Privacy Impact Assessment on the introduction of Action Initiation in the Consumer Data Right

September 2022
This report contains 63 pages

Contents

Notice to Third Parties

This report is solely for the purpose detailed in **Part 1** and **Part 3** of this report and for the Commonwealth Department of the Treasury's information and is not to be used for any purpose not contemplated in the engagement contract. This report has been prepared at the request of the Commonwealth Department of Treasury in accordance with the terms of KPMG's applicable engagement contract. Other than our responsibility to the Commonwealth Department of Treasury, neither KPMG nor any member or employee of KPMG undertakes responsibility arising in any way from reliance placed by a third party on this report. Any reliance placed is that party's sole responsibility. The information contained in this report is of a general nature and is not intended to address the specific circumstances of any individual or entity. Appropriate professional advice should be obtained before acting on this information.

The views and opinions expressed herein are those of the author and do not necessarily represent the views and opinions of KPMG, an Australian partnership and member firm of the KPMG network of independent member firms affiliated with KPMG International.

1 Introduction

1.1 Background and context

1.1.1 KPMG[1] is pleased to provide this Privacy Impact Assessment to inform the drafting of amending legislation to establish Action Initiation in the Consumer Data Right (**CDR**). We appreciate the opportunity to support Treasury in contributing to the expansion of this important data right by undertaking an assessment of the privacy impacts and informing the privacy protections for action initiation.

1.1.2 The CDR was established by the Treasury Laws Amendment (Consumer Data Right) Bill 2019 (**CDR Bill**) inserting Part IVD into the Competition and Consumer Act 2010 (CCA).2 Its object is to enable individual and business consumers in certain (designated) sectors of the economy to control their information by requiring its safe, efficient and convenient disclosure by a data holder to trusted and accredited persons for use, subject to privacy safeguards where that information is identifiable or reasonably identifies the consumer.[3]

1.2 Currently, CDR data is set out in the designation instrument for each sector.[4] For example, the designation instrument for Open Banking specifies the following classes of information as 'CDR data':[5]

(a) information about the consumer or their associate (for example, contact details);

(b) information about the use of a product by a consumer or their associate (for example, transaction data); and

(c) information about a product (for example, terms and conditions).

1.2.1 The security and integrity of 'CDR data' (relating to one or more CDR consumers; either individuals or businesses), underpins the effectiveness of the CDR. Division 5 of Part IVD of the CCA sets out legally binding consumer privacy rights and obligations in the 13 CDR Privacy Safeguards (**Privacy Safeguards**) to protect the privacy or confidentiality of CDR data. These mainly apply to 'accredited persons' to whom consumer data about one or more CDR consumers will be or is disclosed under the Competition and Consumer (Consumer Data Right) Rules (CDR Rules)[6] that are made under Part IVD of the CCA. The CDR Rules cover designated sectors, classes of CDR data and CDR participants. The Australian Information Commissioner has issued Privacy Safeguards Guidelines under s 56EQ(1)(a) of the CCA which are published by the Office of the Australian Information Commissioner (OAIC)[7] (**PS Guidelines**). These explain how the

1 Which includes KPMG Law.
2 Competition and Consumer Act 2010 (legislation.gov.au)
3 See s56AA of the CCA.
4 Section 56AI of the CCA.
5 See: Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019.
6 Current CDR Rules in force: Competition and Consumer (Consumer Data Right) Rules 2020 (legislation.gov.au)
7 Current version: privacy-safeguard-combined-chapters.pdf (oaic.gov.au)

Privacy Safeguards and Australian Privacy Principles (**APPs**) in the *Privacy Act 1988* (Cth) (Privacy Act) will apply.

1.2.2 The statutory framework for the CDR is as follows:

(d) **Primary Legislation:** the CCA establishes the CDR framework and provides key protections in the CDR, including in the sector designation process and the Privacy Safeguards.

(e) **CDR Rules**: the rules outline many of the functional requirements for the CDR. They have been designed so that they will apply economy-wide, but are more flexible than the primary legislation. They can be updated and amended over time to include specific provisions that will apply only to certain classes of product data and consumer data for different designated sectors, having regard to the sector's particular features including to address a new designated sector. Compliance with the CDR Rules by accredited entities is regulated by the ACCC.

(f) **Standards (technical and CX):** these are open Standards that detail common technical specifications that support the CDR, are required to be used by ADRs and DHs (and will include AAIs and ADRs) and allow consumers to use the CDR to access and share their data. The Standards comprise: technical standards (that include security measures) and CX standards (which cover consumer-facing content and interactions including consent management via consumer dashboards and authentication models). The Standards are set by the Data Standards Chair with the assistance of the Data Standards Body (**DSB**). Standards can be amended promptly to resolve technical issues. Community consultation on the development of the Standards also occurs.[8]

1.2.3 The CDR is being implemented across the Australian economy on a sector-by-sector basis through designation instruments. It was initially designated in the Banking sector (Open Banking) and is being implemented in phases. The Energy sector (Energy) is the second sector in which CDR is being implemented followed by the Telecommunications and Non-Bank lending sectors.

1.2.4 Separately, and in parallel to the above, the CDR Rules have undergone a development cycle to expand and increase flexibility for how participants interact with the CDR ecosystem and better enable data sharing use-cases to support positive consumer outcomes.

1.2.5 The Department of the Treasury (**Treasury**) has prepared and commissioned a series of Privacy Impact Assessments (PIAs) on the CDR, sector designations and CDR Rules amendments. Treasury prepared an initial PIA for the CDR and a second version, reflecting feedback, was released in March 2019. A third independent PIA was conducted and released in December 2019. That PIA has been progressively updated to assess the 'version 3' CDR rules (September 2021) and the current 'version 4' CDR Rules (November 2021). In October 2021 a supplementary PIA

8 See: Consumer Data Standards at https://consumerdatastandards.gov.au/.

on the designation of the CDR to the energy sector was published. In November 2021, a PIA for the designation of the CDR to the telecommunications sector was published.

1.2.6 Currently under the CDR:

(a) eligible CDR consumers: can consent to their data being shared with accredited, trusted and/or specified persons for purposes and periods they authorise. This allows them to make more informed decisions about the products and services they use and drives innovation in the data economy across both the designated and other sectors;

(b) a data holder (**DH**): is a business that holds CDR data covered by a sector designation instrument that it must transfer to an accredited data recipient (**ADR**) at the request of an authenticated consumer; and

(c) an ADR: is a business that has been accredited[9] by the Australian Competition and Consumer Commission (**ACCC**) to receive CDR data to provide a product or service to an eligible CDR consumer and must comply with the CDR Rules.

1.3 Action Initiation

1.3.1 On 23 December 2020 the Australian Government published Scott Farrell's final report on the Inquiry into the Future Directions for the CDR (**FD Report**)[10]. The FD Report recommended Action Initiation be implemented in the CDR, with payment initiation as the first action to be included in the CDR. This PIA has been developed in conjunction with Treasury to inform the development of legislation to enable action initiation.

1.3.2 Action Initiation will, in addition to the established data sharing under the CDR, allow write access by creating a new channel for consumers to instruct an accredited entity to initiate actions (such as initiating transactions (payments), closing accounts, obtaining quotes and applying for products) on their behalf, with their consent. It is a significant extension of the CDR.

1.3.3 Implementing Action Initiation requires amendments to the CCA, and the development of new CDR Rules and Consumer Data Standards. Specifically, in relation to consumer privacy protections, amendments may also need to be made to the Privacy Safeguards and related provisions of the CCA.

1.3.4 It is proposed that Action Initiation will also establish **new** types of participants in the CDR:

(a) **Accredited Action Initiator (AAI):** an AAI is an entity that is able to instruct ASPs to carry out actions on behalf of consumers (with valid consent). The CDR Rules would enliven action initiation and set out what data is permitted to be shared as part of an action request. An AAI would be accredited by the ACCC.

9 To obtain accreditation, the prospective ADR must demonstrate they: are a fit and proper person; are able to take the steps required to adequately protect CDR data from misuse, interference, loss, and unauthorised access, modification or disclosure; have internal dispute resolution processes meeting the requirements of the CDR Rules; are a member of a recognised external dispute resolution scheme; have adequate insurance to compensate consumers for any loss that might occur from a breach of their CDR-related obligations, and have an Australian address.
10 Inquiry into Future Directions for the Consumer Data Right - Final Report (treasury.gov.au)

(b) **Action Service Provider (ASP):** an ASP will be an entity that would be required to act on a valid (action) instruction received from an AAI. Only ASPs who are also designated DHs would be mandated to participate in CDR Action Initiation. Those mandated ASPs would be defined by a declaration instrument. However, non-designated entities would have the option to apply to the Minister to participate in the CDR as an ASP, on a voluntary basis. This would have the same effect as designating a person to be a DH, and voluntary ASPs would be required to become DHs for relevant data.

(c) **Eligible CDR consumers:** who could be an existing customer of an ASP, or a prospective customer (e.g. using the CDR action initiation process to set up a new account with an ASP).

Declaration Process

1.3.5 It is proposed that the Minister will identify and specify the types of actions through a 'declaration'. The proposed declaration process would be equivalent to the current sectoral designation process.

1.3.6 It would be possible for the Minister to declare more than one type of action at the same time. Further, the Minister would be able to declare action types across multiple sectors or parts of sectors however, in practice this may require multiple declarations. The proposed policy positions in relation to the declaration process which the PIA has had regard to are as follows:

(a) Consistent with the sectoral designation process for data sharing, the Minister's declaration should not impose substantive obligations or detail how the actions are to be initiated. These would be matters for the CDR rules and data standards to deal with.

(b) The introduction of a declaration mechanism for Action Initiation should not have any impact on the existing sectoral designation process for data sharing.

(c) However, if a subsequent sectoral designation for data sharing expands the notional scope of an action type designation, the Minister may need to amend or make a new declaration.

(d) Actions should not be declared in a way that would require ASPs to provide services through the CDR that they do not already provide outside the CDR.

(e) The declaration to bring in actions will not include any entities beyond designated DHs. This intrinsically links Action Initiation to the CDR data sharing ecosystem - actions cannot be introduced without a clear link to the DHs specified in a data sharing designation.

(f) The privacy risks for each action type will be considered at the declaration stage, and again at the rules stage.

(g) As is already the case for data sharing in the CDR, the Minister would retain flexibility as to whether CDR rules made under a declaration instrument cover the field of that declaration. For example, a declaration might include push, pull and recurring payments, while the rules might only enliven push payments for major authorised deposit-taking institutions in the first instance.

Instruction and action layers

1.3.7 Action initiation will comprise two layers of processes in the CDR that are relevant to the handling of consumer information and their privacy:

(a) **Instruction layer**: concerns the provision of the instructions in the communication channel between an AAI and an ASP whereby an AAI can initiate actions on behalf of a consumer. The flow of data from an AAI (as an ADR) to an ASP (as a DH) would be new to the CDR. The policy intent for action initiation is that the CDR statutory framework (including the Privacy Safeguards as amended) will focus on the steps and data flows that occur at the instruction layer.

(b) **Action layer:** concerns the actions executed by an ASP in response to the instructions from an AAI. The policy intent for Action Initiation is that the action layer will generally not be regulated by the CDR statutory framework as these actions would be carried out by ASPs and the relevant consumer data would be handled in the same way as if they received the instructions from the consumer directly. The notable exception to this is data that is disclosed by an ASP to an AAI in order to confirm or perform an action. The policy position is that any data shared by an ASP to an AAI would be regulated by the CDR in an equivalent manner to a DH sharing data with an ADR (and considered to be part of the instruction layer).

1.3.8 The proposed policy position is that a non-discrimination principle will require ASPs to carry out an action initiation request from an AAI as if it came from the consumer themselves. The non-discrimination principle would also prohibit ASPs charging higher than ordinary fees for the performance of CDR actions. However, the CDR is otherwise not intended to regulate the action layer. The policy intent is that ASPs would not be executing actions that they would not do outside the ordinary course of their business, and the CDR would not interfere in how these actions are completed. Rather, the CDR is introducing a new channel for AAIs to direct ASPs to execute actions (instruction layer). Once the ASP receives the instruction, existing processes will apply as if the instruction came from the consumer directly.

1.3.9 The CDR Rules will set out what data an AAI will be permitted to share with an ASP. It is not intended that an ASP receives data that they would not already receive and handle in the ordinary course of their business.

1.4 Privacy Safeguards for Action Initiation

1.4.1 As is currently the case for ADRs, AAIs will be subject to the Privacy Safeguards in the CCA. Currently, each of the Privacy Safeguards are equivalent to an Australian Privacy Principle (**APP**) except for: APP 12 (Access to personal information), which is covered by an enhanced

equivalent[11] being the entirety of CDR framework, and Privacy Safeguard 10 (Notification of disclosure of CDR data) which has no equivalent APP.

1.4.2 The Privacy Safeguards (and their interaction with CDR Rules) are more prescriptive than their equivalent APPs. They have broader application than the APPs and cover all designated and derived data relating to identifiable natural and legal persons, and bind ADRs in respect of CDR data they collect. The CDR Rules are taken to be consistent with the Privacy Safeguards, but the Privacy Safeguards will prevail over the CDR Rules to the extent of any inconsistency.[12]

1.4.3 The APPs do not apply to an ADR in relation to the CDR data they handle.[13] Similarly, the APPs generally will not apply to a CDR participant if they are bound by a Privacy Safeguard.[14]

1.4.4 DHs are only subject to: Privacy Safeguards 1 (open and transparent management of data), 10 (notification of disclosure), 11 (ensuring the quality of data) and 13 (responding to data correction requests). This is because the current role of the Privacy Safeguards is to protect consumer data that is requested and collected within the CDR. DHs may already be subject to existing privacy and confidentiality obligations in relation to the personal information they handle for their consumers (such as the APPs[15]).

1.4.5 Given that mandated ASPs would be DHs, and voluntary ASPs would become DHs if they hold CDR data relevant to the action being executed, we understand the policy intention is that the Privacy Safeguards will apply to ASPs as similarly as practicable to the current application for DHs.

1.4.6 The Privacy Safeguards impose strict requirements on CDR participants in relation to the collection, use and disclosure, correction and quality, and security of CDR data. The privacy safeguards only apply to CDR data for which there are one or more CDR consumers regardless of whether the CDR data is true or not.[16]

1.4.7 Action Initiation would introduce, in addition to data sharing, additional data flows and uses of personal information. For example, Action Initiation would involve:

(a) authorisations and consents for instructions to act (existing authorisations and consents are only to share CDR data with ADRs);

(b) AAIs issuing instructions to ASPs to act, on a consumer's behalf;

(c) consumers providing data to an AAI to allow the issuing of instructions; and

11 FD Report, page 175.
12 CCA s56EC.
13 CCA s56EC(4).
14 Ibid.
15 KPMG observes that the proposed policy position for CDR appears to assume that the majority of DHs/ASPs are subject to the APPs under the *Privacy Act 1988* (Cth).
16 See CCA s56EB. Note the requirement or CDR data to have a CDR consumer is that there needs to be at least one person who is identifiable, or reasonably identifiable, from the CDR data or from related information (see CCA s56AI(3)(c).

(d) DHs (ASPs) receiving data (with instructions) from AAIs for the purpose of performing the requested action, which is a new form of data sharing not covered by the existing CDR framework.

1.5 KPMG engagement & structure of report

1.5.1 Treasury has engaged KPMG[17] to prepare a PIA to inform amendments to the primary legislation. This includes the preparation of expected use case data flows and recommended changes to the Privacy Safeguards. The use cases are intended to give a broad indication of the types of data flows and participants that may be allowed by the primary legislation. However, the PIA is not limited to the use cases identified.

1.5.2 This Report has been structured according to the following sections. The scope of each section is described in detail in Section 3 of this Report.

(a) **Section 2** (Summary of findings and recommendations);

(b) **Section 3** (Scope, Assumptions & Methodology);

(c) **Section 4** (Data Flow Mapping);

(d) **Section 5** (Analysis of privacy impacts and risks);

(e) Appendices.

17 Which includes KPMG Law.

2 Summary of findings and recommendations

2.1 Summary of thematic risks and recommendations

2.1.1 The privacy risk assessment has been undertaken by key themes, developed from our understanding of the Action Initiation use cases and data flows.

2.1.2 **Table 1** summarises the key privacy risks and recommendations that have been identified in this report. It also provides recommended actions to address having regard to the proposed policy positions. For completeness, this Table consists of the risks with residual recommendations for Treasury to consider, noting that there are further risks identified throughout the analysis that we consider have been mitigated throughout the development of the PIA.

Table 1

No.	Risk	Existing mitigation strategies	Gap analysis and recommendations
1	Participants do not understand the types of CDR data required for certain action types.	It is proposed the Minister will declare action types but not the types of data that will be required to complete an action.	Prior to each action type being declared, we **recommend** that PIAs should be undertaken on the likely privacy risks associated with the data likely to be handled in order to complete the action (**Recommendation 1.1**). The PIA/s should carefully consider the data required for each action type and whether any rules or standards should be developed to manage how that data should be handled by CDR participants.
2	An ASP requests data from an AAI that is not relevant for the purposes of carrying out the action.	It is intended that the CDR Rules would supplement Privacy Safeguard 3 with guardrails on the scope of data permitted to be collected.	In developing the CDR Rules that set out guardrails on the scope of data permitted to be collected, we **recommend** that consideration is given to including a requirement that ASPs are subject to the data minimisation principle (**Recommendation 2.1**).
3	The proposed privacy framework could make it unclear for both consumers and participants about which regulatory framework applies to data handled by an entity as an ASP, or a DH, at a specific point in time. This could increase compliance concerns amongst ASPs trying to navigate their obligations.	The APPs would continue to primarily apply to ASPs, if they are subject to the Privacy Act (and there may be sectoral legislation that applies to the data). There may be some mandated or voluntary ASPs who are not subject to the Privacy Act, as the small business exemption applies to them or they are otherwise not considered to be an APP entity. The Australian Information Commissioner issues PS Guidelines under s 56EQ(1)(a) of	ASPs will not be executing actions that they would not do outside the ordinary course of their business, and the CDR is not aiming to interfere in how these actions are completed. We **recommend** that when an entity applies to participate in Action Initiation as an ASP on a voluntary basis, the Minister considers as a factor in the approval process, whether they are otherwise subject to adequate privacy obligations that are not

		the CCA to guide entities on when the APPs and Privacy Safeguards apply and complying with the Privacy Safeguards.	covered by the Privacy Safeguards (**Recommendation 3.1**).
4	Without explicit consent requirements in place for action initiation, consumers may not understand the purposes for which their data is being collected and how it may be used (i.e. to initiate actions).	**Privacy Safeguard 3** requires ADRs to seek the consent of the consumer prior to collecting their CDR data. Section 4.9 of the CDR Rules as, well as Chapter C of the CDR Privacy Safeguard Guidelines define the elements of a valid consent under the CDR as: voluntary, express, informed, specific as to purpose, time limited, and easily withdrawn. Privacy Safeguard 3 does not extend to consent to initiate an action however, it does apply to the data sharing involved in carrying out the instruction. Under Action Initiation, ADRs would not only be 'collecting' consumers' CDR data but also initiating actions on their behalf.	After identification of the privacy risks involved with **Privacy Safeguard 3** Treasury has proposed a new requirement for AAIs to seek valid requests to initiate an action through the CDR, consistent with their existing requirement to seek valid requests to collect CDR data. The introduction of this requirement would help distinguish the scope of consent requests for CDR data sharing and CDR Action Initiation requests and thereby improve consumers' understanding of how their data is being used however, the details relating to this should be tested in consumer experience research (**Recommendation 4.1**). While the introduction of this requirement would likely mitigate the immediate risk of AAIs initiating CDR actions without the consent of the consumer, we **recommend** that guidance is issued (e.g. by the OAIC and CX Guidelines) that assists AAIs to implement practical consent arrangements that are consistent with the elements in CDR Rule 4.9, and sufficient for consumers to appropriately understand the purposes for which they are consenting for their data to be used and disclosed (**Recommendation 4.2**). This may involve developing further guidance and undertaking consultations with consumers to ensure that the consents sought for action initiation are fit for purpose in regards to the scope of the action initiation activities. Further PIAs should be also undertaken for types of actions prior to them being declared to determine whether the existing CDR Rules in relation to consent adequately address the risks associated with the Action Initiation consent risks as identified below (**Recommendation 4.3**).

