are an Accredited Person for a CDR action.
- Accredited Action Initiators and Action Service Providers would be liable to a civil penalty for breach of their obligations. A breach of the obligations imposed on Accredited Action Initiators and Action Service Providers by the proposed legislation would make that entity liable to pay a civil penalty which would be imposed by a court.

Appendix: Privacy safeguards

Current arrangements

The security and integrity of the CDR is maintained by 13 privacy safeguards contained in the *Competition and Consumer Act 2010* and supplemented by the rules. These privacy safeguards set out the privacy rights and obligations for users of the scheme, including the requirement for informed consent to collect, disclose hold or use CDR data.

The CDR privacy safeguards build on the Australian Privacy Principles to protect a CDR consumer's privacy. The privacy safeguards relate to CDR data only[4]. The rules cover requests to share data, records of consent, authentication and authorisation.

The Australian Privacy Principles are central to the privacy protection framework in the *Privacy Act 1988*. They aim to protect an individual's privacy and apply to businesses with an annual turnover of more than $3 million (with some exceptions).

Proposed key features of the privacy safeguards for action initiation

The draft legislation proposes amendments to the privacy safeguards to apply them to CDR data that will flow in the instruction layer. Key features of the proposed changes to the privacy safeguards are as follows.

- The privacy safeguards focus on the instruction layer. The proposed amendments to the privacy safeguards aim to manage risks that are specific to the CDR, and the proposed changes would extend them to apply to Action Service Providers, focussed on the instruction layer for action initiation. The proposed amendments recognise that an Action Service Provider would not be receiving data that they do not already receive and handle in the ordinary course of their business. As such, once the data is being held by an Action Service Provider, the Privacy Act would apply (subject to thresholds within that Act) as if they received the data outside of the CDR.
- The privacy safeguards would apply to Accredited Action Initiators. Accredited Action Initiators would be required to be Accredited Persons, so any CDR data they receive would be subject to the privacy safeguards. This means that the safeguards would continue to apply to CDR data regardless of whether they receive CDR data as an Accredited Action Initiator or an Accredited Data Recipient.
- The privacy safeguards are proposed to continue to apply to CDR data. This would mean that data provided to an Accredited Action Initiator outside the CDR would be treated according to the Privacy Act, noting that Accredited Persons are subject to the Australian Privacy Principles under that Act.

4 CDR data is data that is captured in designation instruments made by the Minister under section 56AC of the *Competition and Consumer Act 2010*

- Action Service Providers would be subject to relevant privacy safeguards: Action Service Providers should be able to treat relevant data (including CDR data) received in an action request consistent with their existing governance arrangements, as they can also receive this data if the request came outside the CDR. However, there are instances where some of the privacy safeguards should apply to Action Service Providers. This is to manage risks associated with the flow of CDR data in the instruction layer, and where the risks are specifically attributable to the CDR. Details of applicable privacy safeguards are outlined in the table below.

The table below sets out the proposed application of the privacy safeguards. All of the safeguards are proposed to be extended to apply to Accredited Action Initiators, and some to apply to Action Service Providers, focussed on data shared in the instruction layer. The table provides commentary on the suitability of the privacy safeguards for Action Service Providers.

Table: Proposed application of the privacy safeguards

ADR: *Accredited Data Recipient;* ***DH:*** *Data Holder;* ***AAI:*** *Accredited Action Initiator;* ***ASP:*** *Action Service Provider*

