UNSW SYDNEY

Risk Management for the Consumer Data Standards:

A Report to the Data Standards Chair

Lyria Bennett Moses, UNSW Sydney
Katharine Kemp, UNSW Sydney
Peter Leonard, UNSW Sydney
Rob Nicholls, UNSW Sydney

June 2022

Contents

Purpose Statement

About this report

The purpose of this report is to inform the Data Standards Chair in relation to their obligation in regards to risk management for the Consumer Data Standards, with a particular focus upon information security. It explains why a risk framework for the Data Standards is important and how it ought to be designed. It is not itself a risk framework, and therefore does not identify risks or explain how they might be mitigated. The report is based on an analysis of governance obligations in Australian law, in particular with respect to information security risk management. It describes processes to assess and allocate responsibilities in relation to risks in handling of confidential or sensitive information, with reference to applicable international standards.

This report was written in relation to a Statement of Requirements. Work on this report took place over the period 27 May 2022 to 30 June 2022, with changes made during consultation with the Department of the Treasury up to 31 March 2023.

Objectives

The objectives of this report are set out in a contract between University of New South Wales and the Commonwealth Department of the Treasury. The strategic intent is:

> *To develop an authentication and data payload risk framework for the Data Standards Chair to approve, and then use when making related Data Standards. In order to achieve this, the DSB requires advice on how such a framework should be constructed and operated.*

The contract required "research on frameworks and tools relevant to managing security risks that apply to authentication and payload Data Standards". We were instructed to focus on the obligations of the Data Standards Chair and risk management as it relates to the Data Standards.

The deliverable was to include:

1. analysis of relevant legislative and regulatory frameworks and any relevant international standards applicable to authentication and data payload Data Standards;
2. review of relevant artefacts, related to the above, that describe the impacts or consequences that may arise from Data Standards risks being realised;
3. recommendations to the Chair for an authentication and data payload risk framework and on how to operationalise such a framework.

Scope of the report

The focus of this research is on the relevant obligations of the Chair, who is also an official of the Treasury, and therefore subject to Commonwealth policy. This research is focussed on risk management as it relates to the Data Standards; risk management frameworks that do not directly relate to the Data Standards were not in scope. The *development* of a fit-for-purpose security risk management framework is not in scope for this report. A security risk assessment is also not in scope for this report.

Disclaimer

This report reviews general operation of laws and regulatory instruments and is provided solely for the benefit of the Data Standards Chair, and The Treasury. It does not constitute legal advice as to application of laws and regulatory instruments to particular fact scenarios or in particular contexts and should not be used as such. Formal legal advice should be sought in particular matters. While information in this report has been formulated with due care, the University of New South Wales and its subcontractors disclaim and exclude liability to any person (other than the Data Standards Chair, and The Australian Treasury) for use of information in this report.

Citation

This report should be cited as Lyria Bennett Moses, Katharine Kemp, Peter Leonard, Rob Nicholls, *Risk Management for the Consumer Data Standards: A report to the Data Standards Chair* (UNSW, 2022).

This report also benefited from significant contributions by Anna Johnston, Principal, Salinger Privacy, who was engaged by UNSW as a consulting expert.

Executive Summary

The Consumer Data Right (**CDR**) was established in Part IVD of the *Competition and Consumer Act 2010* (Cth) (**CCA, Pt IVD**) to enable consumers in progressively designated sectors,[1] commencing with banking, to authorise the sharing of information about them. As the CDR is rolled out in each sector, consumers are able to require information about them to be disclosed to accredited persons. There are different sources of regulation for the CDR, specifically:

- Pt IVD, which includes the Privacy Safeguards;[2]
- the CDR Rules (**Rules**) made by the Treasurer;[3] and
- the CDR Data Standards (**Data Standards**) made by the Data Standards Chair (**Chair**).[4]

The Data Standards are not legislative instruments, unlike the Rules, and therefore not subject to parliamentary control or scrutiny. Operation of Data Standards nevertheless has a significant impact upon the human rights of persons to whom CDR data relates and rights specifically conferred by the Consumer Data Right.

The Chair is a statutory appointment and also an official of the Treasury. The Data Standards Body (**DSB**) has the sole function of assisting the Chair. Treasury is designated as the Data Standards Body and has a dedicated team to understake this function.

Governance of risk, defined as the impact of uncertainty on objectives,[5] needs to be considered in the context of the Data Standards. Risk is inherent in a situation where a government creates standards with objectives including functionality, consent, security, privacy and customer experience, and relies upon businesses in the sectors to which CDR applies to implement those standards. Different categories of risk arise: security risks relate to the physical security of infrastructure, "insider" risks associated with personnel and "information security" risks to the confidentiality, integrity and availability of data.[6] Information security risks are significant in the context of Data Standards that facilitate automated flows of personal (and sometimes sensitive) information between organisations with differing levels of cyber maturity. Cyber security is a national priority, as illustrated through recent reforms of the *Security of Critical Infrastructure Act 2018* (Cth). Because cyber security of any system, let alone a complex multi-organisation system such as the CDR, is never perfect, it is essential to identify, assess and manage information security risks in order to enhance the trustworthiness and resilience of the CDR and protect consumer privacy. Data Standards, which set the conditions under which the data flows occur, are central to this.

Commonwealth policy provides an essential starting point for governance of risks relating to Data Standards, including the Commonwealth Risk Management Policy (**Risk Policy**) and the Protective Security Policy Framework (**PSPF**).[7]

There are a number of factors that make governing risks in the context of Data Standards critical, complex and hard. Critical, because there are significant threats to information security, generating risks to consumer privacy and the trustworthiness of the CDR regime.[8] Complex, because the risks are shared rather than associated with a single entity. Many information security and associated data handling risks arise through activities of CDR data participants that, while within the subject matter of Data Standards, are not directly controlled or managed by Treasury or other Commonwealth agencies. The application of the Risk Policy and the PSPF in this scenario is complex, and there are gaps and uncertainties in articulating the responsibilities associated specifically with the Chair and others. Risk governance in the context of Data Standards is also hard due to technical complexity and the diverse, evolving cyber security landscape across industries to which the CDR applies. The diverse range of entities handling CDR data across the cross-sectoral CDR system have widely diverging levels of maturity in implementing enterprise risk management, governance and assurance and, more specifically, in managing risks associated with confidential or sensitive consumer data, such as CDR data, and operating data environments in which that data is segregated and handled.

Having regard to the roles of the Chair and the Treasury in assuring safe use of CDR data and public confidence in the CDR system, this report suggests the Risk Policy and the PSPF should be applied in relation to the subject matter of Data Standards to address information security and associated data handling risks.

Given the role of the Chair in assuring safe use of CDR data and public confidence in the CDR system, this report suggests that a strategic approach to risk management should involve consultation with other CDR agencies and stakeholders.

FOR PUBLIC RELEASE

FOR PUBLIC RELEASE

Recommendations to the Data Standards Chair

1. **Critical - Make arrangements for risk governance for the Data Standards**. A strategic approach to risk management requires developing a Risk Management Framework that addresses the particular risks associated with Data Standards, including information security and associated data handling risks. A Risk Management Framework for Data Standards will fit under the umbrella of the Treasury Risk Management Framework, and any Consumer Data Right Risk Management Framework.

2. **Critical - Ensure that the Risk Management Framework for Data Standards incorporates requirements to comply with laws and government policy.**

    a. **Critical - Create binding Data Standards.** At the time of drafting this report, none of the Data Standards that have been issued specify that they are binding which, according to the Pt IVD and the Rules, means there are no binding Data Standards. The Chair is required to make *binding* Data Standards in respect of eight categories of CDR matters. The legal consequences of making binding or non-binding Data Standards differ in terms of enforceability and hence impact. Without binding Data Standards, there is a potential gap between expectations as to the consistency of safe handling and use of CDR data and enforceability of obligations that underpin public confidence in the CDR system, and the actual legal obligations of data participants and powers to enforce these.

    The Data Standards Chair should, to comply with Pt IVD and the Rules and address expectations as to consistently safe handling and use of CDR data that underpin public confidence in the CDR system, issue *binding* data standards.

3. **Critical - Ensure that the proposed Risk Management Framework for Data Standards aligns with accepted methodologies, such as that in ISO/IEC 27005 for security risk management, and incorporates an understanding of the context of the Data Standards.**

    a. **Recommended – Ensure that the Risk Management Framework deals adequately with risks shared with participants in the CDR, including those related to the operational processes and practices of Accredited Data Recipients when handling CDR data.** A Risk Management Framework for Data Standards might assist in assessment and allocation of Shared Risks that, if not appropriately mitigated, may lead to loss of confidence in the CDR and thereby undermine its take-up and use. To ensure the trustworthiness of the CDR, Shared Risks to the privacy of CDR data (including derived data) should be addressed.

    b. **Recommended – Ensure that the Risk Management Framework deals adequately with risks shared with other CDR agencies and CDR participants, including risks relating to (1) threats of inappropriate and unauthorised handling of CDR data by CDR participants including the unauthorised dissemination of data outside the CDR ecosystem and (2) external threats.** Privacy Safeguards, Rules and Data Standards focus more heavily on information security risks associated with external threats than operational risks of inappropriate and unauthorised handling of CDR data, for example those caused by inadequate or failed internal processes, people or systems. Data Standards may assist with assessment, mitigation and management of both categories of risk, including through measures that assure linkage between the scope and quality of data consents and the specification of operational processes and practices as implemented by Accredited Data Recipients.

    c. **Recommended - Ensure that a Risk Management Framework for Data Standards facilitates development of common use cases.** A risk-based approach to Data Standards would assist assessment of how and where risks of inappropriate and unauthorised handling and disclosure of CDR data may be addressed through close linkage between (1) the scope and quality of data consents tailored to particular use cases, and (2) specification of attributes of operational processes and practices that recipients implement for those particular use cases.

    d. **Recommended – Relevant parts of the Risk Management Framework for Data Standards should be shared with CDR participants.** Most importantly, operating a Risk Management Framework that is aligned with appropriate Standards would allow for eco-system participants to collaborate on Shared Risks. This would ensure that the context of risk management is communicated, that information on threats, vulnerabilities and controls may be standardised and shared, and that the possible impacts and harms to CDR consumers and eco-system participants are uniformly considered. This includes the impact on trustworthiness of the CDR, and willingness of consumers to provide further relevant consents.

4. **Critical – As part of the Risk Management Framework for Data Standards, consider their impact on consumer and human rights, particularly in the context of the impact on privacy of the collection, use and disclosure of CDR data and the importance of transparency in data handling.** The Data Standards have a substantive impact on consumers' human rights, particularly the right to privacy. This is managed through the central place of consent in the CDR. However, the effectiveness of consent depends on the information and choices consumers are presented with and the extent to which consumers are permitted to minimise the CDR data disclosed to recipients. These are matters dealt within the Data Standards. This is in contrast to the common misperception of the Data Standards as 'mere' technical specifications. The Data Standards impact human rights, particularly the right to privacy and the right to equality and non-discrimination. Trustworthiness of the CDR as a whole is contingent on a human rights-based lens (particularly in relation to the right to privacy) and awareness of the importance of maintaining a social licence to operate. Risks to human rights and consequential risks should be considered within the Risk Management Framework for Data Standards.