5	In the context of expanded consents, it may not be clear to the AAI when CDR data becomes 'redundant data'.	**Privacy Safeguard 12** requires that accredited data recipients of CDR data destroy or de-identify CDR data that is no longer needed for the purposes permitted under the CDR Rules, or any other purpose for which the information may be used or disclosed in accordance with the Privacy Safeguards. The current CDR Rules set out certain types of otherwise redundant data that is not to be deleted.[18]	It is **recommended** that the CDR Rules are amended to further frame circumstances that redundant CDR data is to be deleted (or not deleted) following the completion of instructions (**Recommendation 5.1**). It is otherwise **recommended** that further guidance is developed (e.g. in guidelines by the OAIC) on the steps an AAI could take to monitor and review the data that it continues to hold, to make it clear that it is the AAI's responsibility to ensure it is not retaining data for longer than is necessary (**Recommendation 5.2**).
6	Consumers provide authorisation for actions under Action Initiation without engaging with the content and/or disengaging from the system entirely.	**Privacy Safeguard 3** addresses the consumer providing the ASP/ADR with consent to 'collect' CDR data, and therefore supports the provision of informed consent. However, as noted above, **Privacy Safeguard 3** does not address consent to 'initiate an action'. In response, Treasury has proposed a new obligation that would require ASPs to seek consent from the consumer to initiate an action. The introduction of this obligation would support the provision of informed consent to initiate an action by the consumer to the AAI. **Privacy Safeguard 1** supports informed consent/authorisation by requiring CDR entities to handle data in an open and transparent way. One of the measures by which this is to be achieved is to require entities to develop and publish a CDR policy that informs consumers of the manner in which their CDR data will be handled. The current **CDR Rules** prohibit consents and authorisations being sought for longer than 12 months.[19] The consistency in the consent expiration timeframe may	Under Action Initiation, consumers will face additional decision-points and may not be able to completely foresee the consequences of the authorisation being provided, unless they are sufficiently advised of such consequences. This may especially impact more vulnerable consumers with lower levels of digital, data or language literacy. There is also a need to ensure that additional complexities built into the authorisation process do not undermine the purpose of the consent elements in the CDR Rules. It is **recommended** Treasury considers making the definition of 'authorisation' in the rules and standards for Action Initiation more prescriptive (**Recommendation 6.1**). It is also **recommended** that user testing is explored to determine the extent that consumers can understand authorisation in the context of action initiation, compared to other types of consent mechanisms under the CDR, and the sector in which the

18 See CDR Rule 1.17A. The listed types are where: paragraphs 56BAA(2)(a), (b) or (c) of the Act applies (deletion request by consumer); or where paragraphs 56EO(2)(b) or (c) of the Act applies (privacy safeguard 12). Where one of these provision applies, the accredited person must retain the CDR data while that provision applies (CDR Rule 1.17A(2)).
19 See for example CDR Rules 4.14(1)(d), 4.26(1)(e)It is noted that Treasury is consulting on extending the duration of business consumer use and disclosure consents as part of the proposed operational enhancements to the CDR Rules https://treasury.gov.au/consultation/c2022-315575

		help consumers understand the scope of their consents/authorisations.	authorisation relates to. It should be clear to consumers which CDR activity or instruction they are authorising, and how this differs from other types of CDR authorisation (e.g. standard CDR data sharing outside of action initiation) (**Recommendation 6.2**).
7	Unauthorised access to a consumer's CDR data from the ASP (as the DH) through the Action Initiation process whether in error or by a malicious actor if a consumer is not able to be effectively authenticated.	DHs are not subject to **Privacy Safeguard 12,** which addresses the security of information. However, **Privacy Safeguard 12** interacts with the APPs, and DHs will in any case be subject to APP 11. APP 11.1 imposes reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure which may include authentication (see the OAIC's Guide to Securing Personal Information). Some sector-specific regulations also support the consumer verification process. For instance, in the banking sector, reporting entities must comply with customer identification procedures including the 'Know Your Customer' (KYC) procedures.[20] Under existing CDR Rule 4.7, a DH has the ability to refuse to disclose CDR data in response to a request if the DH has reasonable grounds to believe that the disclosure would adversely impact the security, integrity or stability of the DH's ICT systems.[21] CDR consumers must be notified of any eligible data breaches in respect of their CDR data. The CCA applies the notifiable data breaches scheme (NDB Scheme) under Part IIIC of the Privacy Act to ADRs that hold CDR data.[22]	APP 11 can apply to an ASP/DH in place of Privacy Safeguard 12. However, it will only apply to APP entities (i.e. those that do not fall within the small business exemption). This means that a scenario could arise whereby an ASP/DH is not subject to Privacy Safeguard 12 or APP 11, therefore potentially without sufficient security in place to protect CDR data. This could be problematic in the context of Action Initiation as the ASP/DH is also receiving CDR data for the purposes of carrying out the action. This type of data flow is not addressed in the current CDR framework. We **recommend** that Guidelines are issued on the grounds in which an ASP could reasonably suspect that a disclosure could adversely impact the security, integrity of stability of their ICT systems (CDR Rule 4.7). It may also be prudent to consider guidance on whether such suspicion would be reasonable to communicate to an AAI, depending on the context of the incident that raises such suspicion (**Recommendation 7.1**).

20 *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth).
21 CDR Rule 4.7(b).
22 Section 56ES of the *Competition and Consumer Act 2010* (Cth).

2.2 Summary of other privacy risks, issues and considerations

2.2.1 We have also set out the following overarching risks and issues to consider as Action Initiation is developed:

(a) Development of targeted education and guidance should be considered to support CDR participant compliance as action initiation is introduced, to assist entities with different levels of privacy maturity, resourcing and ability to meet the increased obligations introduced under Action Initiation (**Recommendation 7**).

(b) Further consideration should be given to how some Action Initiation activities may be targeted to vulnerable consumers (such as those in financial hardship seeking quick financial gains, or those with lower levels of understanding about product/service offerings), and how to mitigate the risk of collection and/or use beyond consumer understanding (or consent) with this cohort in mind. For example, applying a purpose limitation as well as the data minimisation principle (**Recommendation 8**).

(c) The operation of **Privacy Safeguard 8** is further considered in circumstances where a consumer may instruct an AAI to make a payment to an overseas recipient. This may include whether there should be a CDR Rule for an AAI to disclose consumer data overseas based on the consent of a consumer instructing the AAI, and the data minimisation principle. Alternatively, if the intention is that all overseas recipients in scope of Action Initiation are required to also be accredited, we would recommend this is stated explicitly (**Recommendation 9**).

2.3 Recommended changes to Privacy Safeguards

2.3.1 The privacy impact assessment has been developed in consultation with Treasury, having regard to the development of the use cases, the proposed policy positions, discussions with the OAIC and DSB, and feedback from stakeholders who Treasury has consulted with. This has included updates to and feedback on the draft report, findings and recommendations. The primary focus has been on recommended changes to the Privacy Safeguards[23] to address identified privacy risks and impacts to inform legislative amendments.

23 Recommendations focussed on the application of privacy rights and obligations on CDR participants in Action Initiation, particularly for ASPs.

3 Scope, Assumptions & Methodology

3.1 Treasury requirements

3.1.1 KPMG was engaged to prepare a Privacy Impact Assessment. As part of this engagement, KPMG was required to prepare the mapping of data flows and provide recommended changes to the Privacy Safeguards.

3.1.2 This section explains the nature of the aspects to the Privacy Impact Assessment by reference to Treasury's requirements, noting it is a point-in-time assessment. It also details the assumptions that have been made to provide clarity to readers about the breadth and depth of our considerations and our approach to delivering the three aspects.

3.1.3 The scope of the Privacy Impact Assessment is described below.

3.2 Mapping of data flows

3.2.1 Section 4 of this Report provides a summary of the data flows. It maps out the processes, key participants and data flows of different action types, in the CDR. This includes data shared between entities to support actions, consent flows, instructions to act and status notifications.

3.2.2 The work undertaken in preparing the data flows does not replace or replicate work that has been, or may be, undertaken by the DSB in considering and developing the Standards for enabling Action Initiation to be carried out in the CDR.

3.2.3 The mapping of data flows informs Treasury's requirements and supports Treasury in designing a legislative framework for Action Initiation in the CDR.

3.3 Privacy Impact Assessment

3.3.1 Section 5 of this Report details the analysis of privacy impacts and risks undertaken against the data mapping. It provides a targeted analysis of the privacy risks from Action Initiation in the CDR informed by, but not confined to, the data mapping. It identifies how the Privacy Safeguards will apply to CDR participants, whether new participants should be captured, and how they interact with existing privacy laws and the CDR statutory framework. It also includes an analysis of the privacy risks associated with Action Initiation in the CDR and provides recommendations to

amend the Privacy Safeguards to ensure they are fit-for-purpose to cover the privacy impacts from Action Initiation in the CDR.

3.3.2 This sections also includes, more broadly, an assessment of the issues and risks against existing and proposed mitigation strategies including the consent, authentication and authorisation processes currently used for data sharing in the CDR.

3.4 Assumptions

3.4.1 This report has been prepared based on the following assumptions:

(a) **Action Initiation process**: Action Initiation through the CDR will be based on the existing consent, authentication and authorisation processes that currently apply and are used for data sharing, with appropriate amendments (as contemplated in this report). This report focuses on issues and amendments relevant to the CCA as the primary legislation for the purpose of enabling Action Initiation.

(b) **Gateways**: This report does not consider gateways specifically, as at the time of the assessment: no gateways were designated; and the Standards address APIs (not gateways).

(c) **Supplementary, point in time and living PIA**: This report supplements the CDR PIA. It does not revisit and reassess all the risks and issues identified in the CDR PIA, but rather focuses on issues relevant to the implementation of Action Initiation in the CDR. The PIA has otherwise been conducted on the issues and risks assessed and the policy specifications for Action Initiation at a point in time. The issues raised in this report may be subject to further review and analysis as the design and implementation of Action Initiation in the CDR continues.

(d) **Future PIAs**: Further PIAs may also be needed to inform declarations and rules for specific actions in the future. As such, this report focuses on issues relevant to the primary legislation, with a view to informing future changes to enable Action Initiation.

3.5 Methodology

Overarching methodology

3.5.1 The overarching methodology for preparing this report is detailed below. This includes the following steps:

(a) **Initial briefing:** we were briefed by Treasury and agreed on the scope of the report and working assumptions, which were refined during the assessment. We also discussed and identified material to be relied on, including the FD Report and its submissions.

(b) **Collaboration with Treasury**: we reviewed further information provided by Treasury on the proposed amendments. This included 10 suggested use case diagrams including payment initiation and the current approach to action initiation and proposed policy positions for action initiation with privacy risks identified throughout the engagement. KPMG worked collaboratively with Treasury and with engagement from and discussions

with the OAIC and DSB. Treasury also held discussions with the OAIC and DSB (which KPMG was not involved in).

(c) **Publicly available information**: in addition to the information provided by Treasury, this report draws on and reflects a range of publicly available and relevant submissions, reports and papers, including applicable research which were reviewed in the time available. This includes the FD Report which also identifies a number of use cases that were considered as part of the data flow mapping and other action and payment initiation frameworks such as the UK Open Banking standards.

(d) **CDR Rules, CDR Privacy Safeguards & PS Guidelines**: we reviewed the current version of the CDR Rules, the Privacy Safeguards and the PS Guidelines, and the Standards.

(e) **Initial discussions with the DSB and OAIC**: in addition to our consultations with Treasury, we discussed the initial data flows with the DSB and the OAIC. We also reviewed documentation provided by these stakeholders provided to inform the assessment.

(f) **Privacy impact assessment**: This PIA has been conducted in accordance with the OAIC's *Guide to Undertaking Privacy Impact Assessments*. We identified and critically assessed and analysed the potential privacy risks and impacts (both positive and negative) from the proposed implementation of Action Initiation in the CDR. We have not attributed a risk level or rating to the privacy risks we have identified. Our recommendations are also developed on this basis.

(g) **Review of and response to final report**: we understand that Treasury may consult further with stakeholders as required to respond to the findings and recommendations made in this current draft PIA prior to and/or as part of consultation on the Exposure Draft. Following the conclusion of these activities, this report may be updated or supplemented.

Methodology – Data Flows

3.5.2 Treasury confirmed a range of use cases should be included, the data flows should be diverse and should include the 'most likely' use cases across a range of actions and sectors.

(a) **DSB**: We consulted with the DSB in relation to the scope of data mapping, including how identified use cases will best support the data flow mapping. The DSB provided insightful feedback on the complexity of Action Initiation and how it may be applied to the CDR.

(b) **Multiplicity and extension or expansion of use cases**: given the range of actions and sectors that could potentially be declared under Action Initiation in the CDR, the number of use cases are potentially endless. Each use case will have its own nuances based on the action(s) the consumer authorised to be carried out on their behalf, and the data sets required to be shared to effect them. The approach is to provide a sample set of use cases to appropriately inform the PIA with reference to Treasury's requirements, namely that the use cases should include the 'most likely' use cases across a range of actions and sectors.

(c) **Use cases inform the data flows**: the use cases necessarily inform the data flows in circumstances where the data for each action will vary based on both the instruction type and the sector to which the instruction relates. It follows that the identified use cases may not provide a full picture of the potential data flows, and as a result all privacy risks may not be identified. Noting Treasury's requirements in the paragraph above, further privacy risks will likely be identified in the anticipated additional PIAs to inform the declaration and rules of specific actions.

Methodology – identification of risks and impacts

3.5.3 A thematic approach was taken to the impact assessment to inform findings and recommended changes.

(a) **Recommendations:** the recommendations were aimed at ensuring there is flexibility to allow for further identified use cases, and the development of rules and standards. Treasury has proposed that amendments to the primary legislation, to allow for the enactment of Action Initiation in the CDR, should provide flexibility consistent with how the regulatory framework for the CDR is currently structured (i.e. with the primary legislation generally providing high level requirements, and the rules and standards providing detailed requirements)

(b) **Likely use cases vs outliers**: the assessment focuses on the most likely use cases. Some of these use cases are identified in Part 1 of this report. However, there may be potential use cases that have not yet fully emerged. While the assessment focuses on the likely use cases, it also has regard to the 'outliers' being those use cases or aspects of use cases that are less likely to arise or raise particular nuances. An example is a use case involving an ASP that might not be either a DH under the existing CDR framework or an APP entity. Where there are nuances and differences between the likely use cases and outliers, this is clearly identified so that the privacy risks for each are not conflated in the overall assessment to address the most material risks.

(c) **Payment Initiation as focus use case:** payment initiation (which includes a broad range of action types) has been identified as the potential priority action type to be adopted and has been illustrated as an example in this PIA where appropriate. This is based on the recommendations from the FD Report and because payments are likely to be greater in volume than other types of actions. It is also noted that Open Banking was the sector initially designated under the CDR and is the most advanced sector under the CDR.

(d) **Consumer understanding of Action Initiation:** the FD Report notes that "consumers should not be expected, nor need, to understand how certain functions or data sets within the CDR are protected in different ways. However, being able to clearly understand that protections and safeguards do apply to their data, and where to seek redress, will be paramount."[24] This is important in the context of the consumer's understanding of the actions being undertaken and the Privacy Safeguards that may apply to those actions to the extent they involve the processing of CDR data.

24 FD Report page 179.

(e) **Purpose based consent & authorisation:** During consultations, a suggestion was made that purpose-based consents could be used to address a number of existing issues raised by CDR participants but may also address the anticipated complexity of expansion across many sectors. The DSB confirmed that this proposal would allow consents to be tied to a purpose. This would allow more streamlined consents that more efficiently capture required accounts, datasets, and action types. Further, this could be expanded to support purposes as needed. This suggestion can be considered further, and it is noted that for the purposes of this PIA, purposed-based consents is currently not a concept used in the CDR.

(f) **Participants outside the CDR framework:** we understand that it is intended that the role and responsibility of outsourced service providers and representatives will continue to be set out in the rules, which may extend to cover Action Initiation. This could include payment and other intermediaries connecting AAIs and ASPs. We have considered in this report the privacy risks and impacts associated with participants without CDR accreditation, or with different levels of CDR accreditation, in light of the information flows in Action Initiation.

3.6 Summary of CDR participants in Action Initiation

3.6.1 This section acknowledges additional participants and their obligations under the CDR and Privacy Act more generally, in addition to those participants identified above.

(a) **Sponsors:** are persons accredited at the unrestricted level who have entered into a written contract ('sponsorship arrangement') with an affiliate that meets the requirements of CDR Rule 1.10D. Under the sponsorship arrangement, the sponsor discloses CDR data to the affiliate so the affiliate can provide goods or services directly to a consumer. The sponsor can also collect CDR data on behalf of the affiliate, and use or disclose CDR data at the request of the affiliate.

(b) **Outsourced Service Providers (OSPs):** are entities engaged by an accredited person (the principal) to: collect CDR data on their behalf; or to provide goods or services to the principal using CDR data that the OSP collected on the principal's behalf or that was disclosed to the OSP by the principal. To use an OSP, an accredited person must have a written contract in place with the OSP.

(c) **CDR representatives**: are unaccredited persons who collect CDR data from an unrestricted accredited person (CDR principal) for the purpose of providing CDR goods or services directly to a consumer. To engage a CDR representative, the accredited person must have a written contract in place.

(d) **Trusted Advisers:** Rule 1.10C allows an accredited person to invite a CDR consumer to nominate one or more persons as their 'trusted advisor'. With the CDR consumer's consent, the ADR can then disclose their CDR to the nominated trusted advisor. Trusted advisers must belong to one of the professions specified in Rule 1.10C(2).

3.6.2 Under the proposed approach to Action Initiation, the role and responsibility of the entities described above would remain consistent with the approach for data sharing and would extend

to cover Action Initiation. We are instructed that these entities are out of scope for consideration in this PIA as they are covered by the rules, rather than the primary legislation, and would therefore be considered in subsequent PIAs as required

3.6.3 For completeness, this PIA considers the entities that have been defined under the primary legislation, and those intended to be introduced as a result of action initiation (e.g. AAIs and ASPs).