	Privacy safeguard	Currently applies to	Extended to apply to	Commentary on Action Service Providers
1.	Open and transparent management of CDR data	ADR; DH	AAI; ASP	Privacy Safeguard 1 would apply to ASPs consistent with the application to DHs.
2	Anonymity and pseudonymity	ADR	AAI	An ASP would be required to authenticate action types, which would pose challenges if this were to apply to ASPs.
3.	Soliciting CDR data from CDR participants	ADR	AAI; ASP	This would apply to ASPs in the instruction layer, whereby an ASP would not be able to solicit additional CDR data outside the scope of an action type. The rules would specify what data is permitted to be shared with an ASP for different action types.
4.	Dealing with unsolicited CDR data from CDR participants	ADR	AAI; ASP	This would apply to ASPs in the instruction layer, whereby an ASP would be required to destroy CDR data it receives that is outside the scope of an action type. The rules would specify what data is permitted to be shared with an ASP for different action types.
5.	Notifying of the collection of CDR data	ADR	AAI	ASPs would be collecting data they already collect outside the CDR; as such, existing privacy regulation would apply.
6.	Use or disclosure of CDR data by ADRs	ADR	AAI	Privacy Safeguard 10 would apply to ASPs, so it is appropriate this safeguard remains specific to ADRs and AAIs.
7.	Use or disclosure of CDR data for direct marketing by ADRs	ADR	AAI	Applying this safeguard to ASPs may create uncertainty and inconsistencies for ASPs and DHs, as it may be unclear how CDR data should be held if it has been received from an AAI when they already hold identical data.

	Privacy safeguard	Currently applies to	Extended to apply to	Commentary on Action Service Providers
8.	Overseas disclosure of CDR data by ADRs	ADR	AAI	An ASP may be required to send data overseas as part of an action – e.g. an international money transfer. Australian Privacy Principle 8 places conditions on the disclosure of information overseas, which would apply to the vast majority of ASPs in the action layer.
9.	Adoption or disclosure of government related identifiers by ADRs	ADR	AAI	Australian Privacy Principle 9 provides equivalent protection with the exception that disclosure is necessary to identify the identity of an individual, which would apply to the vast majority of ASPs in the action layer.
10.	Notifying of the disclosure of CDR data	ADR; DH	AAI; ASP	If an ASP was required to share CDR data back to the AAI as part of the action request, this should be treated as if a DH shared CDR data with an ADR.
11.	Quality of CDR data that is disclosed under the CDR	ADR;DH	AAI; ASP	AAIs and ASPs may be required to pass on corrected CDR data if it had previously been disclosed as part of an action request.
12.	Security of CDR data and destruction or de-identification of redundant CDR data	ADR	AAI	CDR data held by ASPs would be treated the same way as for DHs to minimise regulatory overlap.
13.	Correction of CDR data that has been disclosed under the CDR	ADR; DH	AAI; ASP	This would apply to ASPs in the same way it currently applies to DHs.

Additional information

The proposed changes to the privacy safeguards aim to create a clear delineation between the regulatory obligations at the instruction layer (which is specific to the CDR), and at the action layer (which is covered by existing privacy regulation). As such, it is proposed that existing privacy regulations continue to apply to Action Service Providers in the action layer. If the privacy safeguards were applied to Action Service Providers in full, there could be duplication with existing regulations that apply to Action Service Providers, including for matters such as the retention and deletion of data and record-keeping requirements. This may create challenges for Action Service Providers to comply with dual regimes. The proposed amendments also aim to provide consumers with consistent rights and protections at the action layer, irrespective of whether they initiated an action themselves or through the CDR.

The Australian Privacy Principles would not apply to Action Service Providers if their turnover is less than $3 million. The proposed framework provides flexibility for the rules to exempt small designated data holders from becoming an Action Service Provider. Conversely, the framework may enable a small business with a turnover of less than $3 million to apply to be a voluntary Action Service

Provider, which may not be subject to the Australian Privacy Principles. Treasury engaged KPMG to prepare a Privacy Impact Assessment to support the design of the proposed changes to the privacy safeguards. In its Privacy Impact Assessment, KPMG acknowledged this risk and recommended the Minister consider the privacy obligations of prospective voluntary Action Service Providers as part of the assessment criteria. The proposed legislation provides flexibility for the rules to include additional requirements.

Treasury welcomes feedback on the proposed application of the privacy safeguards.