5. **Recommended – As part of the Risk Management Framework for Data Standards, ensure that Privacy Impact Assessments (PIAs) are conducted as required.** Triggers for requiring a fresh PIA should include: the on-boarding of new sectors; the on-boarding of new data types; any new functionalities or features; and as part of the development process for new or significantly amended Data Standards. We recommend that a PIA be conducted on draft Data Standards associated with each such expansion of the CDR scheme. The PIA should take a deliberately broad, holistic, 'scheme-wide' view, rather than focus on only one element such as the Data Standards. The PIA should consider which of the risks can be resolved through careful crafting of the Data Standards, versus applying other levers. Future PIAs should also include a review of which recommendations from previous PIAs were not followed or implemented, and why, helping to ensure that nothing has 'slipped through the cracks' over time.

1. Introduction

This report provides external expert advice to the Data Standards Chair (**Chair**) in order for the Chair, in collaboration with the Secretary of the Department of the Treasury (**Secretary**) as Accountable Authority, to consider the best approach to meet their respective obligations for risk management in the context of the Data Standards.

The report presents three challenges - developing a Risk Management Framework with respect to Data Standards is **critical**, **complex** and **hard**.

The task is critical because of the role of Data Standards in the context of the Consumer Data Right (**CDR**). Data Standards instruct private sector actors, in designated sectors (such as banking), how to transfer personal and sensitive consumer data in particular circumstances. To adopt a metaphor, the Data Standards are the rails on which data moves around the CDR ecosystem. CDR data is sensitive, both inherently (as in the case of financial data) and because of what might be learnt from it (as where energy data is used to deduce household activities). A rich picture of individual lives, compromising privacy and facilitating identity theft, exclusion and manipulation, can increasingly be drawn from data circulating in an expanding CDR ecosystem.

There are threats, including malicious actors who seek to use or manipulate data to benefit other nation states or raise money through cybercrime. A separate report – the UNSW Threat Report[9] – on the role of threat modelling in identifying threats has been prepared simultaneously with this report. Findings in the UNSW Threat Report provide an important motivation for developing a comprehensive approach to identifying and managing risk, as discussed in this report.

UNSW Threat Report

The UNSW Threat Report reached the following conclusions on the landscape of Threat Actors that could impact the CDR:[10]

- Large scale attacks against systems of significance, such as CDR, will be attempted by many Threat Actors particularly advanced persistent threats such as nation state actors and organised cybercriminals.
- APIs are foreshadowed to become a significant target for Threat Actors. Threat Actors will target API data security across the CDR and the areas most exposed are in the transport, authentication, insecure coding, and input validation of the API requests.
- Data security across the CDR will be influenced by the data lifecycle and data handling behaviours of CDR participants. Many organisations are pursuing additional insights from data using artificial intelligence. Each of these derivative data processes, and any parties that CDR data is shared with, will create potential new means for threats against the CDR. This is one example of dynamic emerging threats that must be continually monitored and assessed in order to maintain confidence in the overall data security state of the CDR.
- As less mature organisations begin to enter the CDR ecosystem, new security threats will transpire for all parties involved. One challenge that must be managed is the security measures and culture that smaller, less cyber mature entities will have, or rather the potential that they will have limited security and threat management capabilities.
- The frequency of cyberattacks is increasing at a rapid rate and is outpacing the ability to upskill and hire cybersecurity resources. The potential inability of CDR participants to employ security personnel to effectively monitor security systems and controls could impact the CDR's reputation and consumer confidence where a data breach eventuates. This will be particularly felt when a breached entity could have reduced a threat through analyst monitoring, or effective security control configuration.
- API security is likely to pose challenges from numerous Data Holders, ADRs and other parties in the CDR ecosystem. A number of parties will struggle to understand their APIs and their purpose within the environment. Complexities will also arise where the product and services developed by CDR participants rely on multiple APIs or where APIs are not fully supported within an organisation.

The task is also time-critical given current plans to expand the scope of the CDR, both in terms of sectors to which it applies and in terms of functionality. If anything, it has been delayed for too long as illustrated by a statement by the ACCC in 2019[11] that a security risk assessment is "mandated". This security risk assessment, which does not seem to have taken place, was intended to be conducted by a specialist team, and was to lead to a threat model on the basis of vulnerability, or penetration tests, that were to be conducted. An information security review of the Data Standards also recommended development of a Risk Management Framework;[12] this was also not done.

The task of establishing a fit-for-purpose Risk Management Framework is also complex. As explained in further detail in Section 4.2.1 of the Report, it is not always simple to identify the entity responsible for identification and mitigation of risks addressed by Data Standards. The nature of the DSB places primary obligations for developing the risk management system on the Accountable Authority of the Treasury, being the Secretary. Many of the risks associated with the Data Standards, however, are shared with other parts of government (such as the Australian Competition and Consumer Commission (**ACCC**) and Office of the Australian Information Commissioner (**OAIC**)) and also with industry participants who hold, send and receive data through the CDR ecosystem. These participants handle this data in accordance with the settings in the *Competition and Consumer Act 2010* (Cth) (CCA), the *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth) (Rules) and the CDR Data Standards (**Data Standards**). The complexity is fourfold.

First, the Commonwealth is establishing information security controls - in terms of the Data Standards - for use by industry. The Commonwealth is also establishing information security controls for industry through the *Security of Critical Infrastructure Act 2018* and related policy guidance, which is promoting the Commonwealth's Information Security Manual (**ISM**) as a baseline standard. The role of the Commonwealth in setting these controls via the functions and powers of the Chair, however, is unprecedented, and it is not specified how the Chair should engage with the ISM.

Second, the role of the Accountable Authority in terms of applying the Protective Security Policy Framework (**PSPF**) for the context of the Data Standards is similarly unprecedented. Although the PSPF proclaims itself as the basis for protecting people, information and assets from security threats, and there are threats to consumer data that the Data Standards seek to mitigate, the language of the PSPF tends to focus on the people, information and assets of *Commonwealth entities*. Therefore, there is a lack of a conceptual framework for how the Secretary should apply the PSPF in the context of activities of non-government entities where those activities are regulated in part by Data Standards.

Third, the nature of the risks addressed by the Data Standards means they are shared across Commonwealth entities, industry and consumers. The Commonwealth Risk Management Policy (**Risk Policy**) states that, *Accountability and responsibility for the management of shared risks must include any risks that extend across entities and may involve other sectors, community, industry or other jurisdictions.* And that, *Each entity must implement arrangements to understand and contribute to the management of shared risks.* Therefore, the public consultation undertaken during the development of the Data Standards can, and should, be harnessed for this purpose. The requirements for a fit-for-purpose Risk Management Framework, however, means that this public consultation would need to be incorporated into an acceptable security risk management practice that meets relevant Commonwealth requirements.

Fourth, the ISM and the PSPF focus upon identification and mitigation of risks to confidentiality and integrity of data arising from activities of motivated unauthorised intruders. The ISM and the PSPF also expect entities to address the threat of unauthorised access to data environments by trusted insiders. However, the ISM and the PSPF focus upon perimeter controls, and detection of unauthorised activities compromising those perimeter controls, and not upon assessment and mitigation of risks that trusted insiders allow derived data to exit controlled data environments, outside of the scope of authorisations conferred upon an entity as to permitted scope and purpose of uses and disclosures of data. Although this risk of unauthorised use or disclosure may be characterised as an information security risk, data risk management controls built to implement the ISM and the PSPF are likely to focus upon data security (cyber) risk. This means they will not appropriately address and mitigate risks of unauthorised uses or disclosures by trusted insiders that arise from mismatch between (1) scope of permissions conferred by consumer consent, and (2) actual uses and disclosures of CDR data (and particularly, derived CDR data and insights), that arise from gaps or shortcomings in operational processes and practices for handling of that CDR data. Those gaps or shortcomings may include failures by data participants to appropriately assess and control uses of derived CDR data and insights that fall outside the reasonable expectations of CDR consumers as informed by their consents, or which lead to algorithmically enabled adverse impacts upon how a particular CDR consumer is treated relative to treatment of other consumers.

1. Introduction (continued)

The complexity becomes particularly difficult to manage given that developing a Risk Management Framework for Data Standards is hard, requiring specific expertise in the context of and the technical parameters within Data Standards. Security risk management as articulated in the PSPF not only requires an understanding of the Data Standards themselves and the role they play, but also of the broader strategic, operational and security risk management contexts.[13] The contexts change over time as more data moves through the CDR ecosystem (compounding the severity of potential harm) and the international threat landscape evolves. The contexts also vary for each sector joining the CDR ecosystem due to differing levels of cyber maturity, varying data sensitivity, and diverse threat contexts. In particular, entities in the CDR ecosystem exhibit widely diverging levels of maturity in implementation of enterprise risk frameworks. This includes different capacity to manage risks associated with handling of confidential or sensitive consumer data, such as CDR data, and operation of data environments in which that data is segregated and handled. This challenge is compounded by the relatively early stage of development of global standards as to governance roles in data management.

Because a fit-for-purpose security risk framework for the Data Standards is critical, we make specific recommendations as to how the complexity and difficulty can be managed. We describe what needs to be done, not only urgently in the short term, but also over time as the CDR, the surrounding context, and the threat landscape for the Data Standards all evolve.

The Chair was originally envisaged as the person responsible for ensuring appropriate governance, process and stakeholder engagement for the DSB.[14] While ultimate authority now rests with the Secretary, the Chair remains responsible for the day-to-day management of risks associated with decisions in relation to Data Standards. Our report is addressed to the Chair, but it recognises that the Chair will need to collaborate with other relevant stakeholders, including the Secretary, in order to implement our recommendations. As is clear from the Risk Policy (discussed in more detail in Section 4.1.2), Shared Risks require shared oversight and management, thus collaboration will also be required with other stakeholders, both within government and among CDR participants.

This report is organised as follows: Our recommendations are set out in the Executive Summary. In addition, a Summary of each section appears boxed at the beginning of that section. The substance of our analysis is contained in Sections 2-7.

- Section 2 analyses the role, status and impact of the Data Standards in the context of the CCA and the Rules. It is associated with Recommendation 2(a) and provides essential background for Recommendation 4.
- Section 3 explores the link between Data Standards and trustworthiness. It provides important background for Recommendations 3(a), 3(b), 3(c), 3(d).
- Section 4 sets out the requirements under applicable risk governance policies. It is associated with Recommendation 1.
- Section 5 provides guidance on developing a Risk Management Framework. It is associated with Recommendations 2, 3, 3(a), 3(b), 3(c).
- Section 6 analyses the importance of privacy in a Risk Management Framework for Data Standards. It is associated with Recommendation 4.
- Section 7 discusses Privacy Impact Assessments. It is associated with Recommendation 5.