3.6.4 **Table 2** below outlines the entity participants involved in Action Initiation in scope of the PIA and their current coverage under the Privacy Safeguards and Privacy Act.

Table 2

Participant	Application of CDR Privacy Safeguards	Application of Privacy Act (generally)	Application of APPs
AAI (ADR)	An entity choosing to initiate actions on behalf of a consumer would be required to become an ADR under the CDR. As an ADR, the AAI would be subject to all 13 CDR Privacy Safeguards.	As an ADR, an AAI would also be subject to the Privacy Act in respect of personal information generally (i.e. excluding CDR data, even if they are a small business. This is because s6E(1D) of the Privacy Act provides that 'all accredited persons' are subject to the Privacy Act and APPs in relation to personal information that is not CDR data.	APPs 1 – 13 do not apply to ADRs in relation to the handling of CDR data (see section 56EC(4)(a) of the CCA. However, the APPs apply to ADRs in relation to their handling of personal information outside the CDR regardless of their size.
Designated ASP (DH)	It is intended that mandated ASPs will be DHs. As DHs, mandated ASPs are currently only subject to **Privacy Safeguards, 1, 10, 11, and 13.**[25]	DHs are subject to the Privacy Act in respect of personal information generally, unless the small business exemption applies.	Once a DH is authorised to share CDR data, they are required to comply with **Privacy Safeguards 1, 10, 11, and 13** in relation to the handling of that CDR data. **Privacy Safeguards 11 and 13** (data quality and correction) replace APPs 10 and 13 (respectively) in relation to that CDR data that is disclosed through the CDR (see s56EC(4)(b) and (c) of the CCA). However, APP 10 continues to apply to CDR data that is personal information in all other circumstances. Apart from the interaction of **Privacy Safeguards 11 and 13** with APPs 10 and 13, the Privacy Safeguards do not affect how the APPs apply to a DH/ASP in relation to CDR data (see s56EC(5)(a) of the CCA).

25 We acknowledge that the application of additional Privacy Safeguards, or equivalent requirements under the Rules to ASPs, remains subject to legislative design.

			This means that if the DH/ASP is not a small business (or none of the other relevant exemptions in the Privacy Act apply), it will be an APP entity and must comply with the APPs in relation to the personal information it collects and holds relating to the CDR, where there is no applicable obligation in the Privacy Safeguards.
Non-designated ASP (entities that are not DHs but participating as ASP on voluntary basis)	Entities would be allowed to voluntarily participate as ASPs, even if they are not DHs, subject to relevant approvals. This recognises that actions can be taken by entities currently outside designated CDR data sharing. Voluntary participation as an ASP would have the same effect as designating that entity to be a DH if they handle CDR data. Consequently, they would be required to comply with all CDR Privacy Safeguards that are applicable to DHs, i.e. **Privacy Safeguards 1, 10, 11, and 13.**	Voluntary participation as an ASP would subject the ASP to the Privacy Act in respect of personal information generally unless the small business exemption applies. Voluntary participation would place the same obligations on the ASP as a DH.	Same as above.

4 Data flow mapping

4.1 Use cases

4.1.1 **Nine**[26] sample use cases have been identified to support the mapping of data flows. These are detailed as follows:

(a) **Use case 0**: Consumer onboarding to AAI.

(b) **Use case 0.1**: Consumer authentication and authorisation.[27]

(c) **Use case 1: update details across multiple accounts.** Consumer can update details across multiple ASPs using AAI's services.

(d) **Use case 2**: **automatic payments**. The consumer uses AAI's services to set up standing instructions to transfer money between their accounts to maximise interest.

(e) **Use case 3**: **product/service application**. Consumer uses AAI's services to apply for a product or service. Note: this service instruction may follow Use Case 8 – Comparison Services (see below).

(f) **Use case 4: managing customer relationships**:

- **Use case 4a: managing customer products.** Consumer uses AAI's services to set up standing instructions to arrange multiple variable ongoing payments between financial institutions and merchants.
- **Use case 4b: stop recurring payments:** Consumer uses AAI's services to stop recurring payments.

(g) **Use case 5: Closing a product or ending a customer relationship**:

- **Use case 5a: closing a product:** Consumer uses AAI's services to cancel subscription of product.
- **Use case 5b: ending a customer relationship**. Consumer uses AAI's services to cancel a relationship.

(h) **Use Case 6: Revocation of instructions from AAI**. Consumer revokes instructions from AAI.

(i) **Use Case 8: Comparison services**. Consumer uses AAI's services to compare services.

4.1.2 The data flow mapping for the above use cases are enclosed at **Appendix 1.**

26 Use Case 7 was ultimately not progressed following preliminary identif ication.
27 Note: Use cases 0 and 0.1 have been identified to support the mapping of data flows. However, as they occur as part of other use cases (listed below), their privacy implications have been examined within the context of those other use cases.

5 Analysis of privacy impacts and risks

5.1 Overview

5.1.1 This section of the report details the privacy risks associated with Action Initiation in the CDR. As explained above, the approach to the privacy impact assessment is thematic to inform the recommended changes to the Privacy Safeguards for Action Initiation covering the instruction layer and action layer, Consent, Authorisation, Authentication, Security, and Notifications.

5.1.2 This section also, more broadly, identifies privacy issues and high level privacy risks and provides an assessment of the issues and risks against existing and proposed mitigation strategies.

5.2 Instruction layer

5.2.1 The instruction layer is the communication channel between an AAI and an ASP, whereby an AAI can initiate actions on behalf of a consumer.[28] From the use cases identified, a range of data may be collected, used and disclosed in the instruction layer depending on the type of action, participants involved and sector in which the action is to occur.

5.2.2 That is, action initiation in the CDR is designed to be a channel for consumers to give permissions to AAIs to instruct AAIs to act on the consumer's behalf, but neither the consumer nor AAI will play a role in carrying out those actions (which will be left to ASPs to carry out according to their existing processes and integrations).

5.2.3 For example, under Use Case 1, the AAI is engaged on the basis that it will update the address of the consumer with a DH or multiple DHs. In order to support the instruction and data sharing, the AAI would first need to collect relevant information from the consumer, including the consumer's basic contact details, residential address and details of the institutions the consumer has accounts with that need details updated. This information could be collected as part of a CDR data sharing request, or the consumer may provide this information directly to the AAI. The information would then be disclosed to the ASP through the instruction layer so that the ASP could carry out the action in the action layer.

5.2.4 Use Case 3 (i.e. Product/Service Application) involves the use of consumer data including their name, address, mobile number, email address, and application specific details. This information is then disclosed to the ASP who will use it when considering the application. Whereas Use Case 4.a (i.e. Managing Customer Products) involves information about the consumer's use of an ASP's services including financial account and utility bill details.

5.2.5 Similarly, for Use Case 8, the AAI would initially collect information from the consumer to support the action (to provide comparison services). The collection of data by the AAI from the consumer would include the consumer's basic contact details as well as information that is relevant to the service(s) to be compared. In the case of a comparison of utility services, this could include product data (such as the current plan), billing and account data, and usage data. The AAI (as the

28 KPMG is instructed that this will be clearly set out in the legislation.

ADR) and the ASP (as the DH) must handle the data in accordance with the Privacy Safeguards. It is important however, to note how the application of the Privacy Safeguards would differ between AAIs and ASPs.

5.2.6 As AAIs would be required to be ADRs to receive CDR data, any CDR data they receive as a result of a valid CDR request would be subject to the Privacy Safeguards. The Privacy Safeguards would continue to apply to CDR data in their capacity as an AAI role as they would to an ADR.

5.2.7 There would be situations where data that is not designated CDR data is provided by a consumer to an AAI as part of an action initiation request. This includes data shared via screen scraping. It is proposed that any data that the consumer shares with the AAI that is not designated under existing designations or under future action initiation declarations (i.e. CDR data) would not be in scope of the Privacy Safeguards.

5.2.8 Instead, any non-CDR data would be subject to the APPs, noting that under section 6E(1D) of the Privacy Act, small business operators that are ADRs are subject to all APPs in relation to information that is personal information that is non-CDR data. This applies regardless of the ADR's turnover. This would be consistent with the current approach to data sharing, where the ADR may offer additional services to CDR data sharing which involve data outside the scope of the CDR, for example combining Open Banking data with data from non-designated sectors.

5.2.9 Data may also flow back from the ASP to the AAI through the instruction layer as part of the action initiation process. As with the data received by the AAI from the consumer, if this data is CDR data, it is proposed that the AAI would be required to handle the data in the same manner as if it was shared by a DH to an ADR under the CDR. Non-CDR data received by an AAI from an ASP would be subject to the APPs as with similar data received by an AAI from the consumer.

5.2.10 It is proposed that the CDR rules would set out what data an AAI will be permitted to share with an ASP. As noted above, data that is not designated CDR data may be provided by a consumer to an AAI as part of an action initiation request. That said, if this non-CDR data is then shared with the ASP for the purposes of the action initiation request, the APPs would apply to any personal information to the extent the ASP is an APP entity. This may result in scenarios where the APPs would not apply due to the small business exemption.

5.2.11 We understand it is proposed that rules and standards would be developed to address these scenarios. However, the policy intent is that sharing of data should only occur after authentication and authorisation steps, unless there is an existing consent/authorisation with the relevant DH that permits the data sharing to occur. KPMG agrees with this position as it will ensure ASPs do not receive information through the instruction layer without proper authorisation and authentication. We discuss this further under the relevant sub sections below.

CDR data – Privacy Safeguards

5.2.12 **Privacy Safeguard 5** requires that an ADR (but not a DH) *must* notify the consumer in accordance with the CDR Rules[29] when they collect a consumer's CDR data under the CDR as a result of a valid request.[30] Given an AAI (as an ADR) would be collecting this data the AAI would have to notify the consumer of this collection if the data is CDR data.

5.2.13 Importantly, it is understood that the Privacy Safeguards would be activated once CDR data is collected by an AAI. That is, any CDR data that an AAI collects from a consumer to carry out an instruction or any CDR data that is received by an AAI from a DH (ASP). This approach would ensure consistency with the treatment of data that moves through the data flows as discussed above.

5.2.14 As discussed above, the data collected would depend on the type of instruction the consumer has consented the AAI to carry out. For example, in Use Case 1, the data would include the consumer's basic contact details including residential address and details of the institutions the consumer has accounts with and that need details updated. Similarly, for Use Case 8, the AAI would initially collect information (including the consumer's basic contact details as well as information that is specific to the service(s) to be applied for) from the consumer to support the Action Initiation (to provide comparison services).

5.2.15 In other use cases, the AAI would collect consumer CDR data from a DH rather than the consumer directly. For example, Use Case 4.a involves an AAI receiving information from a utility provider on a regular basis in relation to the consumer's billing. The AAI could also receive information from the consumer's financial institution detailing account balances. This is in addition to the initial collection of the consumer's details required to undertake the action of setting up multiple variable and ongoing payments.

5.2.16 As detailed above, this could mean data collected from the consumer by the AAI as part of the instruction layer could be both designated data collected under the CDR, as well as non-CDR data that may later become necessary to share in order to complete an action. Under Use Case 1 the initial data collected would be CDR data if it were for a designated product (e.g. banking product). However, if the product was an insurance policy (by way of example), as the insurance sector is yet to be designated, the data relating to the insurance product would not be considered CDR data until it was brought into the framework by designating that data for data sharing.

5.2.17 Provided that AAIs collecting non-CDR data remain subject to accreditation requirements,[31] we consider this would be a low risk, as accredited entities would need to handle any personal information they collect (or seek to collect) in accordance with APP 3 (e.g., collecting personal

29 The Rules require the ADR to notify consumers through their consumer dashboard. A consumer dashboard is an online service that enables you to see and manage your consents for the collection, use and disclosure of your data. It can be built into existing online portals or mobile apps and must be provided by all businesses participating in the Consumer Data Right.
30 CDR Privacy Safeguard 5.
31 See above: An AAI would be accredited by the ACCC

information that is reasonably necessary for the purpose of the instruction activity, collecting information by lawful and fair means).[32]

5.2.18 **Privacy Safeguard 3** provides for soliciting CDR data from CDR participants and permits ADRs to only collect a consumer's data from another CDR participant in response to a 'valid request' from the consumer. It is intended that this Privacy Safeguard is extended to ASPs.

5.2.19 The CDR Rules would set out what constitutes a valid request, including requirements and processes for seeking the consumer's consent. This is discussed in further detail in the next section under the sub-heading consent. In the context of collection, this would mean that the AAI as an ADR would only be able to receive information from a DH (ASP) if there is a 'valid request' for the data required to undertake the instruction.

5.2.20 As AAIs initiate actions, ASPs would in the first instance receive unsolicited but permitted data set out in the CDR Rules. An ASP may request (to collect) additional data to complete an action, for instance a bank requiring additional details from a consumer to consider an application. We understand it is intended that the CDR Rules would supplement **Privacy Safeguard 3** with guardrails on the scope of data permitted to be collected. It is appropriate that an ASP is able to receive such data when it receives a valid action request.

5.2.21 If an ADR collects CDR data that it did not seek to collect under the CDR Rules, the ADR is required by **Privacy Safeguard 4** - which provides for dealing with unsolicited CDR data from CDR participants **-** to consider whether there is a lawful means to retain the data, and if not, destroy that data. This Privacy Safeguard would apply to AAIs in their capacity as ADRs and it is proposed that this also apply to ASPs.

5.2.22 This could occur for example in Use Case 4.a (Managing customer products) if the consumer's financial institution provided the AAI with information in relation to a consumer account that the consumer did not provide the AAI with consent to access for the purposes of carrying out instructions. The same is possible for Use Case 2 (Automatic payments). As stated above for Privacy Safeguard 3, ASPs would in the first instance receive unsolicited but permitted data set out in the CDR Rules.

5.2.23 Subsequently, as part of the consideration of whether the reason to retain the data is lawful, ADRs would be required to consider whether the scope of permitted reasons to collect (action initiation) data which we understand would be set out in the CDR Rules. By applying Privacy Safeguard 4 to ASPs, they would be required to destroy CDR data they receive for a purpose that is not permitted by the CDR Rules as part of an unsolicited action requestion.

5.2.24 **Privacy Safeguard 6** - use or disclosure of CDR data by ADRs or designated gateways - permits ADRs to disclose consumer data only where required under the CDR Rules in response to a valid consumer request - which includes a consumer's consent - unless the use or disclosure is otherwise required or authorised under the CDR Rules or by or under another Australian law or a

32 See Chapter 3: APP 3— Collection of solicited personal information - Home (oaic.gov.au)

court/tribunal order. This would apply to AAIs as they are ADRs. The CDR Rules outline permitted uses and disclosures (Rule 7.5) and also prescribe prohibited ones.

5.2.25 The PS Guidelines describe a 'use' of CDR data as including accessing and reading CDR data, making a decision based on CDR data, as well as using CDR data to provide goods and services requested by the consumer.

5.2.26 This should cover access both for the purposes of 'read' and 'write'. The CDR data collected, used and disclosed in the instruction layer in each use case for the purposes of the action initiation to be carried out by the AAI would be covered by this requirement. 'Purpose' is a key privacy concept that is defined in the PS Guidelines[33] which states that the substantial purposes for which a person holds CDR data are deemed to be a 'purpose' for which the person holds the data.

5.2.27 **Privacy Safeguard 12** requires ADRs to destroy, delete or de-identify redundant data unless an exception applies. CDR data will be considered 'redundant' data if an ADR no longer needs the CDR data for purposes permitted by the Privacy Safeguards or the CDR Rules. This would apply to CDR Data received by AAI's (as ADRs) from the consumer and ASPs.

5.2.28 It is proposed that this Privacy Safeguard not apply to ASPs, as they already collect this data in the ordinary course of their business and are subject to relevant legislative requirements outside of the CDR.

APPs

5.2.29 There may be some instances where the APPs would not apply to mandated and voluntary ASPs (namely in circumstances where an ASP's annual turnover is less than AUD$3 million). This could result in situations where non-CDR data is not afforded protections under the Privacy Safeguard or the APPs. This is discussed further in the context of the action layer in the section below.

5.2.30 It is otherwise noted that the APPs would apply to non-CDR data that is personal information. The CCA does not affect how the APPs apply to accredited persons and accredited data recipients who are APP entities, in relation to the handling of personal information outside the CDR system. Further, under section 6E(1D) of the Privacy Act, small business operators that are ADRs are subject to all APPs in relation to information that is personal information but is not CDR data. This applies regardless of ADR turnover and the threshold does not apply.

5.2.31 In the context of the instruction layer, the APPs will provide additional privacy protections for consumers in addition to those found in the Privacy Safeguards discussed above (assuming the ASP is an APP Entity for the purposes of the Privacy Act and the small business exemption does not apply). For example:

(a) APP 5 will require ASPs to take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters, such as the purpose of the collection and information about the ASPs privacy policy.

33 See the OAIC's CDR Privacy Safeguard Guidelines,Chapter B: Key concepts - Home (oaic.gov.au).

(b) APP 11 includes requirements to delete or deidentify redundant personal information. This would apply to information an ASP received from an AAI in the instruction layer once it became redundant.

5.2.32 It is otherwise noted that the APPs would apply to personal information that is not CDR data that is handled by ADRs (as AAIs).

5.2.33 **Table 3** sets out the risks, existing mitigation strategies and gap analysis and recommendations for the instruction layer in action initiation.

Table 3

No.	Risk	Existing mitigation strategies	Gap analysis and recommendations
Instruction layer			
1	An ASP requests data from an AAI that is not relevant for the purposes of carrying out the action.	It is intended that the CDR Rules would supplement **Privacy Safeguard 3** with guardrails on the scope of data permitted to be collected.	In developing the CDR Rules that set out the type of data that is permitted to be requested by an ASP for different action types, we **recommend** that consideration is given to including a requirement that the ASP is subject to the data minimisation principle.
2	The consumer is not notified of data that an AAI collects.	**Privacy Safeguard 5** requires ADRs to notify the consumer through the consumer's dashboard when they collect the consumer's data. It is intended that AAIs be ADRs in order to participate in the CDR. This means the existing notification requirement for ADRs would also apply to AAIs.	The existing obligations in **Privacy Safeguard 5** continue to require notification of collection of CDR data, given the proposal that AAIs must be an ADR in order to participate in the CDR.
3	The consumer is not notified of data that an AAI collects from an ASP / the disclosure of their data by the ASP to the AAI.	We understand the intent of **Privacy Safeguard 5** is to require the AAI to notify the consumer when it receives data from the ASP. We understand it is proposed to extend the requirement in **Privacy Safeguard 10** to require an ASP (if they hold designated CDR data) to notify the consumer when it discloses their data to the AAI.	As above. **Privacy Safeguard 10** also ensures notification of disclosure of data by ASPs. However, this is only if the ASP is a DH (noting voluntary participation as an ASP has the same effect as designating that entity to be an ASP/DH). As such, we consider **Privacy Safeguard 10** provides adequate protections in relation to disclosure of consumer data by an ASP to an AAI.
4	The AAI uses information collected about the consumer for a purpose that is different to the purpose for which it was collected. For example, the AAI uses information collected for the	**Privacy Safeguard 6** prohibits the use of CDR data unless it is authorised under the CDR Rules. CDR Rule 1.8 requires that ADRs comply with the data minimisation principle. An ADR complies with this principle if:	The existing obligations for ADRs under **Privacy Safeguard 6** and the data minimisation principle in CDR Rule 1.8 appropriately manage the risk of an AAI using information about the consumer for a purpose that is different to which it was collected.

No.	Risk	Existing mitigation strategies	Gap analysis and recommendations
	purpose of undertaking a specific instruction for another purpose.	• When making a consumer data request on behalf of a CDR consumer, it does not seek to collect more data than is reasonably needed; or CDR data that relates to a longer time period than is reasonably needed to fulfil the consumer's CDR request; and • When providing the requested goods or services, using collected CDR data for any other purpose consented to by the CDR consumer, it does not use the collected CDR data or CDR data derived from it, beyond what is reasonably needed in order to provide the requested goods or services or fulfil the other purpose. It is intended that further CDR Rules would be issued to set out guardrails of the scope of information permitted to be collected. Should data collected be outside of that scope, AAIs would then need to consider Privacy Safeguard 4 (discussed below).	It may be prudent for guidance to be issued about the manner in which the data minimisation principle applies to particular 'actions' initiated in this context and the reasons to collect particular types of data that is commensurate to the actions, however, we acknowledge that a change to Privacy Safeguard 6 is not required in order to do so.
5	The AAI collects unsolicited data from an ASP that is outside of the scope of the action request.	**Privacy Safeguard 4** requires an accredited person to, as soon as practicable, destroy CDR data that the person has collected from a DH or ADR, where the accredited person has not sought to collect that particular data and is not required to retain it by law or court/tribunal order. The CDR Rules would set out additional valid reasons to data that is relevant to action initiation but may not have been solicited by the AAI. As an ADR, the AAI must comply with **Privacy Safeguard 4**. This risk is further mitigated by the proposed requirement for ASPs to be designated as a DH in order to participate in the CDR.	The existing obligations for ADRs under Privacy Safeguard 4 appropriately manage the risk of an AAI misusing any unsolicited data it receives from an ASP. As set out above, it may be prudent for guidance to be issued on the manner in which unsolicited data should be treated and the types of laws to consider prior to destroying the data.
6	CDR data and non-CDR data provided to an AAI (either by the consumer or by an ASP) could be used by AAIs to draw insights about the consumer for a purpose	CDR rule r4.12(3)(b) prohibits ADRs from requesting consent to use CDR data for the purpose of identifying, compiling insights in relation to, or building a profile in relation to any identifiable person	Utility and internet usage data is already provided to utility and internet consumers in bills. It is also generally available to the consumer via online accounts and applications.

No.	Risk	Existing mitigation strategies	Gap analysis and recommendations
	not permitted under the CDR Rules. This could occur for example in the use cases involving comparison services – the AAI could leverage usage data to compile insights about members of a household if the action initiation request related to changing utility or internet provider.	who is not the CDR consumer making the consumer data sharing request.	This data is also already provided to third party comparison services to enable the service to match a product or service to their usage needs. The CDR framework provides existing mitigation strategies for data that is already shared less securely outside of the CDR ecosystem. These existing mitigation strategies will appropriately manage the risk of insights being derived from the sharing of usage data.
7	That participants do not understand or over-estimate the types of CDR data required for certain action types.	It is proposed the Minister will declare action types, but not the types of data that will be considered CDR data required to complete an action.	Prior to each action type being declared, a PIA should be undertaken on the likely privacy risks associated with declaring the action types and the associated data likely to be handled in order to complete that action. The PIAs should carefully consider the data required for each action type and whether any rules or standards should be developed to appropriately manage how that data would be handled by CDR participants This will likely involve a balancing act between what data should be considered CDR data to enable each action type against the obligations of CDR participants in relation to that data. Consideration should also be given to whether the application of the Data Minimisation Principle in the CDR Rules (that applies to collection and use of CDR data) needs to be updated.

5.3 Action layer

5.3.1 The action layer is concerned with how an ASP chooses to execute an action type. It is the policy intention for this to not be in the scope of the CDR. Further, it is proposed that a non-discrimination principle would require ASPs to carry out an action initiation request from an AAI as if it came from the consumer themselves. However, beyond this high-level principle, the CDR is not intended to regulate the action layer.

5.3.2 The reasoning for this policy position is that ASPs will not be executing actions that they would not do outside the ordinary course of their business, and the CDR is not looking to interfere in how these actions are completed. Instead, the CDR would introduce a new channel to direct

ASPs to execute actions. Once the ASP receives the instruction, existing processes would apply as if the instruction came from the consumer directly. Further, there are existing frameworks in place that regulate these actions accordingly.

5.3.3 As ASPs would be designated DHs (or voluntary ASPs, who will become DHs), ASPs would continue to be primarily regulated under the Privacy Act. There may be some instances where the APPs do not apply to mandated and voluntary ASPs – when they are not considered to be an APP entity, or the small business exemption applies to them. As ASPs will only be performing actions that they already can do, they should only be receiving data that they would receive had an action instruction come from a consumer directly outside of the CDR. This is because the CDR is only creating a new channel for ASPs to receive data that they would already be able to receive (outside the CDR). It is not enabling them to receive any other data that they are not already able to receive. Therefore the risk that small ASPs or other non APP entities may receive data they would not otherwise be permitted to receive should be low, although by participating, they may collect and use more consumer data.

5.3.4 The Privacy Act and APPs (subject to the relevant thresholds) will apply to the personal information that ASPs receive from an AAI through the instruction layer when the information is used to execute an action. That is, under the current proposal, CDR data would only be subject to the Privacy Safeguards when it is in the instruction layer. It may cease to be CDR data and instead be subject to the Privacy Act and APPs when it is handled under the action layer and used to execute an action. Similarly, data that becomes subject to the Privacy Act and APPs may revert back to being subject to the CDR if that data is then shared through the instruction layer by an ASP to an AAI.

5.3.5 The Privacy Act will also apply to personal information received from the consumer by the ASP. For example, in the use cases that relate to the provision of a new service or product. There may be situations where the ASP requires more information than provided by the AAI in the instruction layer.

5.3.6 There is a risk that applying both the Privacy Safeguards and the Privacy Act to ASPs at different times could make it unclear which regulatory framework applies to which type of data at a specific point in time. In consultation with KPMG, Treasury considered whether it would be more appropriate to apply the Privacy Safeguards to all ASPs. This approach would apply the same regulations to both ASPs and ADRs, who would both be receiving CDR data. However, it could also cause compliance challenges for ASPs if they were subject to both the APPs and all of the Privacy Safeguards as there could be duplication in the privacy obligations they must comply with including data retention and deletion requirements once the action is completed or the consumer relationship ends. This approach may also be disproportionate, given that ASPs should only be receiving and using data which they would ordinarily be able to receive and handle in the course of their business.

5.3.7 The alternative approach is to create a framework that clearly delineates between the application of regulatory obligations at the instruction layer (which is specific to the CDR), and at the action layer (which is covered by existing privacy regulation). This would manage risks associated with the flow of CDR data in the instruction layer, and where the risks are specifically attributable to the CDR, while existing privacy regulations that apply to ASPs will continue to do so in the

action layer. Consumers would have the same rights and protections at the action layer, whether they initiated an action themselves or through the CDR.

5.3.8 We therefore **recommend** that, due to the application of different regulatory frameworks, clear legislative design and related non-binding guidelines are developed to ensure all parties are aware of and understand the applicable framework for data handled within Action Initiation at each point in the process and their relevant obligations. We also **recommend** that when an entity applies to participate in Action Initiation as an ASP on a voluntary basis, there be a requirement that they cannot be approved to participate without having adequate privacy obligations.

5.4 Consent

5.4.1 Consumer consent is at the heart of the CDR regime as it ensures consumers have control over their data, thereby enhancing trust in the CDR ecosystem. An accredited person is required by the CDR Rules to obtain one or more of the prescribed categories of consents from a consumer, depending on the data-related activity they are carrying out based on requirements in the Rules. For Action Initiation to operate effectively, consumers will need to be asked for a number of consents – to initiate the action itself, and then to collect, use, share, access, and update their data to enable that action to be carried out.

5.4.2 The mapped use cases all begin with the consumer providing the AAI consent to initiate the relevant action. **Privacy Safeguard 3** would support these objectives by requiring ADRs (including AAIs) to seek valid consent from the CDR consumer prior to the 'collection' of their CDR data. However, the scope of **Privacy Safeguard 3** is limited as it does not contemplate scenarios beyond the 'collection' of data, such as initiating actions.

5.4.3 In response, Treasury has proposed to create a new requirement in the primary legislation for an AAI to seek valid consent from a consumer to initiate an action, consistent with the requirement to seek valid consent to collect CDR data.

5.4.4 The identified use cases may involve 'singular consents' or require 'ongoing consents' to undertake actions, and/or share data to support those actions. For instance, Use Case 8 (i.e. comparison services) could involve a singular consent to obtain a quote from a DH. Alternatively, Use Case 1 could support both a singular consent (i.e. one 'round' of address changes with DHs), or ongoing consents (i.e. consent to cover multiple rounds of address changes should the consumer move address frequently). Use Case 2 could involve either singular or ongoing consent, such as where an AAI transfers money between a consumer's accounts on a repetitive basis to maximise interest.

5.4.5 The nature of the required consents raises questions about how data should be managed by the AAI following the expiry of those consents. Once a consumer's consent expires, the AAI would have to delete or de-identify any CDR data that they have received about the consumer. The question then becomes whether the data collected by the AAI is subject to these obligations in circumstances where the action initiation consent may have expired (following the action being carried out) but where the consumer and AAI may have an ongoing relationship involving instructions that may arise intermittently. Initial stakeholder consultations suggested the

'ongoing consents' should be categorised as a singular consent that results in multiple actions (under that consent).

5.4.6 This consent would be for a period of time, to allow for the facilitation of the action consented to. Currently the permitted consent period is 12 months in the CDR Rules. As highlighted in the FD Report, the ongoing ability to initiate actions on behalf of a consumer could have greater potential for harm than ongoing data sharing arrangements, depending on the nature of the instructions. Consistent with the recommendations in the FD Report, applying the maximum 12 month duration for consents and authorisations in the context of Action Initiation may help mitigate privacy risks. However, given the additional risk of harm, we question whether this timeframe should be shortened for Action Initiation based on the risk associated with each action type.

5.4.7 We understand that rules and standards for ongoing consents would be developed at a later stage.

5.4.8 Given the extended nature of consents that may be required for Action Initiation, there is a risk that some consumers may not comprehend the: nature or extent of the consent they are providing; all of the consequences of providing that consent; the actions that may occur and when; how their information will be used (write access); and/or who the data will be shared with and who will carry out the instructions they have authorised (**Action Initiation Consent Risks**).

5.4.9 These risks should be able to be addressed primarily by the existing CDR Framework. Section 4.9 of the CDR Rules defines the standard elements of CDR consent as:

(a) voluntary;

(b) express;

(c) informed;

(d) specific as to purpose;

(e) time limited; and

(f) easily withdrawn.

5.4.10 It is intended that the existing CDR framework for consent is used consistently for read access (current state) and write access (future state under Action Initiation). Further PIAs should be undertaken for types of actions prior to them being declared to determine whether the existing CDR Rules in relation to consent would adequately address the risks associated with the Action Initiation Consent Risks identified above.

5.4.11 In the absence of any of the above elements of consent, the AAI (as an ADR) would be prohibited from undertaking action initiation, or seeking to collect CDR data about the consumer from an entity that is not an ASP and the subject of the consent. However, even with these safeguards in place, the range of consents involved in Action Initiation and the different abilities of consumers to understand those consents, may result in a situation where a consumer provides consent to an AAI to undertake certain instructions but that 'consent' is not valid as they may simply proceed

without fully comprehending (meaning the consent is not voluntary, express and informed (amongst the other elements)), or they did not understand purpose or extent of the 'consent'. This could result in a situation where the AAI does not comply with **Privacy Safeguards 3, 6** and **14.**

5.4.12 It is also important to consider ASPs' privacy obligations in relation to the retention of unsolicited CDR data under Action Initiation. ASPs could receive unsolicited information from AAIs in several use cases. For instance: Use Case 2 involves the AAI providing the ASP with the consumer's account details and transfer amounts per institution; Use Case 4 involves the ASP providing the consumer's billing details to the ASP. Given the AAI is not carrying out the action themselves they may not understand the scope of data required for that action and provide the ASP more information than necessary.

5.4.13 Under the current framework, ASPs may be able to retain this unsolicited data as persons who are not 'accredited' under the CDR are not subject to Privacy Safeguard 4. In this scenario, APP 4 will apply instead – which enables entities to retain unsolicited personal information if they decide it could have been collected under APP 3. We understand that it proposed that Privacy Safeguard 4 be amended to require ASPs to delete any CDR data that is received from an AAI as part of an action request which is outside the scope of the requested action.

5.4.14 A situation could arise whereby an AAI (ADR) or an ASP (DH) attempts to use the data received as part of Action Initiation for the purposes of direct marketing. AAIs would be prohibited from doing this without the consumer's consent by **Privacy Safeguard 7**. Considerations regarding **Privacy Safeguard 7** are discussed in detail in Section *4.6 Further commentary on CDR Privacy Safeguards.* It is noted that Privacy Safeguard 7 would not apply to ASPs. The rationale for this is twofold. Firstly, ASPs are prohibited from using or disclosing personal information for the purpose of direct marketing by **APP 7**. Secondly, ASPs already receive data received as part of action requests in their ordinary course of business and as such, should be able to treat this data the same as data outside the CDR.

5.4.15 **Table 4** sets out the risks, existing mitigation strategies and gap analysis and recommendations for consent in action initiation.

Table 4

No.	Risk	Existing mitigation strategies	Gap analysis and recommendations
		Consent	
8	Without explicit consent requirements in place for action initiation, consumers may not understand the purposes for which their data is being collected and how it may be used (i.e. to initiate actions).	**Privacy Safeguard 3** requires ADRs to seek the consent of the consumer prior to collecting their CDR data. Section 4.9 of the CDR Rules as, well as Chapter C of the CDR Privacy Safeguard Guidelines define the elements of a valid consent under the CDR as: voluntary, express, informed, specific as to purpose, time limited, and easily withdrawn.	In response, we understand it is proposed to include a new requirement for AAIs to seek valid requests to initiate an action through the CDR, consistent with their existing requirement to seek valid requests to collect CDR data. This new requirement would help distinguish the scope of consent requests for CDR data sharing and CDR Action Initiation requests and thereby improve

No.	Risk	Existing mitigation strategies	Gap analysis and recommendations
		However, **Privacy Safeguard 3** does not extend to action initiation requests. Under Action Initiation, ADRs would not only be 'collecting' consumers' CDR data but also initiating actions on their behalf.	consumers' understanding of how their data is being used. While acknowledging the design of this new requirement is yet to be settled, we **recommend** that guidance is issued (e.g. by the OAIC in Guidelines) that assists AAIs to design practical consent frameworks that are consistent with the elements in CDR Rule 4.9. This may involve developing further guidance and undertaking consultations with consumers to ensure that the consents sought for action initiation are fit for purpose against the scope of the action initiation activities. Consumer experience research could also be undertaken to facilitate comprehension and informed consent, and standardise descriptions of actions, as the data language standards do for datasets today. Further PIAs should be also undertaken for action types prior to them being declared to determine whether the existing CDR Rules in relation to consent adequately address the risks associated with the Action Initiation Consent Risks as identified above.
9	In the context of expanded consents, it may not be clear to the AAI when CDR data becomes 'redundant data'.	**Privacy Safeguard 12** requires that accredited data recipients of CDR data destroy or de-identify CDR data that is no longer needed for the purposes permitted under the CDR Rules, or any other purpose for which the information may be used or disclosed in accordance with the Privacy Safeguards. The current CDR Rules set out certain types of otherwise redundant data that is not to be deleted.[34]	It is **recommended** that Treasury consider amending the CDR Rules to further frame circumstances that redundant CDR data is to be deleted (or not deleted) following the completion of instructions. It is otherwise **recommended** that further guidance is developed (e.g. in guidelines by the OAIC) on the steps an AAI could take to monitor and review the data that it continues to hold, to make it clear that it is the AAI's responsibility to ensure it is not retaining data for longer than is necessary.

34 See CDR Rule 1.17A. The listed types are where: paragraphs 56BAA(2)(a), (b) or (c) of the Act applies (deletion request by consumer); or where paragraphs 56EO(2)(b) or (c) of the Act applies (privacy safeguard 12). Where one of these provision applies, the accredited person must retain th e CDR data while that provision applies (CDR Rule 1.17A(2)).

No.	Risk	Existing mitigation strategies	Gap analysis and recommendations
10	CDR data is used by an ADR/AAI for direct marketing purposes without the consumer's consent.	**Privacy Safeguard 7** prohibits the use or disclosure of CDR data for direct marketing unless the consumer consents and such use or disclosure is required or authorised under the CDR Rules.	The existing obligations for ADRs under **Privacy Safeguard 7** appropriately manage the risk of an AAI using information about the consumer for direct marketing purposes.
11	CDR data is used by an ASP/DH for direct marketing purposes without the consumer's consent.	**Privacy Safeguard 7**, which prohibits the use or disclosure of CDR data for direct marketing purposes would not apply to ASPs. The rationale for this is twofold. Firstly, ASPs would be prohibited from using or disclosing personal information for the purpose of direct marketing by APP 7. Secondly, ASPs already receive data received as part of action requests in their ordinary course of business and as such, should be able to treat this data if the request came outside of the CDR.	We consider that the application of APP7 to ASPs is sufficient to mitigate the risk of CDR data being used by ASPs for direct marketing purposes.

5.5 Authorisation

5.5.1 The FD Report categorises 'authorisations' as a type of consent that is provided to the ASP/DH by the consumer to accept the CDR instruction from the AAI. This authorisation would be a prerequisite to the ASP progressing the CDR action.

5.5.2 The use cases provide for a range of authorisations which are necessarily tied to the consents for each action. Under the proposed framework, the CDR consumer first provides a singular consent to the AAI, then completes authentication, and authorises the ASP to engage in the action.

5.5.3 In circumstances where there are multiple or ongoing types of consents (as discussed above), the authorisation(s) required for the ASP to carry out the action (as instructed by the AAI) will vary. For example, the authorisation required under Use Case 1 is relatively straight forward - where the consumer authorises the ASP to change the address details on accounts held by the consumer. In this example, the authorisation is in relation to the specific action being undertaken. The AAI is authorised to effect the change of address instructions with a specific ASP. There are other use cases which are more complex, such as where the consumer provides multiple authorisations tied to the consents given to the AAI. For example, in Use Case 2 (i.e. Automatic payments), a consumer would need to provide details of their account to the AAI (with consent) on an ongoing basis, and authorise the ASP to accept instructions from the AAI, again on an ongoing basis, to transfer funds as required. That is, the consumer would give ongoing

authorisation for the ASP to act on initiation requests falling within particular instructions set by the AAI.

5.5.4 Similar to consents, the types of authorisations (i.e. singular vs ongoing) raise questions about what actions should require specific authorisation, and those under which it is appropriate for ongoing authorisation to apply. The FD Report suggests that higher risk actions, such as the updating of personal/financial details, should require specific authorisation. Whether a particular action requires specific authorisation will have to be considered in the context of the action itself, including the participants to that action, the data types involved, and the sector in which the action is carried out. This could likely be addressed as part of the declaration for each action type or addressed in further PIAs as use cases are further developed.