2. The Role, Status and Impact of Data Standards

1. There is a hierarchy of regulation under which the provuisions of Part IVD of the *Competition and Consumer Act 2010* (Cth) (**Pt IVD**), which include Privacy Safeguards, prevail over the Rules and the Rules in turn prevail over the Data Standards.
2. Data Standards may be binding or non-binding. The consequences of a Standard being binding rather than non-binding are that it becomes enforceable as a contractual term between accredited recipients and the ACCC or an aggrieved person can bring proceedings in the Federal Court for breach of the Data Standard.
3. The Rules currently require the Chair to make binding Data Standards in respect of eight categories of CDR matters, including authentication, security, and processes for obtaining consent, and providing consumers with certain critical information.
4. A Data Standard is only binding if the Data Standard itself specifies that it is binding, as required by the Rules. **Currently none of the Data Standards specify that they are binding, so there are no binding Data Standards**.
5. The Data Standards are not a legislative instrument.
6. The fact that the Data Standards are therefore not subject to Parliamentary control or scrutiny caused concern at the time Part IVD was passed, but was explained on the basis that the Data Standards are largely technical, highly specialised, frequently revised and subject to the Rules.
7. As a matter of law, a statement of compatibility with human rights is not required for the Data Standards because they are not legislative instruments, but the Data Standards themselves nonetheless have an impact on human rights, including the right to privacy and the right to non-discrimination.
8. Despite the common perception of the Data Standards as 'mere' technical specifications, the **Data Standards have a substantive impact on consumers' rights**, including through their role in determining what information and choices consumers are presented with and the extent to which consumers can minimise the CDR data disclosed to recipients.
9. The Future of the CDR Inquiry Report proposed significant reforms to the CDR, such as action initiation. This would be built on the existing foundations of the CDR and the Data Standards, making it even more important for these to be supported by an appropriate Risk Management Framework.
10. The Future of the CDR Inquiry Report also made recommendations that would increase the influence and impact of the Chair, the DSB and the Data Standards, across the broader digital economy. These include using the DSB as a source of expertise in developing data standards for other regulatory regimes; the DSB developing a minimum assurance standard for authentication, including Risk Taxonomy and Risk Matrix; and alignment of other accreditation regimes with the CDR regime.

2.1 Legislative structure and the CDR scheme

The CDR was established in Part IVD to enable consumers in progressively designated sectors,[15] commencing with banking, to authorise the sharing of information about them. As the CDR is rolled out in each sector, consumers are able to require information about them to be disclosed to themselves or to Accredited Data Recipients (**ADRs**). The scheme also provides for greater access to information in the relevant sectors that does *not* relate to any identifiable or reasonably identifiable consumers.[16] There are different sources of regulation for the CDR, specifically:

- Pt IVD, which includes the Privacy Safeguards;[17]
- the Rules made by the Treasurer;[18] and
- the Data Standards made by the Chair.[19]

There is essentially a hierarchy of regulation under which the statutory provisions including Privacy Safeguards prevail over the Rules to the extent of any inconsistency, and the Rules prevail over the Data Standards to the extent of any inconsistency.[20] The Chair must comply with Pt IVD and the Rules when making, varying or revoking components of the Data Standards.

Central to the CDR is the category of 'CDR data', defined in s 56AI. Classes of information are designated when a new sector is designated. Such information, as well as information wholly or partly derived from such information (including derivations of derivations), is 'CDR data'. For the banking sector, the classes of data designated include information about the consumer or their associate, information about the use of a product by a consumer or their associate, and information about a product.[21] Each element of CDR consumer data is linked to a CDR consumer being the identifiable (or reasonably identifiable) person to whom it relates because of the supply of a good or service to that person or an associate. CDR data is not always personal or sensitive because it does not always relate to a CDR consumer. For example, in banking, it can include product reference data. However, CDR data that relates to CDR consumers are often sensitive.

In essence, the CDR scheme requires incumbent suppliers that hold CDR data in respect of a consumer (**Data Holders**) to transfer CDR data to certain third parties upon the consumer's request, with the goal of permitting those third parties to use that data for the consumer's benefit in providing some service or offer expressly requested by the consumer. These might include, for example, comparison services; budgeting products; alternative offers on personal loans, home loans or energy plans. To receive CDR data in this way, the third party must generally meet legislated requirements in order to be accredited by the ACCC as an ADR.[22] Consumer CDR data might also be transmitted, with consumer consent, to a nominated third party Trusted Adviser.

2.2 Evolving the CDR

Identity of the DSB.
The entity to whom the functions of the DSB are allocated has relatively recently changed from a quasi-independent corporate entity (CSIRO[23]) to a central Australian Government Department (Treasury). This means, for instance, that the DSB and the Chair are now bound by the Australian Government Agencies Privacy Code which makes PIAs mandatory for any changes which may have 'high privacy risks'.[24] As discussed in 4.1.1, this change also impacts on the applicability of the *Public Governance, Performance and Accountability Act 2013* (**PGPA Act**).

Expanding sectors.
The coverage of the Data Standards will soon expand beyond banking and energy to other sectors. This will require entirely new categories of Data Standards, which will pose different risks from those associated with Data Standards that have been created to date. New sectors come with new kinds of data sensitivity.

Future directions and growing impact.
The previous government stated its intention to implement reforms in future that would expand the functionality of the CDR to include action initiation by third parties and leverage CDR infrastructure to support the broader digital economy, increasing the impact of the scheme for both CDR consumers and potentially others well beyond the CDR scheme. In January 2020, the then Treasurer announced an Inquiry into Future Directions for the CDR, which was asked to make recommendations to expand the CDR's functionality. Following the publication of an issues paper and extensive consultation, the Inquiry provided its Final Report dated October 2020[25] and the previous government published its Response to the Final Report in December 2021,[26] broadly endorsing the findings of the Inquiry.

Most significantly, the Inquiry recommended that CDR should enable third parties to initiate actions (known as Action Initiation) beyond read-only requests for data sharing. For example, a consumer could consent to the initiation of payments on their transaction account.[27] The then government agreed with this recommendation for Action Initiation, which would first be rolled out in the banking sector, with the prioritisation of bank account-to-account payment initiation, following a designation process with thorough regulatory and privacy impact assessments.[28]

The Inquiry recommended that Action Initiation through the CDR should be based on existing consent, authentication and authorisation processes, with appropriate amendments.[29] By leveraging the existing legal framework for the CDR, compliance burdens for Action Initiation would be minimised.

> The fact that such significant future reforms would be built on the current foundations of the CDR and the Data Standards makes it all the more important for these foundations for consent, authentication and authorisation to be supported by a fit-for-purpose Risk Management Framework at the outset.

The Risk Management Framework should therefore also be amended over-time in order to incorporate additional risks associated with any extensions to the CDR.

The Inquiry's Report also recommended that the government leverage CDR infrastructure to support the broader digital economy, including making the DSB available as a source of expertise in developing and maintaining data standards that other Government initiatives, regulatory regimes and information technology systems could adopt. The then government agreed that, while the DSB should continue to focus on CDR implementation, it should also provide specialist advice as required and where appropriate on other government data initiatives. The then Government also agreed with the recommendation in the Final Report that the DSB should develop a minimum assurance standard for authentication, including a Risk Taxonomy and Risk Matrix.[30] It noted recommendations that being accredited in the CDR regime should be equivalent to being accredited under other regimes, so that efforts should be made to align similar data safety 'accreditations', stating that it supports reducing the burden for industry.

> These proposals made clear the potential for the DSB, the Chair and the Data Standards to have influence and impact well beyond the CDR regime.

2.3 Data Standards: Binding vs non-binding

Under Part IVD, the Chair has the power to make certain Data Standards.[31] The Chair is also *required* to make certain Data Standards.[32] The Chair is required to make a Data Standard if this is required by the Rules.[33] Rule 8.11(1) sets out eight categories of Data Standards that the Chair must make. Data Standards may cover a wide range of matters, such as processes for providing notices to and obtaining consent from CDR consumers; the manner of describing and clustering of CDR data that may be requested; authentication methods; and de-identification processes.

There are two types of Data Standards in terms of their legal effect: binding and non-binding.

A Data Standard is binding if it meets two conditions:

- it must be a Data Standard which the Chair has the power to make under CCA s 56FA(1), and
- the Chair must specify in the Data Standard that it is binding if the Rules require the Chair to specify it is binding.[34]

According to the Rules, there are eight categories of Data Standards that the Chair must make. The Rules state that all eight categories of Data Standards are Data Standards that the Chair must specify to be binding.[35] To be clear, the Rules do not provide that certain Standards *are* binding, but require that certain Standards themselves should specify that they are binding in order to become binding Standards under CCA s 56FA(1).

We have not been able to locate any standards that specify they are binding. If this is correct, it means that **there are no binding Data Standards** according to the meaning given to that term in CCA s 56FA(1) and the Chair has not complied with Rule 8.11[36] and therefore CCA s 56FA(2),(3)[37] in this respect.

The legal effect of binding Data Standards is that they effectively become contractual terms in a contract that is taken to exist between the Data Holder and each accredited person (and between any designated gateway and the Data Holder and accredited person).[38] The ACCC or an aggrieved person can also make an application to the court in respect of breach of a binding Data Standard, and the court may make orders in respect of compliance with or enforcement of the binding Standard.[39] If there are no binding Standards, there are no such contractual terms or rights of action in respect of binding Data Standards.

The second category of Data Standards is **non-binding Data Standards**. Part IVD and the Rules do not give explicit guidance about the legal effect of non-binding Data Standards. Some Rules specifically require compliance with a Data Standard in respect of certain details. If a Data Standard is non-binding, the effect of non-compliance with the Standard will depend on the nature of the Rule that requires compliance with the Standard. Accordingly, while non-binding Data Standards cannot be directly enforced by the ACCC or by a Data Holder as a contractual term, they may be indirectly enforced where the relevant Rule requires compliance with that Standard and:

- the Rule is a civil penalty provision,[40] or
- the Rule relates to the Privacy Safeguards or to the privacy or confidentiality of CDR data.[41]

Another legal effect of the Data Standards relates to the protection from liability for accredited participants. In particular, accredited participants will not be liable to an action or other proceeding in relation to the provision of CDR data, or access to it, if the participant provides the data or access in good faith in compliance with Pt IVD, the regulations and the Rules.[42] The protection from liability provision does not specifically refer to Data Standards (binding or non-binding), but it may be possible to argue by extension that a participant complying with Data Standards referred to in the Rules would be protected from liability on the basis of this provision (given its reference to compliance with Part IVD and the Rules).[43]

2.4 Human rights and the absence of scrutiny

In this section, we set out the lack of a requirement to prepare a Statement of Compatibility (**SoC**) that would explain the impact of the Data Standards on human rights, explain why the Data Standards should be assessed within a human rights framework, and suggest a mechanism by which this might be done.

2.4.1 Absence of Parliamentary scrutiny or control over Data Standards

The fact that Data Standards are not subject to Parliamentary control or scrutiny was an issue raised by the Senate Scrutiny of Bills Committee[44] at the time Part IVD was passed.[45] The Committee expressed concern that:

> *Although the explanatory memorandum explains that the data standards will cover largely technical matters, the committee notes that the power to make such standards is not so limited: the data standards could potentially cover a number of significant matters relating to the management of CDR data.*

The Committee stated its expectation that:

> *a sound justification be provided for the use of non-disallowable standards, especially where those standards may potentially be addressing significant matters and could affect large classes of persons (as the standards may do as a result of proposed sections 56FD and 56FE). The explanatory memorandum provides no such justification.*

In response, the previous Treasurer advised the Committee, and it was noted by the Committee, that the data standards were 'highly technical and specialised' and were subject to frequent, high-volume revisions. The previous Treasurer illustrated with reference to the work on the draft Standards:[46]

> *Data61 prepared large volumes of draft data standards, much of which are comprised of, or closely resemble, computer programming code. Data61's log of changes identified almost 40 revisions to the draft standards between December 2018 and July 2019.*

Further, the previous Treasurer explained that the ACCC was able to impose limits and controls on the making of Data Standards under the Rules and that the Data Standards could not be inconsistent with the Rules. The Committee accepted this justification of the Data Standards' status as a non-legislative instrument and did not pursue the matter further.

The new Government may choose to take a different position, including for the reasons set out in Sections 2.4.3 and 2.4.4.

2.4.2 Human rights and the absence of a legislative instrument

According to the *Human Rights (Parliamentary Scrutiny) Act 2011* (Cth), a proposed bill or disallowable legislative instrument must be accompanied by a Statement of Compatibility (**SoC**), regardless of whether human rights are impacted by the bill or legislative instrument.[47] While the Rules are a disallowable legislative instrument, [48] the Data Standards are not a legislative instrument.[49] Accordingly, an SoC is not required for the Data Standards as a matter of law.

The Parliamentary Joint Committee of Human Rights has sometimes expressed concern about the absence of SoCs for instruments that fall outside section 42 of the *Legislation Act*, such as non-disallowable legislative instruments.[50] This concern might justifiably be extended to Data Standards since there are human rights which may be significantly affected by the Data Standards, particularly the right to privacy and rights to equality and non-discrimination.

Article 17 of the International Covenant on Civil and Political Rights (**ICCPR**) provides that:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

The rights of equality and non-discrimination are contained in articles 2, 16 and 26 of the ICCPR. The Convention on the Rights of Persons with Disabilities (**CRPD**) also sets out the protections and reasonable accommodations that must be provided to ensure that

2.4 Human rights and the absence of scrutiny (continued)

persons with disabilities are able to participate fully in all aspects of life, including the conduct of their financial affairs and accessing information.[51] While persons with disabilities have an equal right to control their financial affairs, measures relating to the exercise of legal capacity must also provide for appropriate and effective safeguards to prevent abuse.[52]

These human rights are significantly impacted by the CDR. By way of example: (1) Data Standards related to accessibility (or any lack thereof) might lead to a failure to make reasonable accommodations for consumers with impaired vision to facilitate their access to the CDR; (2) Data Standards may fail to incorporate proportionate safeguards to prevent abuse of measures relating to the exercise of legal capacity; (3) Data Standards may fail to provide sufficient protection from information security risks, resulting in loss of privacy. In relation to the first example, the DSB is already engaged in work to determine relevant accessibility obligations and conventions for the Chair. That work, together with recommendations in this report that focus on how a Risk Management Framework ought to approach privacy risks, have the potential to support the human rights of consumers participating in the CDR.

2.4.3 Perception of Data Standards as mere technical specifications

From the time the CDR legislation was passed, there has been a general policy position that the Data Standards do not have the same significance for consumers' substantive rights as Pt IVD and the Rules. The Data Standards have been explained as flexible, technical specifications aimed at ensuring the functionality of information technology solutions. The Explanatory Memorandum stated that:[53]

> *The [D]ata [S]tandards will be largely in the nature of specifications for how information technology solutions must be implemented to ensure safe, efficient, convenient and interoperable systems to share data. They will only describe how the CDR must be implemented in accordance with the rules which will set out the substantive rights and obligations of participants.*

It continued:[54]

> *These information technology specifications will be living documents subject to continual change, in order to adapt to changing demands for functionality and available technology solutions. … It is designed to ensure maximum flexibility at the level of the[D]ata [S]tandards.*

As noted above, despite initial concern about the fact that Data Standards are not subject to Parliamentary control,[55] the Senate Scrutiny of Bills Committee accepted the previous Treasurer's justification that the Data Standards were 'highly technical and specialised', frequently revised and subject to the Rules. The fact that the Data Standards are technical, however, does not mean that their impact on, and alignment with, human rights are less important.

2.4.4 Data Standards impact consumers' substantive rights

The matters addressed by the Data Standards, in accordance with the Rules, do in fact affect the substantive rights of consumers in ways that are particularly relevant to individuals' right to privacy. This is because the Rules leave it to the Standards to determine how Data Holders and ADRs interact with consumers in significant respects, including what information and options are presented to consumers in the process of sharing their CDR data. If the Data Standards result in consumers receiving inadequate or even misleading information, or inappropriately restricted options, this has serious consequences for consumers' privacy as well as their trust in the CDR scheme.

The manner in which the Chair makes Data Standards may also affect whether participants have certain rights of redress under the CDR scheme. For example, if as a matter of law none of the existing Data Standards are binding Data Standards, this will mean the ACCC cannot directly enforce those Standards and the Standards will not become contractual terms within a contract between Data Holders, ADRs and/or Gateways.[56]

The following discussion provides examples of specific ways in which the Data Standards themselves can have a significant impact on the privacy of individual consumers by affecting the accuracy of information provided to consumers about CDR data practices, the choices allowed to consumers in respect of their privacy and CDR data, and consumers' trust in the system.

Anonymity and pseudonymity

The Data Standards affect consumers' ability to interact anonymously or pseudonymously with ADRs.[57] The Data Standards on notice and consent processes shape the user interface that ADRs present to consumers, the information requested from consumers who are considering sharing their CDR data and how requests are made.[58] This can affect the stage at which the consumer may be required by the ADR to provide their legal name and contact details and whether the consumer can interact anonymously or pseudonymously when appropriate. For example, a consumer could be inappropriately prevented from interacting with an ADR anonymously or pseudonymously if the interface requires them to, or seems to indicate that they must, provide these identifying details before they can obtain all the information necessary to make a decision about the ADR's service and their data practices.

Data minimisation principle

The Data Standards affect the degree to which the data minimisation principle can be adhered to in that the Data Standards determine the types, description and clustering, of data to be used in making or responding to requests.[59] An ADR must not seek to collect CDR data from a consumer unless the CDR consumer has requested this by giving a valid request under the Rules.[60] However, the Data Standards determine the minimum amount of data the consumer can request a Data Holder to share with an ADR, even if less data is required for the consumer's purposes. Therefore whenever data cluster(s) specified by the Data Standards are too broad, for a given use case, this would undermine the data minimisation principle, and therefore unnecessarily expose consumers' personal data.

Notice of data practices

The Data Standards have an impact on the extent and accuracy of notice provided to consumers about the ADR's data practices, given that the Rules require compliance with the Standards on notice.[61] The Data Standards therefore influence the ADR's user interface (including consumer dashboard)[62] and notices to consumers, including by reference to the Customer Experience (**CX**) Guidelines.[63] Examples of potentially misleading statements are provided in Box 1:

Box 1: Examples of potentially misleading statements in user interface

The Data Standards influence the ADR's user interface and notices to consumers, including through the consumer dashboard.

For example, the Data Standards (through the CX Guidelines)[64] indicate that the ADR should include in its user interface among 'Key things you should know' the statement that 'You can choose to delete shared data we no longer need'.[65] This has the potential to mislead consumers if, for instance, the ADR exercises its statutory option to de-identify the data and sell it to a third party.[66] **The consumer is unlikely to understand that the ADR could still exercise this option to de-identify and sell the data before it becomes redundant**.

Similarly, the recommendation of a notice to consumers that 'We don't sell your data to anyone' could be misleading if the ADR will commercially exchange the data with third parties other than by way of sale, or if the data can be acquired as part of a merger, or if the ADR sells or otherwise discloses the data once it is de-identified as permitted by the Rules.[67]

It is important to consider both the insights the DSB has obtained about consumers' attitudes to deletion versus de-identification of CDR data (including preferences for deletion), and comments by the Federal Court[68] and the ACCC[69] about potentially misleading information in privacy notices and settings.

The Chair should consider the insights the DSB has obtained about consumers' attitudes to deletion versus de-identification of CDR data (including preferences for deletion). It is also important for the Chair to consider comments about the potential for privacy notices and settings to mislead consumers by the Federal Court of Australia,[70] and in the ACCC Digital Platforms Inquiry Final Report.[71]

2.4 Human rights and the absence of scrutiny (continued)

Consent to data practices

The Data Standards have a critical role in determining the quality of consumer consent. ADRs must obtain this consent as a precondition to receiving CDR data from a Data Holder.[72] Consent is also required where CDR data is shared with Trusted Advisers. Data Standards for the consent process and the user interface affect:

- the kind of action required by consumers for valid consent (eg, whether consumers must scroll through the terms before indicating consent, or click on one of two equally clear and neutral options);
- the extent to which consent for different purposes is specific and unbundled;
- the kind of consent necessary for joint accounts; and
- whether consent to CDR data access effectively becomes a precondition of service depending on the stage and manner in which a manual option is presented to the consumer (eg, if the consumer can only discover the manual alternative after they press 'Cancel').

The design of user interfaces is not merely a matter of 'form rather than substance'. Research on consumers' behavioural biases and designs that intentionally or unintentionally exploit these reveals how matters of design can prevent consumers acting in accordance with their own preferences and interests. User interface designs that are 'intended to confuse users, make it difficult for users to express their actual preferences, or manipulate users into taking certain actions' are known as 'dark patterns'.[73]

De-identification process

The de-identification process for CDR data is not currently determined by the Data Standards. However, according to Part IVD and the Rules, this is one of the topics that may be addressed by the Data Standards, and accordingly this type of Data Standard could become relevant in future.[74] To the extent that any such de-identification process fails to prevent re-identification of purportedly de-identified data, this is likely to substantially undermine consumer trust in the CDR scheme as a whole, underscoring the need for a Risk Management Framework to manage such risks before Data Standards regarding de-identification are created.

At present, the de-identification process for CDR data is contained in the Consumer Data Rules,[75] and requires the ADR to consider several matters, including the De-identification Decision-making Framework (**DDF**) published in 2017 by the OAIC and CSIRO's Data61,[76] in determining whether it is possible to de-identify the data. There is no link between the DDF and technical requirements found in information security standards commonly used in industry (such as those set out at 4.1.5). This creates risks that data will be treated as 'de-identified' (and thus unregulated) when it could in fact be re-identified (and thus threaten privacy rights). The DDF does not adequately mitigate this risk.

The de-identification process for CDR data has great significance for consumers' privacy, given that the legislation permits ADRs to choose to de-identify (rather than delete) the consumer's data and sell it, even without the consumer's consent in some cases.[77] While there is an ever-present risk of re-identification which should be well-known to the DSB and ADRs,[78] many consumers would not be aware that this risk persists.

An incident which led to the re-identification of CDR data would be likely to have very negative consequences for consumers' trust in the CDR scheme as a whole, particularly given that consumers have no choice as to whether ADRs de-identify the consumer's CDR data and disseminate it to third parties.[79]

Security

Consumers' privacy also depends on the implementation of appropriate security measures to protect the CDR system and CDR data from improper access and/or attack by internal and external actors. Such security breaches could lead to significant harms to consumers, including harms from identity theft, fraud, blackmail, discrimination and humiliation.

The Data Standards clearly impact consumers' privacy due to their influence on the security of CDR data,[80] in light of encryption and authentication specifications.

These examples demonstrate that it is unsafe to treat the Data Standards as 'merely' technical and practical, given the potential for the Data Standards themselves to have a substantive impact on consumers' rights.

We would therefore question the current characterisation of the Data Standards because they extend well beyond "computer programming code" and technical specifications, and have a substantive impact on consumers' human rights. This could lay the foundation for the inclusion of human rights compatibility assessment as part of the Risk Management Framework.