5.5.5 In addition to the above distinction between singular and ongoing authorisation, we understand it could be possible for a consumer to provide caveated, conditional or limited authorisation. The FD report refers to this as 'fine-grained' authorisation and notes it could include the ability for consumers to impose limits to their authorisation, for instance limits on transaction amounts initiated by AAIs.

5.5.6 Introducing fine-grained and singular authorisations may increase complexity for consumers. This complexity will grow over time, as consumers engage with more CDR participants. Increased complexity in the consent and authorisation framework may increase the likelihood of consent fatigue among CDR consumers, which may lead to consumers providing consent/authorisation without engaging with the content or disengaging from the system entirely.

5.5.7 Increased complexity may also reduce understanding, especially among vulnerable consumers such as those with lower levels of digital and data literacy.

5.5.8 These outcomes may undermine the proposed elements of authorisation and consent outlined in the CDR if they are not suitably designed to assist consumers. It is therefore critical for any additional authorisation measures to be designed to provide consumers with choice, so they are able to specify the purposes for which they are providing authorisation and properly understand the consequences, without becoming overwhelmed by complicated requests for consent.

5.5.9 Further complexity is introduced when considering the different authorisation steps that CDR sectors follow based on the nature of their product/service offerings and existing practices and processes within the sector. For instance, the energy designation introduces the concept of a secondary DH whose disclosure must be covered by the primary DHs authorisation service. This authorisation step, however, does not apply to the Open Banking designation, as secondary DHs do not exist within that sector. The authorisation process for Action Initiation should be tested on a sector-by-sector basis from a privacy risk and consumer experience perspective.

5.5.10 Finally, we understand the policy position (expressed by both Treasury and the DSB) is that authorisation and authentication (see next sub section) should occur before any data is shared as

part of an action initiation request. This approach is sensible to mitigate privacy risks associated with action initiation.

5.5.11 **Table 5** sets out the risks, existing mitigation strategies and gap analysis and recommendations for authorisation in action initiation.

Table 5

No.	Risk	Existing mitigation strategies	Gap analysis and recommendations
12	Privacy Safeguard 3 does not address consent to 'initiate an action'. Consumers provide authorisation for actions under Action Initiation without engaging with the content and/ or disengaging from the system entirely.	**Privacy Safeguard 3** addresses the consumer providing the ASP/ADR with consent to 'collect' CDR data, and therefore supports the provision of informed consent. In response, Treasury has proposed that a new requirement be introduced in the primary legislation to require ASPs to seek consent from a consumer to initiate an action. **Privacy Safeguard 1** supports informed consent/authorisation by requiring CDR entities to handle data in an open and transparent way. One of the measures by which this is to be achieved is to require entities to develop and publish a CDR policy that informs consumers of the manner in which their CDR data will be handled. The current **CDR Rules** prohibit consents and authorisations being sought for longer than 12 months.[35] The consistency in the consent expiration timeframe may help consumers understand the scope of their consents/authorisations.	Under Action Initiation, consumers will face additional decision-points and may not be able to completely foresee the consequences of the authorisation being provided, unless the dashboard appropriately presents sufficient information to inform the consumer. This may especially impact more vulnerable consumers with lower levels of digital, data or language literacy. There is also a need to ensure that additional complexities built into the authorisation process do not undermine the purpose of the consent elements in the CDR Rules. It is **recommended** Treasury considers making the definition of 'authorisation' in the rules and standards for Action Initiation more prescriptive. It is also **recommended** that user testing is explored to determine the extent that consumers can understand authorisation in the context of action initiation, compared to other types of consent mechanisms under the CDR, and the sector in which the authorisation relates to. It should be clear to consumers which CDR activity or instruction they are authorising, and how this differs from other types of CDR authorisation (e.g. standard CDR data sharing outside of action initiation). The development of CX Standards may further mitigate this risk.

35 See for example CDR Rules 4.14(1)(d), 4.26(1)(e).

5.6 Authentication

5.6.1 The current CDR authentication process provides DHs and ADRs with sufficient confidence that the person who makes a request is indeed an existing customer of the DH. This occurs through one-time password (OTP) authentication, whereby the consumer is sent a password (through one of a range of channels) to enter into the DH's customer interface.

5.6.2 The use cases assume that the ASP would be required to authenticate the consumer before the ASP can progress the action. This is consistent with the approach proposed in the FD Report and is consistent with current data sharing obligations in the CDR.

5.6.3 The existing process will likely remain the same for the use cases identified where the AAIs or ASPs involved have an existing relationship with the consumer. There are use cases however where the current authentication process is not applicable. For example, in Use Case 8 (comparison services), the ultimate ASP may not have an existing relationship with the consumer and therefore is unable to authenticate the consumer through the OTP method. Rather, based on the flow, the ASP would be reliant on the consumer information provided by the AAI to produce a quote (assuming that specific consumer information is required to do so). We understand the policy intention is to allow for rules and standards to be developed to set out authentication requirements for the ASPs who do not have existing relationships with consumers (which could include OTP or other digital mechanisms to set up a sufficient relationship with a consumer to carry out the action).

5.6.4 In Use Case 3, the AAI holds consent and authorisation to apply for a product with the ASP on the consumer's behalf. For this to occur, we consider the ASP would have to authenticate the consumer in circumstances where the relative risk of entering into a contract is much higher than simply obtaining a quote. In circumstances where there is no existing client relationship, the ASP would onboard the consumer as a customer outside of the CDR framework. We understand it is proposed that the data collected by the ASP in this circumstance would not be CDR data until it is the subject of an action initiation request by the AAI. Once the consumer is onboarded with the ASP, the ASP can then authenticate the consumer for the purposes of the action to be carried out.

5.6.5 Use Cases 3 and 7 also raise questions about how authentication should occur if an ASP does not have a pre-existing relationship with the consumer.

5.6.6 The inability to authenticate the consumer may compromise the consumer's privacy. Without processes in place to verify the identity of a CDR consumer and to authenticate the consumer, the CDR data that an ASP holds would be vulnerable to unauthorised access and misuse. Currently such an outcome would not contravene Privacy Safeguard 12 as it does not apply to DHs, but it may contravene APP 11 which applies to DHs instead. ASPs (who may be APP entities) would be at risk of non-compliance with APP 11.1 where they are unable to authenticate the customer due to the absence of an existing customer relationship. As detailed above, the

ASP would onboard the consumer as a customer in these situations. This process would occur outside of the CDR.

5.6.7 The security of CDR data is a key privacy consideration at the authentication stage that ensures trust in the CDR. CDR data is overall afforded a high level of protection by the Privacy Safeguards and their interaction with the CDR Rules and designations. Action Initiation has the potential to increase and broaden the volume and types of CDR data that flows between and is used by CDR participants, at a consumer's instruction, over a period of time as new use cases are introduced and as more entities participate (including industry sectors with different regulatory frameworks).

5.6.8 **Table 6** sets out the risks, existing mitigation strategies and gap analysis and recommendations for authentication in action initiation.

Table 6

No.	Risk	Existing mitigation strategies	Gap analysis and recommendations
13	Unauthorised access to a consumer's CDR data from the ASP (as the DH) through the Action Initiation process whether in error or by a malicious actor if a consumer is not able to be effectively authenticated.	DHs are not subject to **Privacy Safeguard 12,** which addresses the security of information. However, **Privacy Safeguard 12** interacts with the APPs, and DHs will in any case be subject to APP 11. APP 11.1 imposes reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure which may include authentication (see the OAIC's Guide to Securing Personal Information). Some sector-specific regulations also support the consumer verification process. For instance, in the banking sector, reporting entities must comply with customer identification procedures including the 'Know Your Customer' (KYC) procedures.[36] Under existing CDR Rule 4.7, a DH has the ability to refuse to disclose CDR data in response to a request if the DH has reasonable grounds to believe that the disclosure would adversely impact the security,	APP 11 can apply to an ASP/DH in place of Privacy Safeguard 12. However, it will only apply to APP entities (i.e. those that do not fall within the small business exemption). This means that a scenario could arise whereby an ASP/DH is not subject to Privacy Safeguard 12 or APP 11.This creates a potential gap in privacy protections for consumers, including for CDR data which is received by the ASP/DH for the purposes of carrying out the action. The likely risk and impact of this gap requires further analysis at the declaration stage for specific action types. We **recommend** that in (albeit limited) circumstances where an ASP is not subject to the APPs, that the ASP (for the purposes of Action Initiation) is required to comply with equivalent security obligations to Privacy Safeguard 12. While we acknowledge this is subject to legislative design, this could be considered as part of the development of revised CDR Rules or Standards, for instance by extending the application of CDR Rule 4.7 to all ASPs, or to develop CX Standards in relation to security for all ASPs.

36 *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth).

No.	Risk	Existing mitigation strategies	Gap analysis and recommendations
		integrity or stability of the DH's ICT systems.[37] CDR consumers must be notified of any eligible data breaches in respect of their CDR data. The CCA applies the notifiable data breaches scheme (NDB Scheme) under Part IIIC of the Privacy Act to ADRs that hold CDR data.[38]	We **recommend** Guidelines are issued on the grounds in which an ASP could reasonably suspect that a disclosure could adversely impact the security, integrity of stability of their ICT systems (CDR Rule 4.7). It may also be prudent to consider guidance on whether such suspicion would be reasonable to communicate to an AAI, depending on the context of the incident that raises such suspicion.

5.7 Notifications

5.7.1 The use cases break down the notifications, generally, into the following processes:

(g) notifications regarding the disclosure or use of data, and

(h) notifications regarding the progress of the action.

5.7.2 Under Privacy Safeguard 10, where a DH (including an ASP) or an ADR (including an AAI) discloses a consumer's data to an accredited person, they would be required to notify the consumer by updating their consumer dashboard (in accordance with the matters set out in the CDR Rules).

5.7.3 For instance, under Use Case 4.a (Managing customer products) the ASP discloses a consumer's utility bill details to the AAI to enable the AAI to set up instructions for recurring payments. The disclosure from the ASP to the AAI would be treated as if a DH shared CDR data with an ADR. It is proposed that Privacy Safeguard 10 would require the ASP to notify the consumer of the disclosure of their CDR data to the AAI.

5.7.4 Relatedly, under Privacy Safeguard 5, where an ADR (including an AAI) collects consumer data from a DH (including an ASP) (for example, as described in Use Case 4.a above), the ADR/AAI would be required to notify the consumer through the consumer dashboard.

5.7.5 In some use cases, the ASP collects consumer data from the AAI. For instance, under Use case 1 (i.e. Update details across multiple accounts) the ASP collects the consumer's details to be updated from the AAI. In such scenarios, Privacy Safeguard 5 will not apply to the ASP/DH. However, we consider ASPs existing notification obligations under APP 5 are sufficient to ensure the consumer is aware of the collection of their information from the AAI. Specifically, APP 5 would require ASPs who collect personal information about an individual to take 'reasonable steps' to either notify the individual of certain matters or to ensure the individual is aware of

37 CDR Rule 4.7(b).
38 Section 56ES of the *Competition and Consumer Act 2010* (Cth).

those matters. Further, ASPs already collect the data relevant to Action Initiation and have existing processes in place to notify consumers of its use.

5.7.6 Notification steps can ensure that that mistakes in instructions or in the performance of the action are identified and rectified, so that data remains 'accurate, up to date, and complete'. Notification steps, therefore, support compliance with Privacy Safeguard 11 which aims to ensure consumers have trust in and control over the quality of their CDR data and sector participants can rely on the data, allowing consumers to enjoy the benefits of the CDR.

5.7.7 While these notification safeguards address read-access to CDR data, further consideration may be required of whether and how consumers should be notified of write-access to their data which arises in the context of Action Initiation.

5.7.8 Write-access notification steps can protect against identity theft and financial fraud by alerting the consumer when their personal information has been updated (for example, as part of Use Case 1 – Update details across multiple accounts) or when a payment has been made from their account (for example, as part of Use Case 2 – Automatic Payments). Therefore, write-access notification may also support the intent of Privacy Safeguard 12 which includes the prevention of harm to individuals such as financial fraud and identity theft. We note however that in some scenarios, consideration should be provided to the practicality of providing consumers with notification on data receipt as well as on the status of the action request, and the ability of the CDR Rules or guidelines[39] to be accommodating in this respect.

5.8 Security

5.8.1 ASPs (whether designated or voluntary) would not be subject to Privacy Safeguard 12. Instead, they would be required to comply with the comparable information security requirements in APP 11. APP 11 will only apply if the ASP does not fall within the small business exemption. This means an ASP (who is a small business) may not be subject to either Privacy Safeguard 12 or APP 11 which leaves a gap in the CDR framework.

5.8.2 While we acknowledge that the policy intent of action initiation is not to disturb the existing privacy obligations that an ASP/DH may be subject to when handling a consumer's personal information in the ordinary course of business, when considering the manner in which consumer data is being collected by, and subsequently used by an ASP through the CDR, there is potential for neither the CDR framework or the APPs to apply to certain ASPs. Consumers would reasonably expect that data handled through the CDR would be treated in a more secure and protected manner than through other means. We **recommend** that in circumstances where an ASP is not subject to the APPs, that the ASP (for the purposes of Action Initiation) is required to comply with security obligations equivalent to Privacy Safeguard 12. While this is subject to legislative design, this could be considered as part of the development of revised CDR rules or

39 The CX Guidelines currently recommend DHs issue a CDR receipt. It would be open for further CX Guidelines to be developed.

standards, such as CX Standards for all ASPs, or as a factor considered by the Minister when approving voluntary ASP participation.

5.8.3 Action initiation would give AAIs write-access (i.e. the ability to use and modify a consumer's data) for declared action types, thereby elevating their privileges to access and use consumer data received through the CDR, subject to requirements specified in the rules. Depending on the action type, the required data flows and access privileges would mean different types of data (including sensitive data) could be exposed - such as identification details, financial information and government identifiers. By way of example, Use Case 2 (Automatic payments) and Use Case 4.a (Managing customer products) will involve financial information being disclosed to AAIs to engage in financial transactions. This raises both privacy risks as well as other potential impacts for consumers in relation to the actions that will be carried out on their instructions, often automatically over a period of time.

5.8.4 The FD Report identified the risk from the elevation of privileges provided to ASPs (as well as the increase in data flows) noting this may make them attractive to malicious actors who target an AAI/ADR's systems to gain access to those privileges.

5.8.5 These issues would need to be considered on a case-by-case basis to identify any additional rules that may be required to mitigate data access risks. We accordingly **recommend** that during the development of the rules and standards, security risks from increased data access privileges and data sharing arising from each action type are considered (for instance through consultation with the CDR agencies, and/or other agencies and industry bodies with responsibility for cyber security, identity and data protection more generally). It any also be prudent to consider user testing with consumers to ensure that these processes are sufficiently understood, balanced against consumer expectations about the treatment of CDR data from a privacy and security perspective.

5.9 Further commentary on Privacy Safeguards and Action Initiation

5.9.1 In this section, we assess a number of the Privacy Safeguards further.

1: Open and transparent management of data

5.9.2 Privacy Safeguard 1 requires accredited businesses to have procedures and systems in place to ensure they meet their CDR privacy obligations, and to publish a clearly expressed and up-to-date CDR policy about how they manage consumer data. The following OAIC guidance highlights how this requirement differs depending on the type of entity:

5.9.3 The CDR regime imposes a range of privacy obligations upon CDR entities. Some of these privacy obligations apply to all CDR entities, while other privacy obligations apply only to a particular entity type. Entities will need to ensure that they consider the relevant obligations that apply to them when deciding on the steps to be taken in relation to Privacy Safeguard 1.

5.9.4 For example, an accredited data recipient of CDR data must comply with the privacy safeguards in relation to the CDR data. However, a data holder needs to comply with the APPs in relation to CDR data that is also personal information with the exception of APPs 10 and 13, which are

replaced by Privacy Safeguards 11 and 13 once the data holder is required or authorised to disclose the CDR data under the CDR Rules. Data holders must also comply with both Privacy Safeguard 1 and APP 1, as well as Privacy Safeguard 10.

5.9.5 Currently, both DHs and ADRs are required to comply with Privacy Safeguard 10. We understand that it is proposed the application will extend to both AAIs, and ASPs. Irrespective of the use cases applicable, an entity should be required to comply with this overarching requirement. That is, it would be a matter for an entity to ensure that changes to the way they handle consumer data, once a use case commences, is reflected in their CDR Policy, and considered against the relevant Privacy Safeguards and/or APPs, when designing procedures to implement the use case.

5.9.6 Consumers need to clearly understand how the protections and safeguards would apply to their data, and where to seek redress. We consider this could addressed by a requirement for entities to consider when developing their CDR policy (i.e. as a matter of design), as well as further user testing with different types of consumers to ensure that this issues can be communicated clearly.

5.9.7 Accordingly, we do not consider that a change to Privacy Safeguard 1 is required.

2: Anonymity and pseudonymity

5.9.8 Privacy Safeguard 2 provides that accredited businesses (but not DHs) must provide consumers with the option to not identify themselves or to allow them to use a pseudonym. Exceptions apply to this requirement, such as where it is not practical for a business to deal with a consumer that has not appropriately identified themselves, or if a law or a court order requires businesses to deal with an identified consumer.

5.9.9 In our view, the exceptions would more than likely apply to all the use cases applicable to this PIA. This is because an AAI would need data about the consumer to effect instructions on the consumer's behalf (with their consent), and it would not be practical to allow an AAI to proceed without reasonably identifying the consumer to whom the instructions relate.

5.9.10 We note the following from the Explanatory Memorandum to the Bill introducing the CDR to the CCA:

(a) Unless the consumer data rules specify instances where an accredited data recipient is unable to provide a CDR consumer with the ability to use a pseudonym, a pseudonym is permitted. The option may be given through a designated gateway. [Schedule 1, item 1, subsections 56EE(1) and 56EE(2)]

(b) The Government would not expect that a consumer could use a pseudonym when exercising their consumer data right in the banking sector. A consumer cannot typically engage with the banking sector without identifying themselves.

(c) Privacy Safeguard 2 does not apply to data holders or a designated gateway. As applicable, the Privacy Act 1988 and APPs will apply to data holders.

5.9.11 **Recommendation**: Consideration should be given to including further guidance, or additional rules, to support the Government's expectations on the sectors to which the exceptions to

Privacy Safeguard 2 would apply (noting the existing sectoral commentary). Alternatively, examples or guardrails could be provided on the circumstances that AAIs would be expected to allow a consumer to elect to use a pseudonym, and how this would be communicated to an ASP in circumstances where there is not an existing customer relationship. Such guidance could be provided in non-binding settings (such as the OAIC Guidelines). Considering the current use cases, we do not consider that any change to Privacy Safeguard 2 is required.

7: Direct marketing

5.9.12 Under Privacy Safeguard 7, accredited businesses (but not DHs) cannot use CDR data for direct marketing unless a consumer consents and the marketing circumstances (activities) are permitted under the CDR Rules.