2.5 Options in response to the role, status and impact of Data Standards

Without binding Data Standards, there is a potential gap between expectations as to the consistency of safe handling and use of CDR data, the enforceability of obligations that underpin public confidence in the CDR system, and the actual legal obligations of data participants and powers to enforce these. The Chair should issue binding Data Standards, to comply with the Act and the Rules and address expectations as to consistently reliably safe handling and use of CDR data that underpin public confidence in the CDR system.

Because Data Standards have a substantive impact on consumers' human rights, particularly the rights to privacy, equality and non-discrimination, an assessment of the impact of the Data Standards on consumers' human rights should be incorporated in the Risk Management Framework for Data Standards. This assessment should incorporate the same elements as a statement of compatibility with human rights, and could take advantage of the tools provided by the federal Attorney-General's Department for the assessment of the compatibility of instruments with human rights.[81] This recommendation is made with the caveat that incorporation of this assessment in the Risk Management Framework could not be regarded as equivalent to SoCs provided in respect of legislative instruments, since the latter are subject to Parliamentary scrutiny and oversight.

Further, the Chair should consider whether it is appropriate to advocate for certain future Data Standards to be contained in a legislative instrument, with Parliamentary scrutiny and formal SoCs. For example, the Final Report of the Future Directions Inquiry recommended that the Chair be given power to set certain Data Standards in respect of proposed Action Initiation functionality. It will be important for the Chair to consider the appropriate characterisation of such future Data Standards, having regard to their potentially substantial impact on human rights.

3. Data Standards and Trustworthiness

1. Aside from legal requirements, acceptance of the CDR scheme will depend on its trustworthiness, which depends critically on constraints on how the CDR data is collected and used, the transparency of data handling for consumers, and the security of CDR data.
2. A Risk Management Framework for Data Standards can assist in assessment and allocation of Shared Risks that, if not appropriately mitigated, may lead to loss of confidence in the CDR and thereby undermine its take-up and use.
3. For the CDR to be trustworthy, the Risk Management Framework for Data Standards needs to: (1) ensure clear allocation of responsibility for risk to the entity/ies and role or function within that entity/ies best placed to address each risk; and (2) ensure those responsible for each risk can assess and mitigate those risks through their own processes and practices or through clear and understood allocation to other entities.
4. It is not clear whether data breaches due to gaps or shortcomings in an ADR's, or Trusted Adviser's, operational processes or practices after CDR data is safely delivered to the ADR, or Trusted Adviser, ought to be included in a Risk Management Framework for Data Standards. On the one hand, this could be considered out of scope. On the other hand, such breaches may lead to a loss of confidence in the CDR itself, particularly as consumers could associate those data breaches with their participation in the CDR and the benefits they sought to derive from that participation.

   We recommend that the Risk Management Framework for Data Standards include allocation and assessment of Shared Risks associated with the operational processes and practices of ADRs and Trusted Advisers for handling CDR data, including derived CDR data and insights.

5. We consider how, and why, a Risk Management Framework for Data Standards might facilitate development of use cases that might be used for standardisation as to solicitations for consent, and forms of consent, that are tailored to be appropriate to a particular use case, and assured by specification of operational processes and practices for handling of CDR data (including derived CDR data and insights) specific to execution of that use case.

3.1 Trustworthiness of the CDR

Section 56AA of the CCA states an object of the CDR as:

… to enable consumers in certain sectors of the Australian economy to require information relating to themselves in those sectors to be disclosed safely, efficiently and conveniently (1) to themselves for use as they see fit; or (ii) to accredited persons for use subject to privacy safeguards.

For sustainable take-up and use of the CDR, the CDR needs to be regarded by consumers and by data participants as reliably and verifiably safe. Confidence in a system that is complex, and therefore not commonly understood, flows from the widely held perceptions that the system is safe to use.

There are four key attributes of "safe" use of the CDR system.

- Firstly, there is **prior consumer consent**: fully informed unambiguous prior express consent provided by a CDR consumer before a CDR request is initiated.
- Second, a **request that is made is within scope of consent and justified**: the request is only for such CDR data as is within the scope of that authorisation, and complies with the data minimisation principle. In particular, the data requested should be the minimum necessary for the particular use proposed to the consumer.
- Third, there are **secure pathways and data environments**: the request is made using a secure pathway, and responsive CDR data is communicated using a secure pathway and received into a secure data environment controlled by an ADR or other entity for whom an ADR is responsible and accountable.
- Fourth, **subsequent handling is only within scope of consent**: after receipt of CDR data, subsequent handling, use and any disclosure of CDR data (including derived CDR data and insights) by an ADR, or Trusted Adviser, and other entities acting under its control or direction, is only as is within the scope of that consent.

Safe disclosure of CDR data to accredited persons for use subject to Privacy Safeguards, as contemplated by the stated object in section 56AA of the CCA, should display each of those four attributes.

The fourth attribute, that subsequent handling is only within scope of consent, requires data management by the service provider that obtained the relevant consent to reliably and verifiably assure that handling, use and any disclosure of CDR data (including derived CDR data and insights) by an ADR or Trusted Adviser, and other entities acting under its control or direction, is only within the scope of prior consumer authorisation.

The CDR regulatory framework includes two types of measures to assure 'safe' use of the CDR:

- accreditation of CDR data recipients, including ongoing attestation as to existence and adequacy of controls to effect compliance with mandated safeguards and statutory requirements, and
- standardisation through the Rules and Data Standards as to requirements for solicitations for consumer consents, CDR data requests, and responsive disclosures.

CDR participants and consumers will rely on different indicators in making decisions as to whether to rely on the CDR.

Individual CDR participants (as insiders within the CDR system) should understand the required attributes of solicitations for consumer consents and valid consumer consents. Through the combined operation of accreditation, Rules and Data Standards, a Data Holder that receives a facially valid CDR data request and accordingly is legally required to provide a responsive disclosure is effectively required to make assumptions as to compliance by the initiator of the request. In addition, business incentives may promote trustworthy behaviour by individual data participants: in particular, the risk that if a particular participant is deceptive or engages in unauthorised data practices, the participant will suffer adverse reputational effects and associated business damage.

At a high level, consumer confidence in the CDR system is a function of whether CDR consumers collectively read and understand a solicitation for consent that they are being asked to give. CDR consumers may simply assume that the CDR system is safe to use. However, the position is more complex.

The CDR regulatory framework enables consumers to assume trustworthiness of the CDR system despite the fact that the operation of the system remains largely opaque to them. A consumer is unlikely to consider the nature of the CDR ecosystem or the nature or extent of regulatory measures to assure 'safe' use of the CDR and whether those measures are reasonably effective. Many consumers are unlikely to wish to (or have the *capacity* to) read and understand a CDR policy or other lengthy explanation by a service provider of Privacy Safeguards, Rules, and Data Standards through which the legislature and regulators intend to assure safe handling of CDR data.

This is not, of itself, a criticism as to design of the CDR regulatory measures or of the lack of engagement of consumers in management of risks that they activate through provision of consent. However, it is important to recognise that as a result of the legislature and regulators implementing the CDR regulatory framework and promoting use of the CDR system, consumers and consumer organisations develop a reasonable expectation that the CDR regulatory framework will reliably operate to assure, over time and across industry sectors, safe handling of CDR data.

To the extent that the consumer engages in understanding why the consumer's consent to CDR data sharing is being sought, it is likely to be by reading the text of the actual form of consent and closely adjacent explanations of a service provider's statement of purpose(s) for obtaining CDR data and how that CDR data will be used to the benefit of the consumer. Consumers are unlikely to consider attributes or characteristics of data sharing, beyond a limited evaluation of whether a service provider's statements in a form of consent and closely adjacent explanatory text about attributes of a product or service and the purpose of its provision corresponds to the consumer's understanding as to (1) the data input needs, as stated by the service provider, of an offered product or service, and (2) the output characteristics, as stated by the service provider, of that offered product or service.

Solicitations for consent, and the form of consent, may be overly broad, and may rely upon consumer behavioural economics and 'dark patterns' to 'game' provision by consumers of overly broad consents. Although the data minimisation principle requires a solicitation and form of consent to request to be limited to CDR data is "reasonably needed … in order to provide the goods or services requested by the CDR consumer", that requirement is to be construed in the context of a service provider's characterisation of their product or service, and may also be supplemented by "any other purpose consented to by the CDR consumer". This creates risk that a service provider's statement in the solicitation for consumer consent:

1. about the nature of the goods or services is overly broad, thereby broadening the scope of CDR data "reasonably needed to provide the relevant product or service", and
2. as to "any other purpose" is overly broad, and thereby what CDR data is "reasonably needed" is determined by reference to an overly broad statement of purpose or multiple purposes.

For these reasons, the consumer experience as to presentation of solicitations for consent, and as to the form of consent, is important to reducing risks of service providers obtaining overly broad consents.

3.2 The role of a Risk Management Framework for Data Standards

A Risk Management Framework for Data Standards might address development of use cases that could be used for standardisation as to solicitations for consent, and forms of consent, that are tailored to be appropriate to a particular use case, and assured by specification of operational processes and practices for handling of CDR data (including derived CDR data and insights) specific to execution of that use case. This may lead to dual benefits of better quality of consents, and mitigation of risk of occurrence of out-of-scope uses or disclosures by a service provider. In other words, a Risk Management Framework for Data Standards might facilitate development of risk assessments of common use case scenarios that simplify linkage between (1) solicitations for content and forms of consent, and (2) specification of use case specific technical, operational and contractual controls and safeguards as to operation of data environments, and releases from those data environments, that mitigate risks of uses or disclosures by a service provider that are outside the confines of reasonable expectations of a consumer as informed by a readily understandable consent.

A Risk Management Framework for Data Standards that facilitates development of risk assessments of common use case scenarios should also reduce risk of system-wide loss of confidence in the CDR system upon occurrence, or recurrence, of incidents of failures of controls, or other out-of-scope uses or disclosures of CDR data. Implementation of risk assessments of common use case scenarios mitigates risk of occurrence of incidents, and increases the possibility that when incidents occur within implementations of that use case:

1. root cause analysis can more readily determine the cause,
2. remediation can be effected across similar implementations within that use case, and
3. impacts upon confidence in the broader system may be contained.

If risk assessments of common use case scenarios are not implemented, many consumers may not accept root cause analysis of individual incidents. They will then be unlikely to accept conclusions that failures are limited to individual transactions or transactors. After-the-event remediations based upon learnings from failures may not be accepted by many consumers as mitigating risk of reoccurrence of failures that undermined consumer trust in the system. Isolated or outlier cases may therefore result in contagion effects for levels of consumer trust across the system and in the system itself that are very difficult to contain and reverse.

A Risk Management Framework for Data Standards that facilitates development of risk assessments for common use case scenarios also enables transaction types that are likely to involve ADRs, and Trusted Advisers, with lower levels of data maturity. Such ADRs, and Trusted Advisers, would be assisted to implement safe data environments with use-case-specific technical, operational and contractual controls and safeguards as to operation of those data environments and evaluation criteria for decisions as to whether releases from those data environments are safe.

Finally, a Risk Management Framework for Data Standards that guides development of use cases where confidentiality and integrity of data is assured by specification of operational processes and practices for handling of CDR data (including derived CDR data and insights) specific to execution of that use case enables the diversity in use-cases to be better addressed. Information security risks associated with external threat vectors are less diverse and accordingly are more readily risk managed through generic (system-wide) and relatively detailed and prescriptive information security safeguards as specified in Schedule 2 of the Rules, and the requirement for implementation of associated security controls, with associated attestation reports. Further, because generic (system-wide) information security safeguards do not address management of data environments to mitigate risks that CDR data may be used outside the scope of consumer consent, specification and testing of controls for attestation reports may not detect deficiencies in management of data environments that enable out-of-scope uses.

3.3 The limits of trust in sectors and organisations

Consumers' perceptions about the trustworthiness of a particular system do not simply depend on the sector in which that system operates or the data privacy and security record of that sector as a whole. Nor does existing consumer use of an organisation's services necessarily indicate consumer trust in that organisation. The reasons for this are explained in this section. The following section explains why consumers' perceptions about trustworthiness depend especially on the particular project and use case.

The level of trust Australians place in an organisation to handle their personal information does depend in *part* on the type of organisation itself. The OAIC's regular surveys into community attitudes towards privacy reveal that the most trusted organisations are health service providers and financial institutions. However, these two sectors also had the *worst* record in terms of the number of notifiable data breaches.[82] All sectors suffered a significant lessening of trust from 2013 to 2020.[83] The organisations with the lowest level of trust are social media companies. Some businesses with the lowest level of customer trust, including Facebook/Meta, remain in business.

Clearly, simply asking whether a *sector* is trusted is not giving us the full picture. This is for two reasons.

First, trust in a sector as a whole does not necessarily correlate with *use* of a sector as a whole. Individuals cannot really choose not to engage at all with the banking sector or the healthcare sector, let alone avoid engaging with government.

Second, gaining a social licence to use data is far more nuanced than simply a matter of checking that a particular organisation or brand enjoys an underlying level of trust. Instead, it is necessary to look at a multiplicity of factors which impact on whether any particular *project* will have a social licence to operate.

3.4 Attitudes vary by project and use case

Community attitudes towards privacy are heterogenous, but attitudes also vary greatly between projects, depending on the *use case* on offer.

A multi-year, eight-nation research project by the World Economic Forum and Microsoft sought to measure the impact of context on individuals' attitudes towards privacy and the use of their personal information.[84] The findings from this research are outlined in more detail in *Appendix 3A*. Two of the insights from the research are particularly pertinent to considering consumer trust in the CDR scheme and accredited participants.

First, there are four factors which influence an individual's degree of trust in any given proposal to use their personal information: (1) the situational context; (2) demographics; (3) culture; and (4) perceptions. However, for the most part, the Chair, the DSB and accredited participants will only have control over the first of those four factors: the situational context, which is the proposed data-related project or data handling scenario. Or in other words, the use case.

Interestingly, the single most important variable affecting the 'acceptability' of a scenario was not the type of data at issue, the way it was proposed to be used, the type of organisation or institution seeking to use it or even the pre-existing level of trust enjoyed by the particular organisation proposing the project – **but the method by which the personal information was originally *collected***. In the case of the CDR, the focus would be on how the relevant range of personal information was collected by the ADR and any subsequent recipients, as a result of the CDR.

An individual's ability to control how his or her personal information may be used depends on both an awareness of the collection and control over that collection. As awareness and control over the point of collection lessen, so too does confidence in the subsequent use of that data. Consumers' understanding of how personal information is *collected* therefore becomes critical to understanding the likely community expectations around the *use* of that data.

Second, **trust in data-related projects is specific to the use case and the design of each project**, as well as the type of customers to be affected, far more than it is about underlying levels of trust in particular organisations or sectors.

Aside from the fairness of and constraints on data handling under the CDR scheme, the degree of transparency provided to consumers about that data handling will have a significant impact on the perceived trustworthiness of the scheme. Qualitative research conducted in New Zealand on behalf of the Data Futures Partnership found that being transparent about how data is proposed to be used is a crucial step towards community acceptance.[85] This includes transparency about who will use the data, for what purposes and to whose benefit; as well as choices available to the consumer on access, correction and the ability of the organisation to sell or otherwise disclose their data.

The answers to those questions will be different for every project and have almost nothing to do with the pre-existing level of trust enjoyed by any particular entity or brand. Therefore the question is not whether consumers trust Treasury or the ACCC or any given accredited participant, but whether the CDR system and each participant's proposal for the use of CDR data have been designed to incorporate the elements needed to make those projects *trustworthy.*

Accordingly, it is important to create the Data Standards within a Risk Management Framework designed to manage risk appropriately having regard to consumers' expectations,[86] rather than relying on consumer trust in the financial sector or in government in general. This will aid in optimising participation by consumers in the CDR system by improving the trustworthiness of the CDR system itself and participants' proposals for use of CDR data.

4. Risk Governance

1. The primary government policies for risk governance are the PGPA Act, the Risk Policy and the PSPF.
2. These require Risk Management Framework(s) for the activities of the Department of the Treasury. This includes risks relating to decisions to issue Data Standards and the content of those Data Standards and Shared Risks with other entities in the CDR ecosystem. Primary responsibility for this lies with the Secretary as Accountable Authority.
3. The Chair is responsible for day-to-day management of risk as an official. The Chair's responsibilities in this regard are ongoing and intertwine with their respective duties of care and diligence and to act honestly, in good faith, and for a proper purpose.
4. We recommend a Risk Management Framework for Data Standards. This should align with Treasury's Risk Management Framework. It should include allocation for the responsibility for risks associated with Data Standards to officials with sufficient expertise in this area.
5. There are some ambiguities in the application of the PSPF to Data Standards, and advice might be sought from the Attorney-General's Department in relation to these.
6. Given the CDR is subject to Gateway Reviews, advice might also be sought from the Digital Transformation Agency (**DTA**) on the application of their Whole-of-Government Digital and ICT Investment Oversight Framework in relation to Data Standards.
7. Where possible, the Risk Management Framework for Data Standards should rely on relevant trusted international standards, including in relation to risk management and information security.

Commonwealth entities, including the Department of the Treasury, and Commonwealth officials, including the Chair, must comply with relevant parts of the *Public Governance, Performance and Accountability Act 2013* (**PGPA Act**) and related policies that sit underneath it. This is the baseline for setting out what is required in terms of development of a Risk Management Framework and other activities related specifically to security risks. While we describe in more detail what ought to be done as part of a Risk Management Framework for Data Standards in Section 5, here we describe what is currently required under government policy. In particular, we describe the applicable governance requirements, highlighting complexity.

4.1 Sources of policy

In this section, we analyse three parts of the security governance framework for the CDR – the PGPA Act (which contains relevant definitions and imposes the primary obligations), the Risk Policy, which supports PGPA Act s 16, and PSPF. For ease of reading, we use the term "Finance Law" to refer to the PGPA Act and related rules and instruments as well as associated appropriation Acts.

We also describe adjacent policies, being the DTA's Whole-of-Government Digital and ICT Investment Oversight Framework and standards that are not formally part of the Finance Law, but with which government agencies may be generally expected to comply.

Obligations relevant to a Risk Management Framework that relate to the *Competition and Consumer Act* were analysed in Section 2 and are not repeated here.

4.1.1 PGPA Act

The PGPA Act is at the centre of obligations relating to expectations for Commonwealth entities, accountable authorities and officials. While the PGPA Act and related policies cover diverse areas (e.g. financial reporting), the focus here is on what is required in the context of risk governance.

The PGPA Act places different requirements on different persons or bodies. The Department of the Treasury and the ACCC are both "non-corporate Commonwealth entities". A "Commonwealth Entity" will be designated to undertake the functions of the DSB;[87] currently the Department of the Treasury is so designated. Previously, when CSIRO's Data61 was designated to undertake the DSB's functions, its obligations under the Finance Law were contingent on an order by the Finance Minister that a particular policy apply (see PGPA s 22). The change in the identity of the body undertaking the DSB's functions changed the risk governance activities required.

Under PGPA Act s 16, it is the Accountable Authority that must "establish and maintain an appropriate system for risk oversight and management for the entity and an appropriate system for internal control of the entity, including by implementing measures directed at ensuring officials of the entity comply with the finance law." In the case of the Treasury (or other Commonwealth Entity undertaking the DSB's functions), the risk oversight and management must be appropriate not only to the general functions of the Department but also to any specific functions associated with its role as the DSB. The responsibility for overseeing and managing risk related to the functions of the DSB can be allocated by the Secretary to the officials within the Department responsible for those functions.

4.1.2 Commonwealth Risk Management Policy (Risk Policy)

The Risk Policy supports the statutory requirement under the PGPA Act s 16. It was issued by the Australian Government Department of Finance on 1 July 2014 in support of the Finance Law. It applies to Commonwealth entities, including the Department of the Treasury. The Risk Policy offers a guide to Accountable Authorities in fulfilling their obligation to establish and maintain appropriate systems and internal controls for the oversight and management of risk.

Officials, such as the Chair, also have obligations with respect to risk.

First, they may be allocated responsibility within the entity's Risk Management Framework. For example, they may be made responsible for managing specific risks or given broad responsibility for the entity's appetite and tolerance for risk.

Second, as the Risk Policy states, all officials have responsibility for the day-to-day management of risk. This would include compliance with risk management systems and internal controls and those assigned responsibilities by them, noting that the systemic management of risk should be embedded into all key business processes.

Third, and relatedly, officials have general obligations under the PGPA Act, including a general duty of care and diligence in section 25. This includes weighing foreseeable risks of harm before acting, particularly in contexts where risk is high. In the context of the Data Standards, this would include considering risk elements of decisions such as those around whether and when to create Data Standards, whether those Data Standards will be specified to be binding, the content of Data Standards, and so forth.

4.1.3 Protective Security Policy Framework (PSPF)

The Attorney-General's *Directive on the Security of Government Business* (October 2018) establishes the **Protective Security Policy Framework (PSPF)** as Australian Government policy. All non-corporate Commonwealth entities (including the Department of the Treasury) that are subject to the PGPA Act must apply the PSPF, to the extent consistent with legislation (including Pt IVD). There are five "Principles" and four "Outcomes" underlying the PSPF, set out in *Appendix 4A*.

With the exception of PSPF Principle 2, these Principles are expressed at a high level, recognising the importance of security measures not only for the business of government but also for those with whom risks are shared. In the context of the Data Standards, this includes Data Holders, ADRs, Trusted Advisers, and CDR consumers. The principles urge (1) the taking of responsibility for security, (2) proportionate action in line with risk, (3) 'owning' impact on Shared Risk, and (4) an ongoing cycle of learning.

There are core and supporting requirements to be applied to achieve the outcomes, set out in a series of numbered PSPF Policies. The most relevant of these are described briefly in *Appendix 4A*.

PSPF Policy 8 primarily deals with government information holdings. CDR data is held by government. However, given that risks are shared with CDR participants, it is also appropriate to consider how criteria in this Policy, for assessment of damage to the national interest, government, organisations or individuals, might be applied to assessment of consequences of compromise of CDR data. PSPF Policy 8 includes a "Business Impact Levels tool" in Table 1. This is intended to assist in assessing damage to the national interest, government, organisations, and individuals. Information can then be classified in a manner commensurate with the level of potential harm associated with loss of confidentiality. Even without using the tool to make classification decisions, it is a useful means of differentiating between different levels of business impact.