5.9.13 CDR Rule 7.5(3) permits the following permitted direct marketing activities (with consent, which would practically operate in conjunction with Privacy Safeguard 6):

(a) sending the consumer information about upgraded or alternative goods or services to the existing goods or services;

(b) sending the consumer an offer to renew existing goods or services when they expire;

(c) sending the consumer information about the benefits of existing goods or services;

(d) sending the consumer information about other goods and services provided by another accredited person if the accredited data recipient reasonably believes the consumer might benefit from these other goods or services, and only sends such information on a reasonable number of occasions;

(e) using CDR data in a way and to the extent that is reasonably needed in order to send the consumer something permitted by the point above (e.g., analysing the data to identify the appropriate information to send); and

(f) disclosing the consumer's CDR data to an outsourced service provider:

(g) for the purpose of doing the things referred to in the two points above, and

(h) to the extent reasonably needed to do those things.

5.9.14 The marketing that AAIs will likely wish to undertake about their services that support the use cases are likely to fall within the above activities. This approach, covering permitted Action Initiation related marketing activities in the CDR Rules, together with the consent obligation in Privacy Safeguard 7 appear adequate to effectively manage marketing activities.

5.9.15 If an AAI wanted to send marketing information to a consumer about their ability to conduct Use Case 1, for example, they would need to ensure that:

(a) the consumer has consented to the marketing, and

(b) the activity is permitted under Rule 7.5(3) - for example, by determining that the use case is an 'updated or alternative' service to their existing service offering.

5.9.16 Privacy Safeguard 7 will not apply to DHs (including ASPs), as we understand the policy intention is that ASPs should be able to treat data received in an action request as part of their ordinary course of business, and as if the request came outside of the CDR. We understand the majority of DHs/ASPs would be subject to APP 7 when handling personal information for marketing purposes.

5.9.17 **Recommendation**: At this point in time, we therefore currently consider that no changes to Privacy Safeguard 7 are required.

8: Overseas disclosure of data

5.9.18 Privacy Safeguard 8 prohibits accredited businesses (but not DHs) from sending consumer data overseas unless one of the following exceptions applies:

(a) the overseas recipient is also an accredited person;

(b) the ADR takes reasonable steps to ensure the overseas recipient will not breach the privacy safeguards (noting that, for this exception, the accredited data recipient remains accountable for any breach of the privacy safeguards by the overseas recipient); or

(c) the ADR reasonably believes the overseas recipient is subject to a law equivalent to the privacy safeguards and there are mechanisms available to the consumer to enforce that protection.

5.9.19 For use cases 2, 3 and 4a, it may be difficult for AAIs to undertake due diligence in determining whether every account to which they receive instructions from a consumer meets an exception. For example, under use case 4a, a consumer could instruct an AAI to set up payments to five institutions, two of which are based overseas. It may not be practical to necessarily require the AAI to determine whether the overseas institutions meet the existing exceptions.

5.9.20 For DHs/ASPs, we understand that it is proposed that APP 8 should continue to apply, given that any disclosure of consumer data overseas would occur as part of the action layer, which is out of scope of the CDR.

5.9.21 **Recommendation**: consideration should be given to including an additional exception to Privacy Safeguard 8 - based on the consent of the consumer instructing the AAI, and applying the data minimisation principle. Using the example above for Use Case 4a, a consumer could provide their consent for the AAI to disclose only the minimum information required to facilitate the payment that they instruct the AAI to provide. Alternately, if the intention is that all overseas recipients are required to also be accredited under Action Initiation, we would recommend this is stated explicitly. Therefore, we recommend that Treasury consider amending Privacy Safeguard 8 to cover instructions where, for example, there may be payments to overseas recipients.

9: Adoption or disclosure of government identifiers

5.9.22 Privacy Safeguard 9 prohibits accredited businesses from adopting, using or disclosing a government-related identifier unless required or authorised under another law, court order or privacy regulation.

5.9.23 Depending on the nature of the action and the ASP requirements, some of the current use cases may require the use or disclosure of a government-related identifier. It is also intended that government entities may become AAIs or ASPs in the future as the scope of action initiation expands and use cases identified. If and when this were to occur, Treasury would need to consider further:

(a) in the first instance, whether the adoption, use or disclose of government-related identifiers (by the government entity) would be required or authorised under another law or privacy regulation, and

(b) if not, what other reasons (outside of what is already authorised under law) would require the government identifier to be adopted, used or disclosed, in addition to other identifying information about a CDR consumer.

5.9.24 This assessment can occur by reference to use cases that identify the government entities that may become AAIs or ASPs including the actions that may be declared. This process would identify whether any government identifiers may need to be used to carry out an action, which in turn will frame Treasury's consideration of whether Privacy Safeguard 9 requires amending to allow those actions to occur in the CDR.

5.9.25 **Recommendation**: At this point in time, therefore we do not currently consider there are any circumstances in the scope of this PIA that require a change to Privacy Safeguard 9.

13: Correction of data

5.9.26 Privacy Safeguard 13 interacts with CDR Rule 7.15 to require DHs, and accredited businesses, to consider and action requests made from consumers to correct their data. The obligations are separated as follows:

(i) responding to a consumer's request, by completing the following (using the 'steps' prescribed in the Rule):

i. to either correct the data, or include a statement with the data to ensure that it is accurate, up-to-date, complete and not misleading, and

ii. to either give notice that the correction/statement above has been completed, or give notice of why the correction/statement would be unnecessary or inappropriate; and

(j) taking the 'steps' in the Rule which are: acknowledging receipt of a consumer's request as soon as practicable, actioning the request within 10 business days, issuing the notice described above by electronic means, and including in that notice complaint mechanisms if the consumer is not satisfied with the outcome.

5.9.27 We understand that the Rules may be amended to require an AAI to disclose corrected data to an ASP in circumstances where the AAI deals with these requests.

5.9.28 **Recommendation**: The right of a consumer to seek correction of data is an important privacy mechanism for the CDR. None of the use cases informing our assessment raise any further risks that would in our view require amendments to Privacy Safeguard 13.

5.10 Other privacy risks, issues and considerations

Privacy maturity

5.10.1 Given the number of entities who may become CDR participants over time, there may also be different levels of privacy maturity, resourcing and ability to meet the increased obligations in the Privacy Safeguards. As the CDR rules are developed to cater for the different impacts and requirements for actions, the complexity of the obligations may increase. As actions are proposed and phased in this can give participants time to prepare. The role of the DSB in consulting with the stakeholders and developing appropriate Standards will also be a key mitigation step.

5.10.2 **Recommendation:** It is **recommended** that targeted education and guidance for participants should be considered to support compliance as action initiation is introduced.

Vulnerable consumers

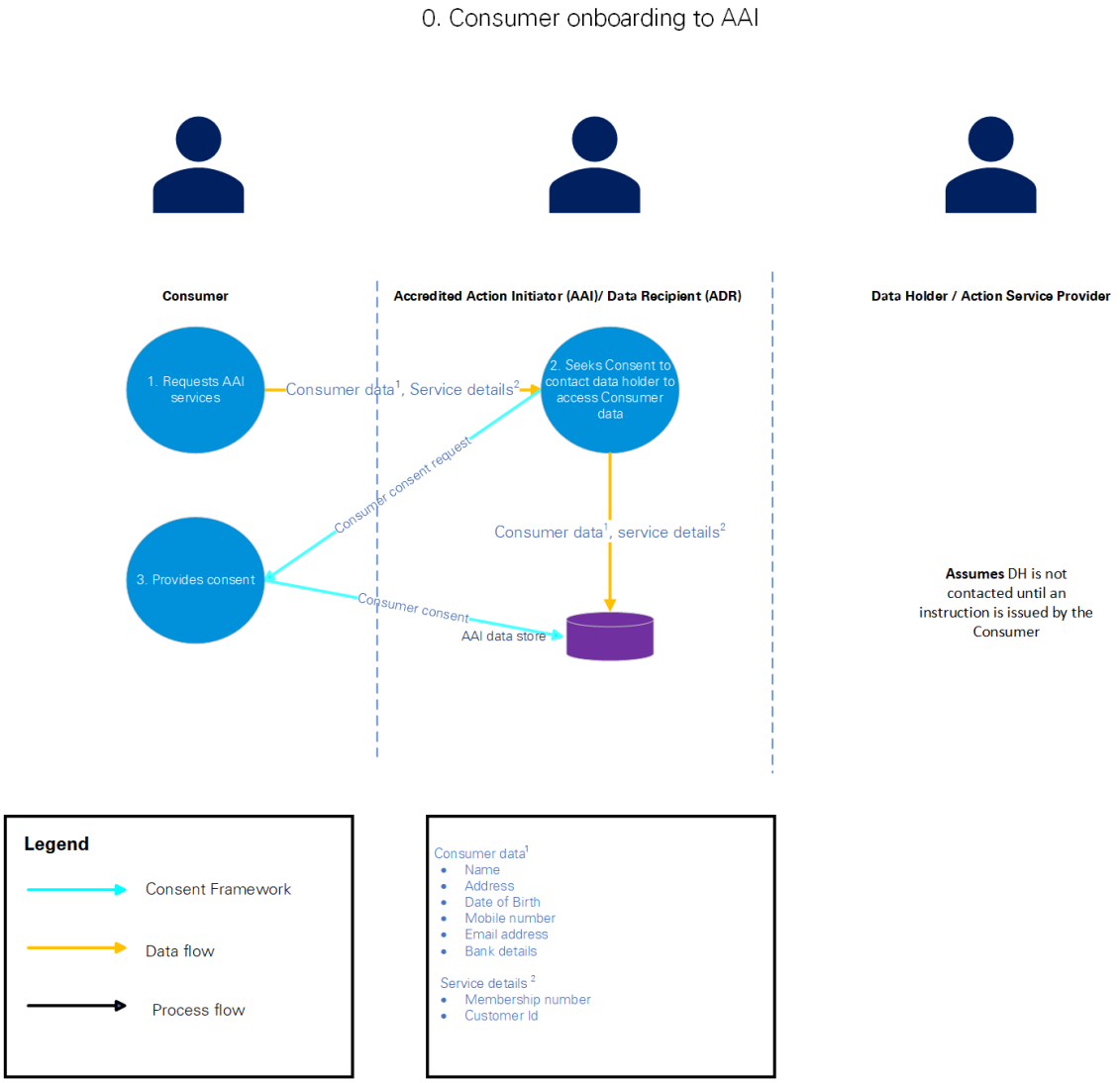
5.10.3 There is a risk that certain actions may be more attractive to more vulnerable consumers such as: those in financial hardship seeking access to quick loans or high financial risk products and services, or those with lower levels of understanding about product/service offerings and how to navigate the system through which they are provided.

5.10.4 Such consumers may be more likely to consent to write access and providing action instructions for a range of purposes without the appropriate advice for their needs, or may struggle to engage with ongoing and more complex consents. This risk could be exacerbated by the range of CDR participants who may seek to engage these types of consumers. Consideration should be given to how these risks could be addressed, reflecting the recommendations in earlier PIAs that have been undertaken on these issues, for example in the telecommunications and non-bank lending PIAs.

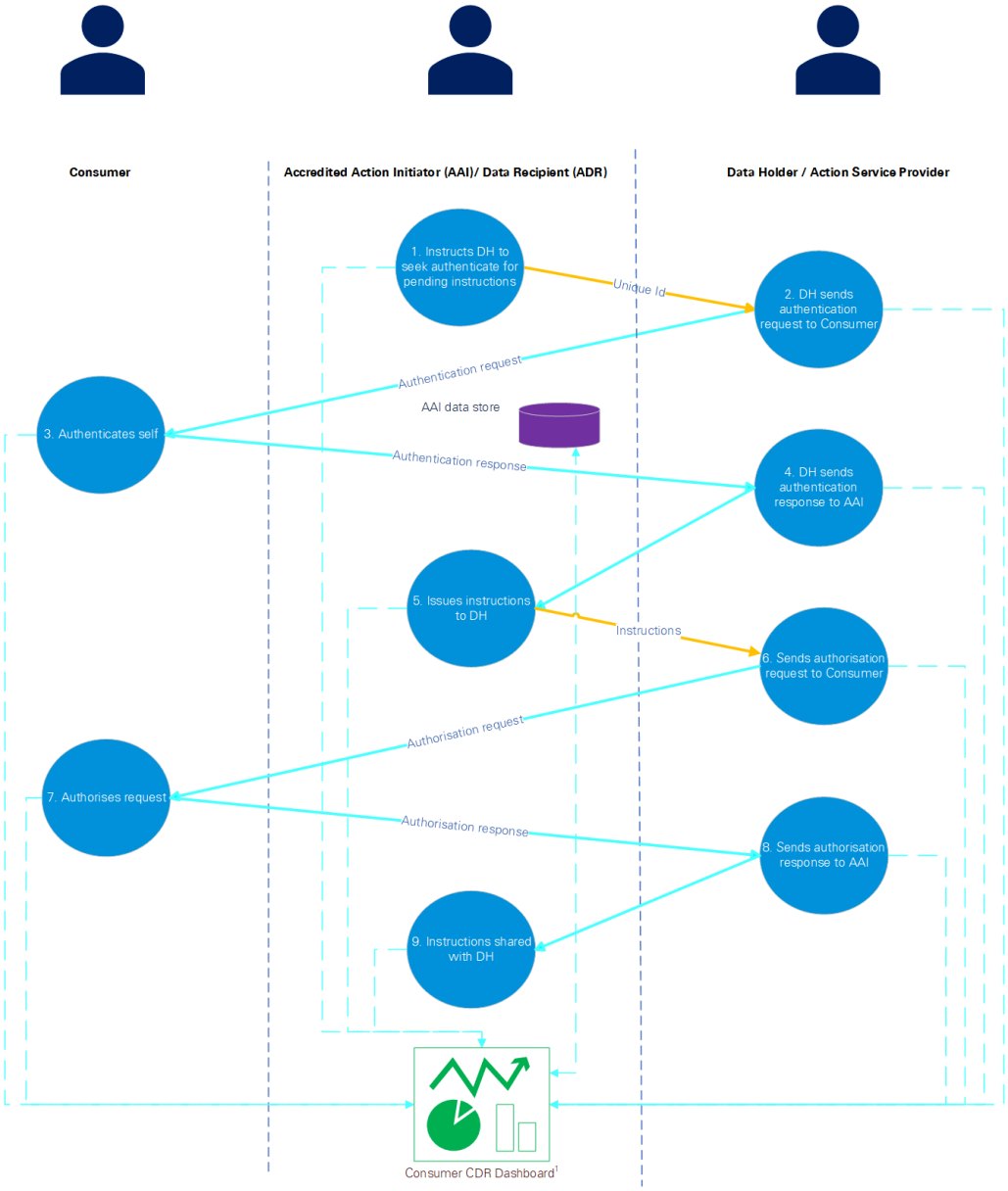
5.10.5 **Recommendation**: In developing the CDR Rules for action initiation, it is **recommended** that consideration should be given to including a purpose limitation (in addition to the data minimisation principle), that applies to action instructions, collection and use. This together with the data minimisation principle will help to mitigate the risk of over collection or use and the potential privacy risks to these consumers as well as consumer more generally.

Appendix 1: Data flow mapping

The work undertaken in preparing the data flows is indicative only and does not replace or replicate work that has been, or may be, undertaken by the DSB in considering and developing the Standards for enabling Action Initiation to be carried out in the CDR.



0.1 Consumer authentication and authorisation



Legend

- Consent Framework
- Consent dashboard flow
- Data flow
- Process flow

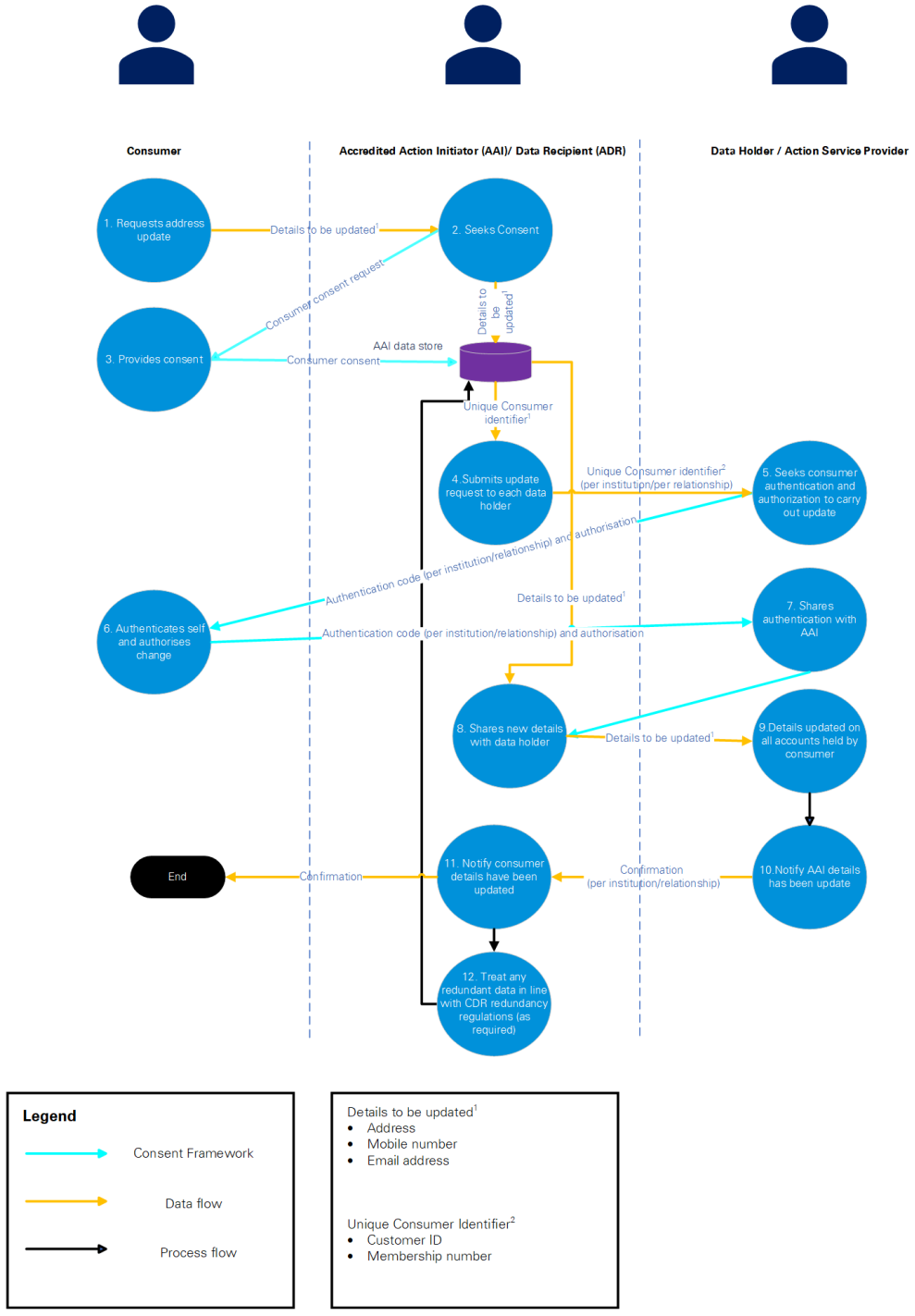
Consumer CDR Dashboard[1]

Dashboard manages consent, authentication and authorisation status in relation to each consumer instruction. It is maintained by the AAI.