This tool can be helpful in classifying business impacts of risks associated with the Data Standards. In addition to understanding the impact of different discrimination risks, the tool classifies different levels of loss of confidence in government from "minor" (low to medium), "major" (high) to "directly threatening the internal stability of Australia" (extreme). Other classifications that might be relevant include those relating to failure of statutory duty, compromise of aggregated data, impeding the development or operation of policies and undermining the financial viability of Australian-based companies. Damage to an individual through "discrimination, mistreatment, humiliation or undermining of an individual's dignity or safety that leads to potentially significant harm or potentially life threatening injury" is categorised as "High business impact". Significant damage to an individual could either psychological or physical harm. Damage "that could reasonably be expected to directly threaten or lead to the loss of life of an individual or small group" is categorised as "Extreme business impact".

4.1.4 Assurance

The DTA provides strategic advice and assurance to the Australian government on its digital and ICT-enabled investments to help drive the transformation of public services.[90] Within this mandate, the DTA has developed a Whole-of-Government Digital and ICT Investment Oversight Framework.[91]

The focus of that Framework is on *the government's* "digital and ICT-enabled investments" rather than on government-mandated standards like the Data Standards that are implemented within the systems of third parties. Nevertheless, the language is broad and the Data Standards could fall within the policy as "an investment which uses technology as the primary lever for achieving expected outcomes and benefits", albeit one where the transformation relates to how people and business interact with each other (as directed by government policy and Data Standards), rather than how people and business interact *with the Australian Government.* In

4.1 Sources of policy (continued)

any event, even if the framework does not apply directly, it states that agencies are encouraged to follow the Key Principles for Good Assurance and apply the Framework to the extent of its relevance.

There were earlier assurance activities undertaken by other agencies prior to the DTA's mandate in this area. The ACCC issued an Assurance Strategy for the Consumer Data Right on 28 August 2019. While this predated the DTA's mandate and the Whole-of-Government Digital and ICT Investment Oversight Framework, it aligns with the activities contemplated in Stage 1 of the Framework. Despite the fact that CSIRO was at the time responsible for the functions of the DSB, it does not seem to have been involved in the drafting of the Assurance Strategy, but was rather listed as part of its audience. It was, however, included on the Test Working Group, which had roles in the strategy, including in the planning of industry testing. As part of the contemplated actions under the strategy, the ACCC noted that "a security risk assessment is mandated to determine the threat model and level of vulnerability and penetration testing required at the ecosystem level" for the use of the relevant authentication process and standards (Oauth2.0 and OIDC), and that this would be conducted by "a specialist team on behalf of ACCC". That has not been done.

Since that time, the Department of the Treasury has been designated to undertake the functions of the DSB, and the lead policy agency for the CDR. The responsibility to conduct assurance activities, including the security risk assessment to which ACCC had committed, may thus have shifted. Although the 2019 Assurance Strategy is out of date and does not match current activities and requirements, security risk assessment remains critical. The UNSW Threat Report makes specific recommendations for threat modelling that would align with the Risk Management Framework for Data Standards recommended in this Report.

4.1.5 Relevant Standards

According to the *Industry Innovation and Competitiveness Agenda: An Action Plan for a Stronger Australia* (2014), the Government adopts the principle that "if a system, service or product has been approved under a trusted international standard or risk assessment, then Australian regulators should not impose any additional requirements, unless there is a good demonstrable reason to do so." The aim underlying this policy is the reduction in regulatory burden. The principle effects that aim by reducing duplication of compliance requirements and enabling use of already mature standards and frameworks that are generally well understood and widely accepted. Based on this rationale, the principle should be extended to Data Standards even though the Chair may not be a 'regulator'.[92] It can also be extended to the development of risk management frameworks and processes.

There are a variety of national and international standards that are of relevance to risk management. At the level of enterprise-wide (cross-functional) risk, the ISO 31000 risk management standards framework includes ISO 31000:2009 – Principles and Guidelines on Implementation, ISO/IEC 31010:2009 – Risk Management – Risk Assessment Techniques and ISO Guide 73:2009 – Risk Management – Vocabulary.

A number of standards and risk assessment frameworks specifically focus upon (1) information security, and (2) protection of privacy and other information specific aspects of safe handling of data, including design and specification of data environments and associated technical and operational process and practices. These include the following standards:

Privacy related standards as at 1 July 2022	Subject matter
ISO 19286	Privacy enhancing protocols and services
ISO/IEC 27001:2013	Information security management
ISO/IEC 27002:2013	Information technology – Security techniques
ISO/IEC 27005:2018	Information security risk management
ISO/IEC 27018:2019	Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
ISO/IEC TR 27550:2019	Privacy engineering for system life cycle processes
ISO/IEC DIS 27552:2018	Information technology — Security techniques — Extension to ISO/IEC 27001 and to 1299 ISO/IEC 27002 for privacy management – Requirements and guidelines
ISO/IEC 27555:2021	Guidelines on personally identifiable information deletion
ISO/IEC FDIS 27556	User-centric privacy preferences management framework
ISO/IEC WD 27562	Privacy guidelines for fintech services (under development)
ISO/IEC CD TR 27563	Privacy protection - Security and privacy in artificial intelligence use cases
ISO/IEC 27701:2019	Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
ISO/IEC 29100:2011	Security techniques — Privacy framework
ISO/IEC 29101:2013	Security techniques — Privacy architecture
ISO/IEC 29134:2017	Privacy Impact Assessment
ISO/IEC 29151:2017	Information technology — Security techniques — Code of practice for personally identifiable information protection
ISO/IEC 29184:2020	Online privacy notices and consent
HB 167-2006	Security risk management
NIST 800-37 rev.2	Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
NIST 800-53	Security and Privacy Controls for Federal Information Systems and Organizations
NISTIR 8062	An Introduction to Privacy Engineering and Risk Management in Federal System

A full list of standards, technical specifications and technical standards specific to digital technologies and handling of data and published between 2016 and 2021, and of those currently under development, can be found in the annex to the Data and Digital Standards Landscape published in July 2022 by Standards Australia.[93]

There are a number of standards referenced in government documents, including the PSPF and ISM, that are not directly mandatory (at least not in this context) but that should ideally be followed unless there are reasons not to do so. This includes: ISO 31000, NIST SP 800-37 Rev 2, and HB 167:2006. Given that such standards are embedded in government security policy more broadly, divergence should be both noted and justified. This might be done where, for example, a particular process is not, in fact, best practice, or is not appropriate to the context.

Some standards are mentioned as options in the draft risk program management rules for the *Security of Critical Infrastructure Act 2018* (which, as discussed below, regulates many CDR participants). These include:

- The Australian Cyber Security Centre's Essential Eight Maturity Model at maturity level one;
- AS ISO/IEC 27001:2015 - Information Security Management;
- The National Institute of Standards and Technology (NIST) Cybersecurity Framework;
- The Cybersecurity Capability Maturity Model (C2M2) at Maturity Indicator Level 1; and
- Security Profile 1 of the Australian Energy Sector Cyber Security Framework.

4.2 Complexities

4.2.1 Locating governance for Data Standards

Structurally, the Department of the Treasury is designated to undertake the functions of the DSB.

The PSPF operates at a high level and does not require that responsibilities for assessing and managing risk associated with Data Standards be allocated to any particular official.

There have been previous calls for risk management specifically in the context of Data Standards. On 19 December 2018, Galexia delivered a report[94] for CSIRO's Data61, which at the time had responsibility for Data Standards. This report recommended that in addition to the development and implementation of the Information Security Profile (about which they were specifically advising), there should be a comprehensive Risk Management Framework with respect to the CDR. It stated that this should involve all the relevant entities at that time (Data61, the Treasury, the ACCC and the OAIC) because "a structured and coordinated approach to risk management will be essential across these key organisations in order to deliver the required CDR outcomes". To the best of our knowledge, there is no Risk Management Framework specifically for Data Standards.

In our view, there are good reasons to consider developing a Risk Management Framework for Data Standards and allocating specific responsibility for risks associated with the Data Standards, given that these are technically complex and distinct from other risks managed within Treasury.

4.2.2 Governance in the context of Shared Risks for the CDR ecosystem

Many risks that arise in the context of the CDR are shared among more than one entity.

In Section 3, we discussed the role of Data Standards in assuring trustworthiness of the CDR system, in particular through assisting data recipients to closely link the scope of consumer consents and their operational process and practices for handling of CDR data received pursuant to those consents. We considered why and how risk of unauthorised data use (that is, outside the scope of consent and associated reasonable expectation of consumers) is a Shared Risk.

There are other relevant Shared Risks. For example, in the event of an external security attack, different individuals and entities may suffer harm - consumers may have their privacy compromised, ADRs may receive inaccurate data, and government departments and agencies involved in the program may suffer reputational harm. The risk of such harm may be mitigated by the actions of more than one entity - for example the processes ACCC uses in accreditation, and the Data Standards issued by the Chair.

It is therefore important to consider how such Shared Risks are managed under the Risk Policy and the PSPF.

Both policies refer to Shared Risks.

Element 7 of the Risk Policy is clear about responsibility for Shared Risk, requiring entities to "implement arrangements to understand and contribute to the management of shared risks". The PSPF also requires Shared Risks to be identified with clear allocation of roles and responsibilities with respect to these (see Policy 3, supporting requirement 3 and C.2.3.2). This includes the appointment of a Risk Steward or manager responsible for each security risk or category of risk. Thus all Shared Risks associated with Data Standards should have an assigned Risk Steward or manager.

In the Risk Policy, a focus on Shared Risk is central and guidance is provided. In particular, and relevantly for the Data Standards, an information sheet includes the relationship between policy and implementation as an example of a Shared Risk.[95] In the context of the Data Standards, this is analogous to the relationship between the promulgation of Data Standards and the risks experienced by those implementing the CDR framework. This is most obvious in a context where implementing Data Standards directly creates a vulnerability, but it is also important in contexts where the standards do not deal with particular matters, or are not binding, and the vulnerability results from an absence of implemented standards.

However, the relative emphasis on shared, as opposed to purely internal risk, differs between the Risk Policy and the PSPF. On the one hand, the PSPF also refers to Shared Risks as described above. PSPF Policy 3 also deals with "security risks" broadly. On the other hand, the PSPF Outcomes focus primarily on an entity's *own* people, information and assets. Further, many of the PSPF Policies are expressed in terms of contexts involving government assets or involving transactions with government. For example:

- Core requirement (b) in PSPF Policy 3 focusses on 'threats, risks and vulnerabilities that impact the protection of *an entity's* people, information and assets'
- Policy 8 applies to an entity's own information holdings (official information), not information flows among other entities in accordance with government policy or following government-imposed standards such as Data Standards.
- Supporting requirement 1 in Policy 10 requires entities to not expose the public to unnecessary security risks when they transact online *with* the government.
- Policy 11 only requires entities to ensure that "their" ICT systems meet the security requirements under the ISM. It is explained in the guidance that this is ICT systems that they operate or outsource. It thus does not directly apply to ICT systems of CDR data holders and recipients or APIs implemented by others in compliance with the Data Standards.

Applying these to the Data Standards, which mandate or guide the conditions for transactions among others, is not straightforward. In that case, the Chair's actions in issuing Data Standards does not directly impact *official information* held by government entities, but does impact the circumstances under which CDR data flows between non-government entities and also the ACCC. The wide language in the Principles around Shared Risk and taking responsibility are in tension with a focus on an entity's own information holdings, transactions, assets and systems. A broadening of PSPF Policies, in line with the PSPF Principles for contexts such as Data Standards, may be something that the Attorney-General's Department wishes to consider.