It is the primary tool for the Consumer to understand for what purpose authentication and authorisation is being requested.

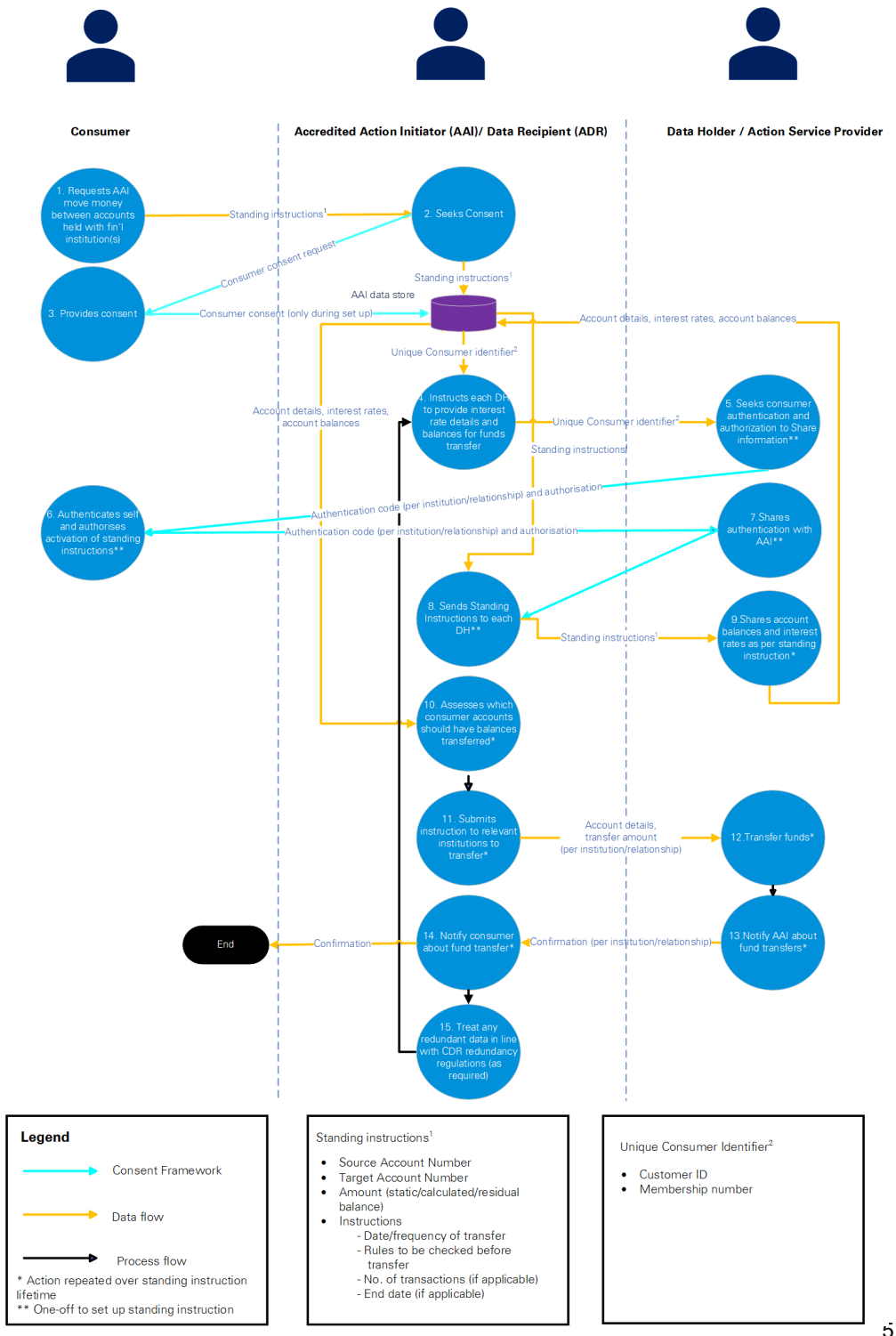
1. Update details across multiple accounts

Use Case Description : Consumer can update details across multiple data holders using AAI's services



2. Automatic Payments

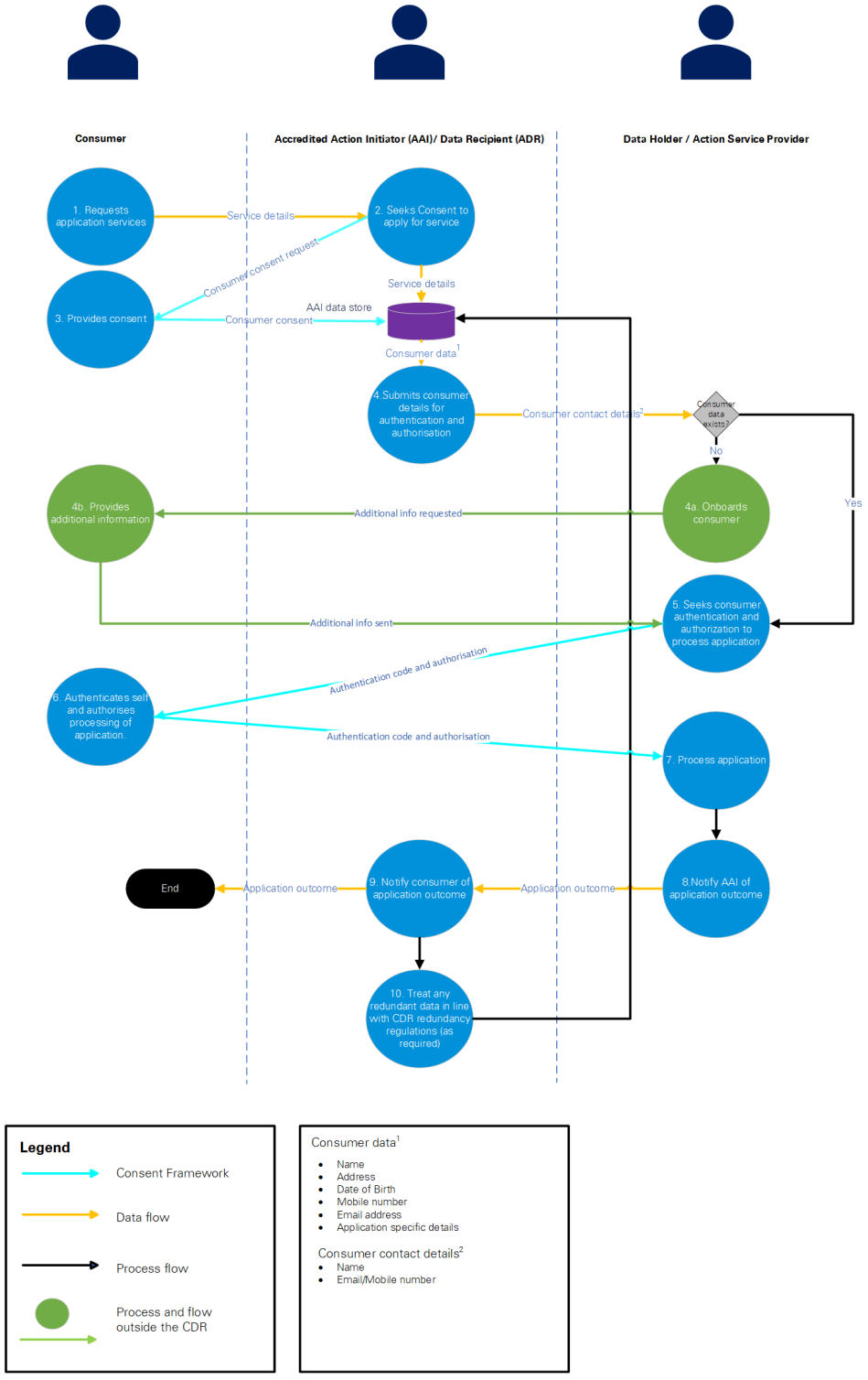
Use Case Description : Consumer uses AAI's services to set up standing instructions to transfer money between their accounts to maximise interest



3. Product/Service Application

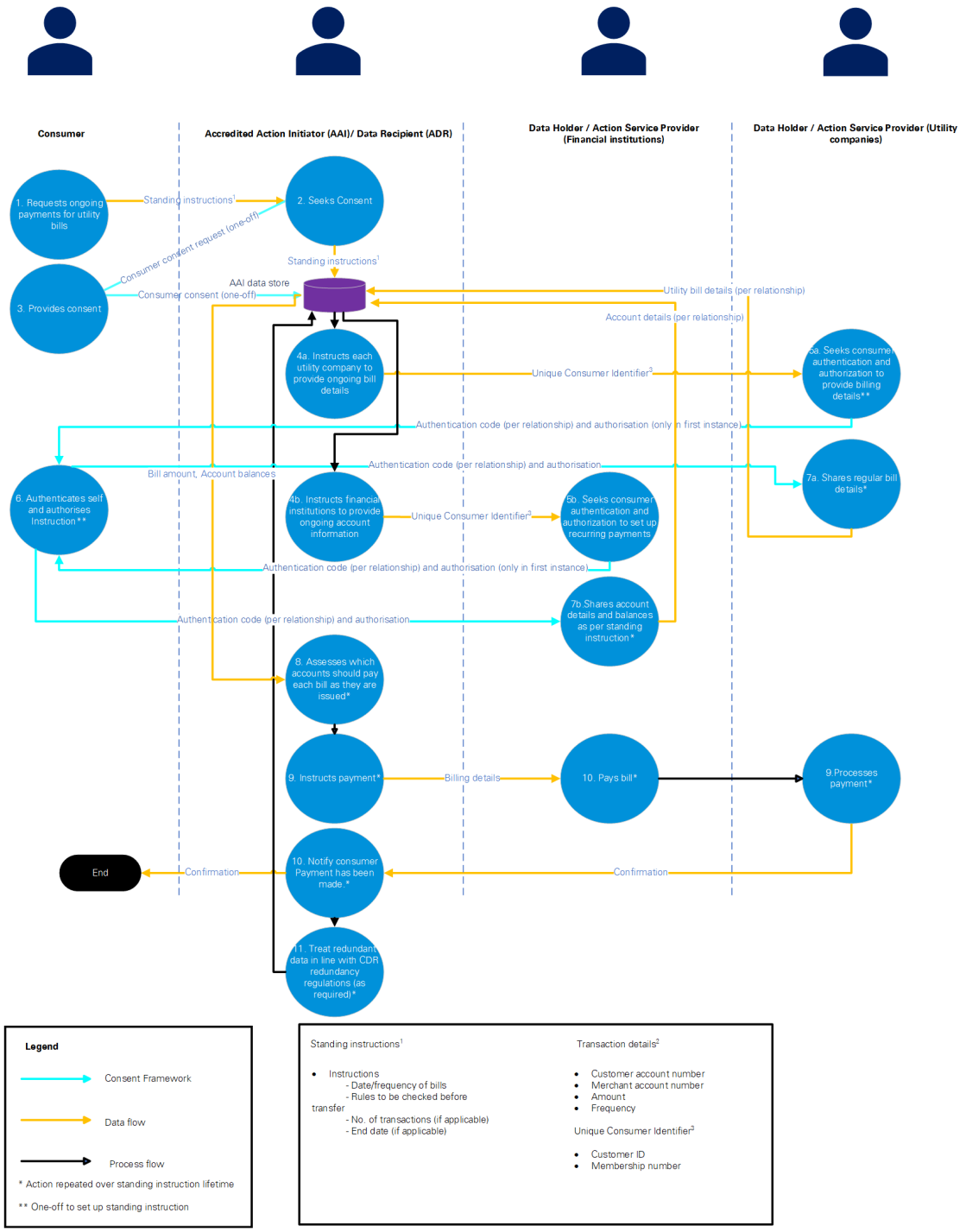
Use Case Description : Consumer uses AAI's services to apply for a product/service

Note: This service instruction may follow Use Case 8 – Comparison Services



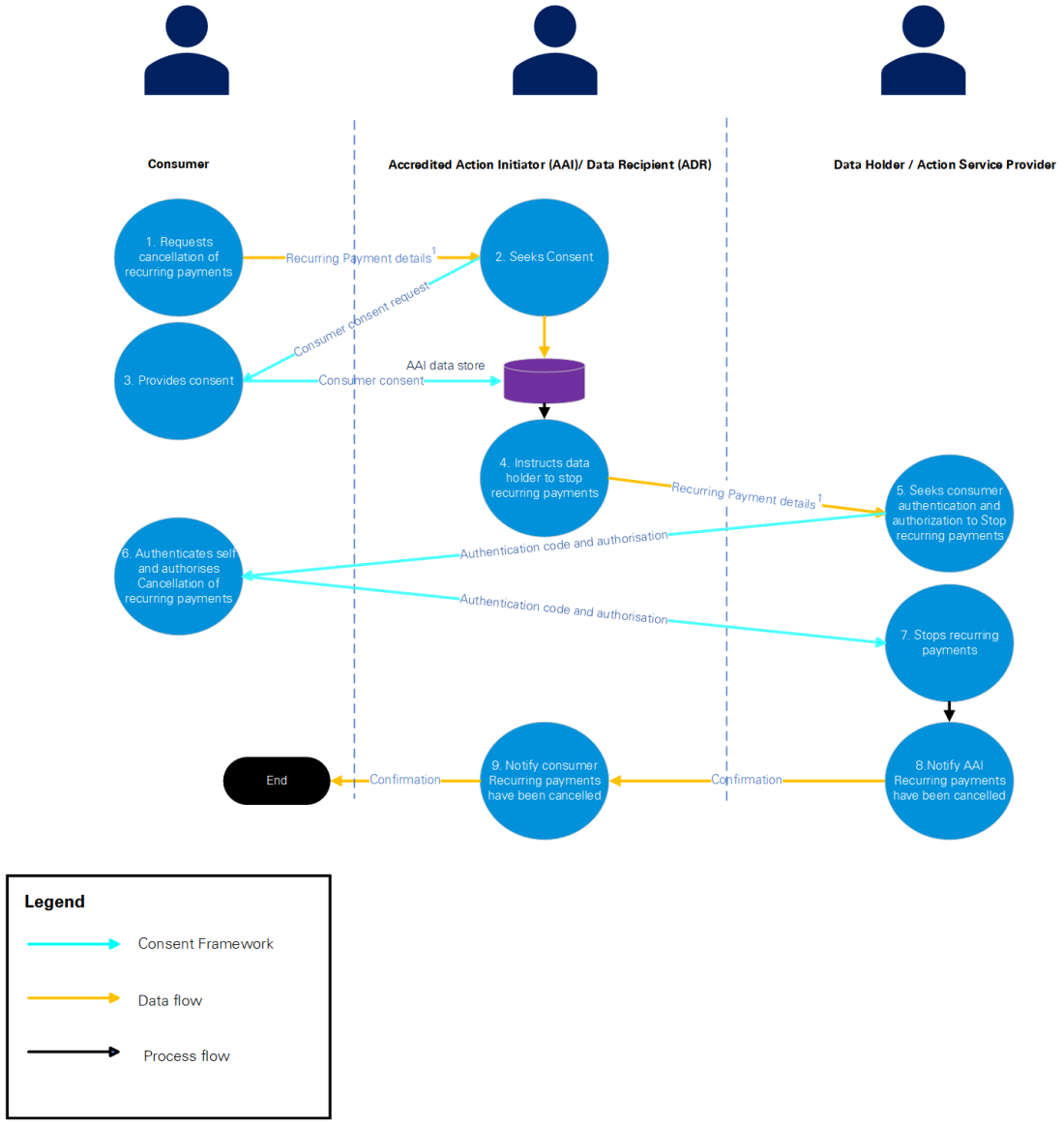
4.a Managing multiple variable payments, including recurring payments across multiple accounts

Use Case Description : Consumer uses AAI's services to set up standing instructions to arrange multiple variable ongoing payments between financial institutions and merchants



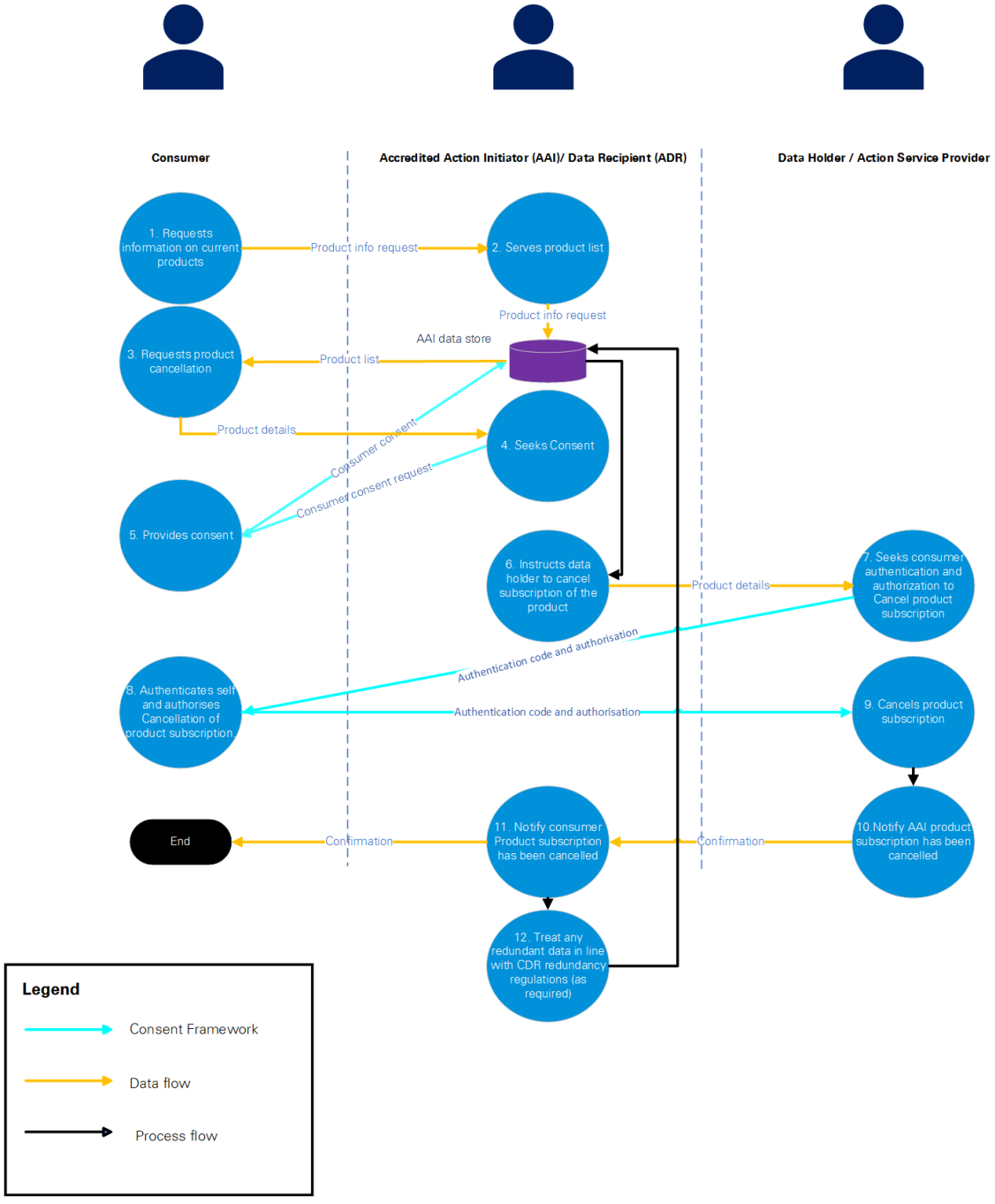
4.b Stops Recurring Payments

Use Case Description : Consumer uses AAI's services to stop recurring payments



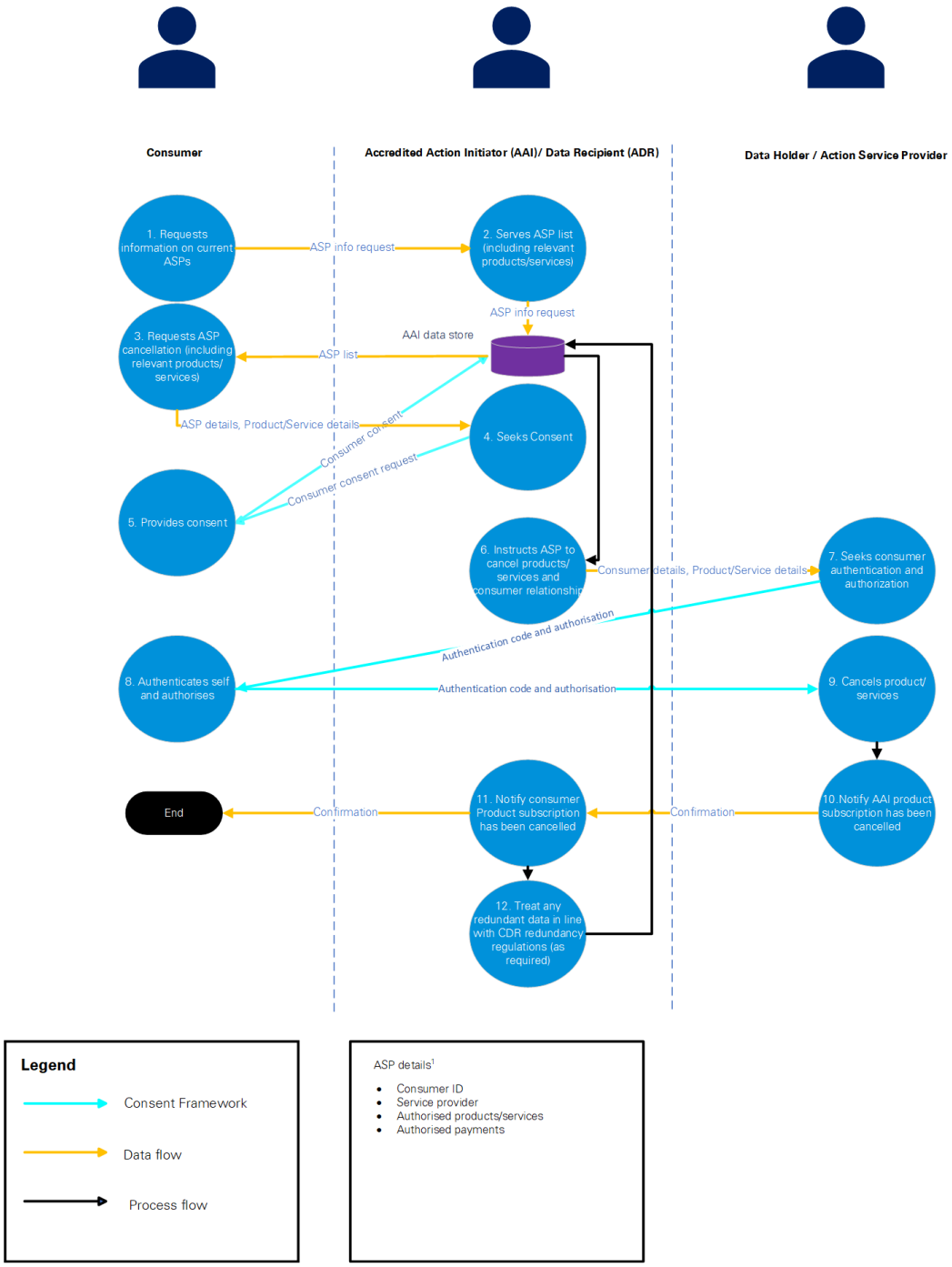
5.a Closing a Product

Use Case Description : Consumer uses AAI's services to cancel subscription of product



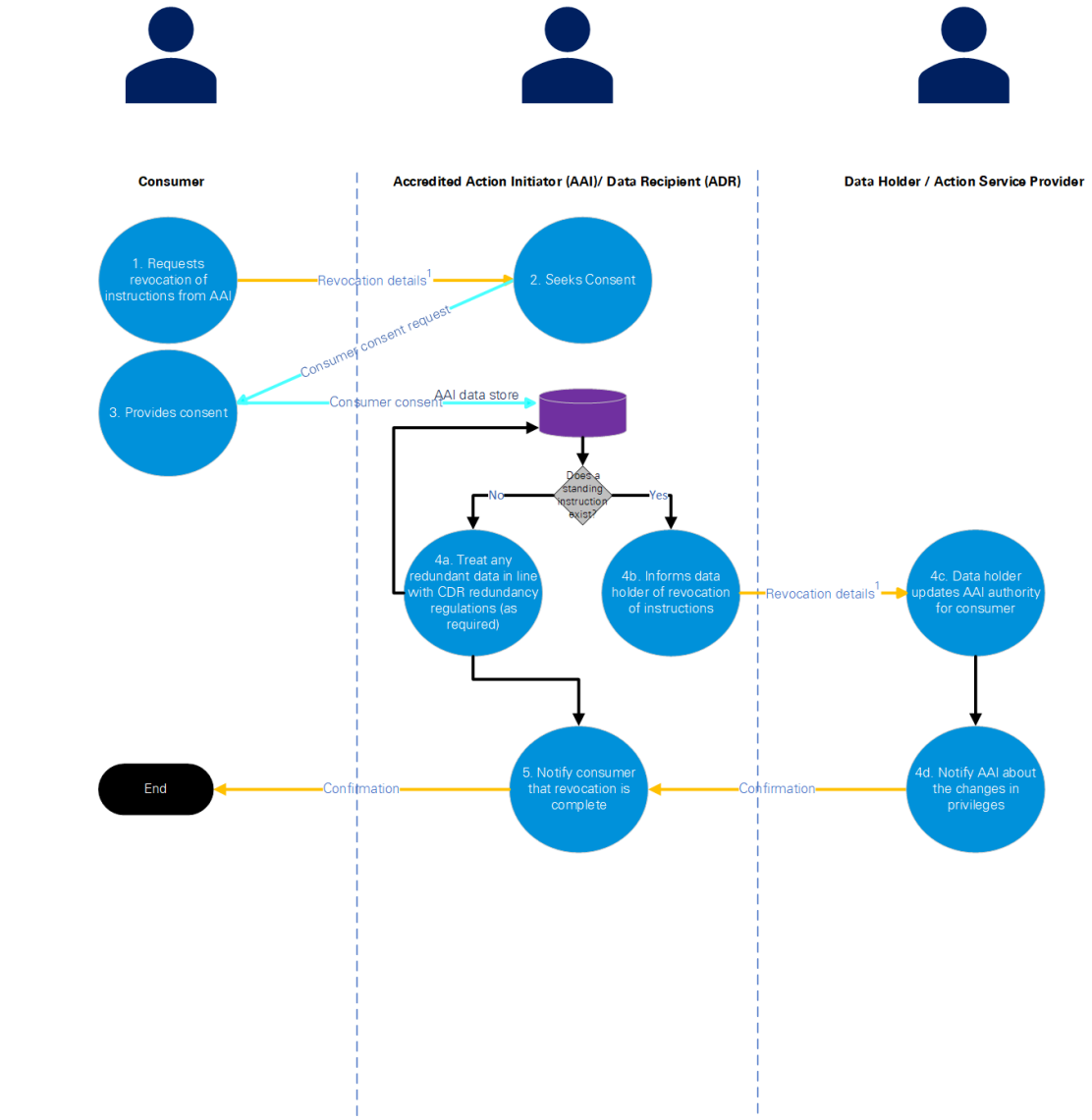
5.b Ending a Customer relationship

Use Case Description : Consumer uses AAI's services to cancel a relationship



6. Revocation of instructions from AAI

Use Case Description : Consumer revokes instructions from AAI



Legend

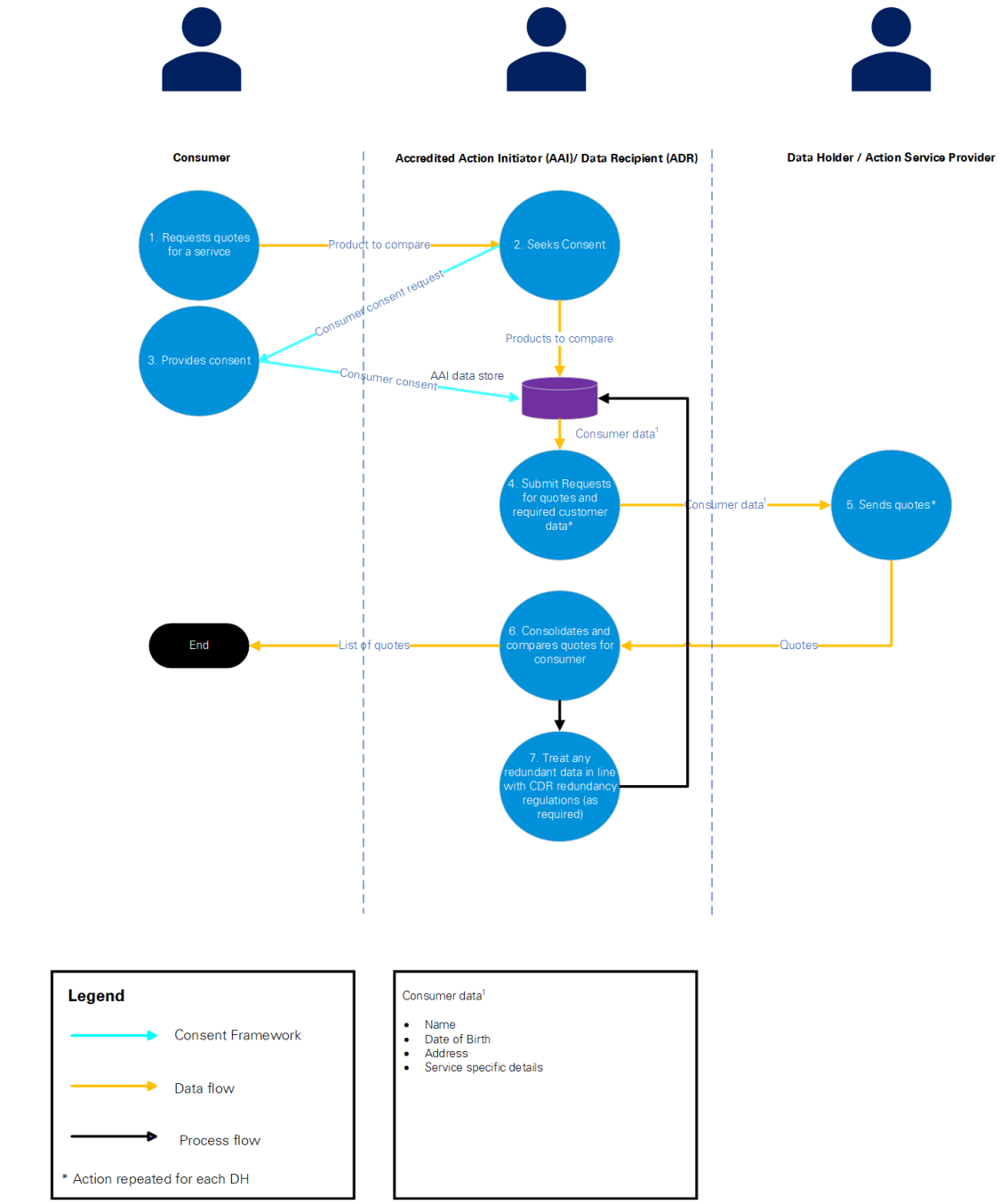
- Consent Framework
- Data flow
- Process flow

Revocation details[1]

- Account numbers
- Instructions
  - Date/frequency of action
  - Rules to be checked before initiating action
  - No. of transactions (if applicable)
  - End date (if applicable)

8. Comparison services

Use Case Description : Consumer uses AAI's services to compare services



Appendix 2: Glossary and Abbreviations

A: Glossary

Accredited Action Initiator means an entity that that is able to instruct an Action Service Provider to carry out actions on behalf of CDR Consumers.

Accredited Data Recipient has the meaning given to that term in section 56AK of the CCA.

Accredited Person means a person who holds an accreditation by the Data Recipient Accreditor (i.e. the ACCC) under subsection 56CA(1) of the CCA. This person and the ADR are the same person.

ACCC means the Australian Competition and Consumer Commission, which is responsible for, among other things, maintaining the Register of Accredited Person for the purpose of the CDR regime as set out in Part IVD of the CCA.

Action Layer means the actions executed and confirmed by an Action Service Provider in response to the instructions from an Accredited Action Initiator.

Action Service Provider means an entity required to act on a valid (action) instruction received from an Accredited Action Initiator.

Australian Consumer Law means Schedule 2 to the CCA.

Australian Privacy Principles means the Australian Privacy Principles in Schedule 1 to the Privacy Act.

CCA means the *Competition and Consumer Act 2010* (Cth).

CDR Consumer has the meaning given to that term in subsection 56AI(3) of the CCA.

CDR Data has the meaning given to that term in subsection 56AI(1) of the CCA.

CDR Participant has the meaning given to that term in subsection 56AL(1) of the CCA.

CDR Privacy Safeguard Guidelines means the version 1.0 guidelines issued by the OAIC in February 2020 in relation to how the Information Commissioner interprets and applies the Privacy Safeguards when exercising its functions and powers relating to them under Part IVD of the CCA.

CDR Rules means the *Competition and Consumer (Consumer Data Right) Rules 2020* made by the ACCC dated 10 February 2022.

Consumer Dashboard means:

a) in relation to an Accredited Person, an online service described in paragraph 1.14(1) of the CDR Rules; and
b) in relation to a Data Holder, an online service described in rule 1.13(1)(a) of the CDR Rules.

Consumer Data Request means a request for CDR Data as described in rule 1.4 of the CDR Rules.

Consumer Data Standards means the technical standards developed by the Data Standards Body which represent the current baseline for implementation of the CDR by the relevant participants.

Consumer Experience Guidelines means the consumer experience guidelines developed by the Data Standards Body to support the implementation of the CX Standards. See version 1.17.0, 21 July 2022.

Consumer Experience Standards means standards developed by the Data Standards Body in relation to consumer experience under rule 8.11 of the CDR Rules and may have binding effect under section 56FA of the CCA. See version 1.17.0, 21 July 2022.

Customer Provided Data means data provided by the CDR Consumer including name of account holder, contact details including billing address or postal address, and information provided about the property including appliances.

Data Holder has the meaning given to that term in section 56AJ of the CCA.

Data Minimisation Principle means a requirement that needs to be complied with by an Accredited Person and has the meaning given to that term in rule 1.8 of the CDR Rules.

Data Standards Body means the entity appointed under section 56FJ of the CCA. At present, this entity is the Department of the Treasury.

Data Recipient Accreditor means the person appointed under subsection 56CG(1) of the CCA. At present, this is the ACCC.

Declaration means the process whereby the Minister will identify and specify (in a declaration instrument) the types of actions that can be initiated by an Action Service Provider.

Derived CDR Data has the meaning described in subsection 56AI(2) of the CCA.

Designation Instrument means a statutory instrument designating a particular sector to implement the CDR regime.

Eligible CDR Consumer means a CDR Consumer that is described as such under the CDR Rules (in relation to a particular sector of the Australian economy).For action initiation, this could also mean an existing customer of an Action Service Provider, or a prospective customer (e.g., using the CDR action initiation process to set up a new account with an Action Service Provider.

Instruction Layer means the provision of instructions received from a consumer to initiate actions, between an Accredited Action Initiator and an Action Service Provider.

Personal Information has the meaning given to that term in the Privacy Act.

Privacy Act means the *Privacy Act 1988* (Cth).

Privacy Safeguards means the 13 privacy safeguards set out in Division 5 of Part IVD of the CCA for which the OAIC is responsible for administering.

Register of Accredited Persons means the register of Accredited Persons maintained by the Accreditation Registrar in accordance with Subdivision B, Division 3 of Part IVD of the CCA.

Treasury means the Commonwealth Department of Treasury.

Use Cases means the 9 sample use cases identified by KPMG in consultation with Treasury to support the mapping of data flows.

B: Abbreviations

Abbreviation	Definition
ACCC	Australian Competition and Consumer Commission
AAI	Accredited Action Initiator
ASP	Action Service Provider
ADR	Accredited Data Recipient
APP entities	Private sector 'organisations' that are subject to the APPs as they do not come under the 'small business' exemption as they an annual turnover of more than AUD $3 million and collect and hold personal information.
APPs	13 Australian Privacy Principles under schedule 1 of the *Privacy Act 1998* (Cth)
CCA	*Competition and Consumer Act 2010* (Cth)
CDR	Consumer Data Right
CDR Rules	*Competition and Consumer (Consumer Data Right) Rules 2020* (Cth) version 4
CX	Consumer Experience
DH	Data Holder
DSB	Data Standards Body
FD Report	Inquiry into the Future Directions for the CDR 23 December 2020
NDB	Notifiable Data Breaches
OAIC	Office of the Australian Information Commissioner
Open Banking	The designation and implementation of CDR in the Banking sector
PIA	Privacy Impact Assessment
Privacy Act	*Privacy Act 1988* (Cth)

Appendix 3: List of key publicly available materials reviewed

The following key materials were considered by KPMG for preparing this PIA.

a) *Competition and Consumer Act 2010* (Cth).

b) Consumer Data Standards and the latest CX Standards and Guidelines version 1.17.0.

c) OAIC's 'CDR data: What is 'CDR data'?' webpage.

d) OAIC's June 2021 version 3.0 Guidelines '*Consumer Data Right: Privacy Safeguard Guidelines*'.

e) OAIC's 5 May 2014 guide 'Guide to Undertaking Privacy Impact Assessments'.

f) *Privacy Act 1988* (Cth).

g) *Treasury Laws Amendment (Consumer Data Right) Act 2019* (Cth).

h) Treasury's October 2020 Report 'Future Directions for the Consumer Data Right'.

i) Treasury's December 2021 Report 'Government Response to the Inquiry into Future Directions for the Consumer Data Right'.

j) Treasury's 8 February 2021 (with analysis as at 29 September 2020) PIA 'Australian Competition and Consumer Commission: Consumer Data Right Regime: Update 2 to Privacy Impact Assessment'.

k) Treasury's 29 November 2019 (with analysis as at 23 September 2019) PIA 'Consumer Data Right Regime'.

l) Treasury's 29 October 2021 (with analysis as at 26 October 2021) PIA 'Consumer Data Right Regime: Update 4 Privacy Impact Assessment'.