In the meantime, there is a need to apply the PSPF as written to the context in which the Data Standards have the potential to create, or mitigate, security and related data handling risks *to Data Holders, ADRs, Trusted Advisers, and consumers*, as well as to the government itself. This can be done by treating the CDR (as a government program) as an "asset" of the government and recognising that Data Standards may generate reputational risks to government generally and the Department of the Treasury in particular.

Further, supporting requirement 2 of PSPF Policy 3 suggests that what must be identified is not only the people, information and assets critical to the ongoing operation *of the entity,* but also the people, information and assets critical to the *national interest*. Even if the CDR were not considered an asset of the Department of the Treasury, its effective and secure operation should be considered to be in the national interest.

The CDR should thus be protected as critical assets within PSPF Policy 3.

In this way, even though the systems and information associated with the Data Standards are not (with one exception) the systems of a government entity or information held by a government entity, PSPF Policies can guide security risk management for the Data Standards.

The exception mentioned above is the CDR Register (or Register of Accredited Persons), maintained by the ACCC. The ACCC falls under the PGPA Act96 and the Register is part of its own information holdings. Primary responsibility for PSPF compliance for the Register lies with the ACCC, although it would be anomalous for the Chair to impose Data Standards that would be inconsistent with the ACCC's obligations under the PSPF, including compliance with ISM controls.

In summary, we recommend that the PSPF be re-considered in light of the government's security risk obligations beyond an entity's own people, systems and assets. Specifically, in the context of Data Standards, risks might be generated or mitigated by decisions to issue Data Standards on particular topics, the content of those Data Standards, and decisions on whether they are to be made binding. These risks are shared with other participants in the CDR ecosystem, including CDR data holders, CDR data recipients and consumers. In the meantime, we recommend an expansive approach in interpreting PSPF requirements. By recognising the CDR program as a government "asset" and capturing people, information and assets critical to the national interest, the security and related data handling risk implications of such decisions can be better captured in the PSPF framework as written. Advice should ideally also be sought from the Attorney-General's Department (who is responsible for the PSPF framework) on what is required under current policy and whether that policy ought to be revised.

4.2 Complexities (continued)

4.2.3 Interaction with other legislation

Another complication in developing a Risk Management Framework for the Data Standards is the interaction with other legislation and policy that also deals with risk management in intersecting subject matter. There are two examples that we note here – critical infrastructure regulation and the draft National Data Security Action Plan.

Critical infrastructure is regulated under the recently-amended *Security of Critical Infrastructure Act 2018*. The focus is on sectors of the Australian economy rather than government itself as critical infrastructure. The intersection with the Data Standards is thus not that entities in the CDR ecosystem become critical infrastructure by virtue of that fact, but that many of the entities bound by and implementing the Data Standards will also be regulated as critical infrastructure. For example, 'critical banking asset' is defined in s 12G, and may include "computer data" that is used in carrying on banking business that is critical to the security and reliability of the financial services sector. A regulated category that will cut across the CDR, and particularly capture organisations in the CDR ecosystem whose business is data storage or backup or data processing, is 'critical data storage and processing asset' (defined in s 12F). Those organisations in the CDR ecosystem who are captured are *inter alia* required to have and comply with a 'critical risk management program' that meets the terms of that legislation (Pt 2A).

The link between the CDR and critical infrastructure legislation will need to be analysed in the context of any expansion of the CDR to incorporate Action Initiation.

While these risk management programs are independent of the risk management we propose here for the Data Standards, there are important areas of intersection. This is because many risks are shared with entities (such as banks) whose risk management must align with the requirements of the *Security of Critical Infrastructure Act 2018*. This may affect how Shared Risks are identified and managed, particularly in context where the choice of data standards impacts on levels of risk.

A National Data Security Action Plan is currently undergoing consultation, and is primarily concerned with data security as important for national security (e.g., threats from foreign adversaries) but incorporates importance beyond that (including to individual data subjects). They are considering the introduction of technical controls, policy and legislative mechanisms and capabilities gaps, with a goal of consistency across government and the economy but at a high level. The principles being developed are currently named Secure, Accountable and Controlled. There is at least potential, depending on the outcome of that consultation (report due end of 2022) that there will be greater integration across data standards nationally (potentially incorporating Data Standards). Because the outcomes of this policy process are currently unknown, it is not otherwise considered in our recommendations

5. Developing a Risk Management Framework

1. We recommend that the Chair ensure that there is a Risk Management Framework for the Data Standards in place. This must align with the Treasury's Risk Management Framework. This section sets out elements of a Risk Management Framework for Consumer Data Standards.
2. Some risks associated with the CDR, including some reputational and security risks, will be Shared Risks across CDR agencies, including the ACCC and Treasury.
3. The current Consumer Data Standards feature a number of risk management safeguards. These focus on assessment, mitigation, and management of information security risks. However, they do not address the risks of inappropriate or unauthorised handling of CDR data, including through failures in assessment of whether output data from those data environments is safe to egress.
4. Identification of data security risks can be based on a standards approach, specifically, ISO/IEC 27005.
5. It is likely that only a qualitative measurement of systematic risk, and of operational risk of inappropriate and unauthorised handling of CDR data within data environments managed by recipients, will be available. This may be contrasted with the more prescriptive assessment criteria as to information security of recipient's data environments and associated controls and audit and attestation reporting as to implementation of information security within those environments.
6. That gap means the controls designed to assure implementation of those safeguards may not operate to assure that operational processes and practices implemented by ADRs, and Trusted Advisers, appropriately address risks of inappropriate and unauthorised handling and disclosure of CDR data.
7. While it is not entirely clear that Data Standards are the best fit mechanism to close that gap, a Risk Management Framework for Data Standards would assist assessment of how and where risks of inappropriate and unauthorised handling and disclosure of CDR data may be addressed through close linkage between the scope and quality of data consents tailored to particular use cases, and the specification of operational processes and practices that recipients implement for those particular use cases.
8. The Chair should regard the risk of unauthorised uses and disclosures of CDR data as a high risk to be managed by the Chair under the appropriate Risk Management Framework.
9. The Chair may like to consider making the Risk Management Framework for Data Standards public, so CDR participants can access those parts of the Risk Management Framework that assist with their own identification and management of risk.

5.1 Introduction

As set out in Section 4, there are a range of policy and governance issues that create the need for systematic risk management of Consumer Data Standards. Design of the framework, and any specification of methodologies to implement that framework, should be consistent with the PSPF (as addressed in Section 4.1.2), the Risk Policy (as addressed in Section 4.1.3), the Whole-of-Government Digital and ICT Investment Oversight Framework (as addressed in Section 4.1.4), and (for the reasons discussed in Section 4.1.5) either adopt a trusted international standard or risk assessment framework, or closely align to standards and frameworks that are already well understood, widely accepted and familiar to entities and their advisers tasked with implementing them.

This section identifies our recommendations on elements for a Risk Management Framework for Data Standards. We seek to closely align to well accepted existing approaches to risk management, including security risk management. In considering alignment with existing standards and frameworks, we also seek to accommodate the unusual aspect of the CDR which is outside the ambit of enterprise risk management as addressed by those existing standards and frameworks: namely, the risk shared between the Treasury, ACCC, OAIC, CDR participants and CDR consumers that was the focus in Section 3. This is the risk that failures in safe handling of CDR data through the CDR ecosystem or through uses or disclosures outside of reasonable consumer expectations as informed by consumer consents will undermine trust in the CDR.

5.2 Risk context

The nature of the CDR and proposed expansion, discussed in Section 2, provides an important context for risk management in the context of Data Standards.

Consider, for example, the cross-sectoral expansion beyond the banking sector. Incoming CDR participants are likely to have lower cyber maturity compared to banks and financial institutions. As noted by McKinsey, "banks have traditionally viewed the custody and protection of their clients' data as a responsibility."[97] Application of Data Standards in the banking sector followed that sector's approach to data security, data privacy risk and related risks in handling of confidential or sensitive information relating to customers and their transaction. This approach:

1. is consent-based;
2. has an audit requirement;
3. is subject to regulation; and
4. is driven by the risk management practices of regulated financial services providers.

In the banking sector, many of the risks addressed with Data Standards were addressed in whole or part by existing data handling processes and practices, and associated governance (oversight) and assurance controls, of regulated entities. Many of those banks, either through operation of existing risk management requirements and guidance issued by ASIC or APRA, or through their recognition of exposure to reputational risk, demonstrate a risk aversion aligned with that of the Treasury. Many of those providers:

1. have a level of familiarity with complex risk assessment and management frameworks, standards and methodologies,
2. already have in place 'three lines of defence' governance structures and reporting lines, including allocation of a senior executive with responsibility and accountability for their reliable operation,
3. have aligned assessment and mitigation of information security, privacy, data handling and data lifecycle management risks with enterprise-wide risk management frameworks, governance and assurance,
4. have established programs for 'end-to-end' data risk management, including for ongoing oversight of risk management by outsourced service providers and subcontractors who process of otherwise handle confidential or sensitive data on their behalf, and
5. have implemented audit controls and assurance mechanisms aligned with the Standard on Assurance Engagements ASAE 3150 (Assurance Engagements on Controls) or similar standards.

Banks typically exhibit a level of maturity[98] in assessment and management of information security and related data handling risks that may not be present when the CDR is deployed in other sectors or in relation to ADRs that are not regulated financial services providers. For example, businesses which provide comparison websites do not have the risk management history that is found in the financial services sector. They will nevertheless be in a position to access sensitive data from a wide variety of Data Holders across sectors. The risks associated with relatively cyber immature actors aggregating such data increases as the CDR expands to new sectors.

In *Appendix 5A*, we further discuss the effect of differing levels of data maturity of particular entities and associated systemic risk of cross-sectoral expansion of the CDR system leading to increases in instances of mishandling or other unauthorised collection, use or disclosure of CDR data.

Another relevant context is the position of consumers in relation to consent, which will vary both in the extent to which they are informed and what is authorised. Risk management systems for operational risk in consent driven data systems must also accommodate the diverse contexts in which risks of adverse effects upon relevant stakeholders (including privacy harms) arise from mismatch between the scope of consumer consent, and uses and disclosures that are dependent upon and should be bounded by the scope of consumer consent. Data warehouses and data analytics environments, and pathways for communication of sensitive and confidential data, should be secured (safeguarded and controlled) against data security (cyber risk) threats regardless of the nature and scope of consumer consents that relate to the curated and managed data. By contrast, operational risk of inappropriate and unauthorised uses and disclosures of that data can only be appropriately assessed, mitigated and managed by ongoing linkage of consent and permitted handling.

5.3 Identification and analysis of risks

The purpose of risk identification within a system of risk management is to establish the context: what, where, when, why, and how something could affect an organisation's ability to operate. Risk identification enables organisations to develop plans to minimise harmful events before they arise. This means identifying all possible risks that could harm operations.

It is usual to apply a range of processes in risk identification. The UNSW Threat Report includes discussion of threat identification methodologies used in threat modelling.

As discussed in 4.2.1, allocation of responsibility for identifying (and managing) risks associated with Data Standards should recognise the importance of expertise, both as to the context for Data Standards and as to the Data Standards themselves.

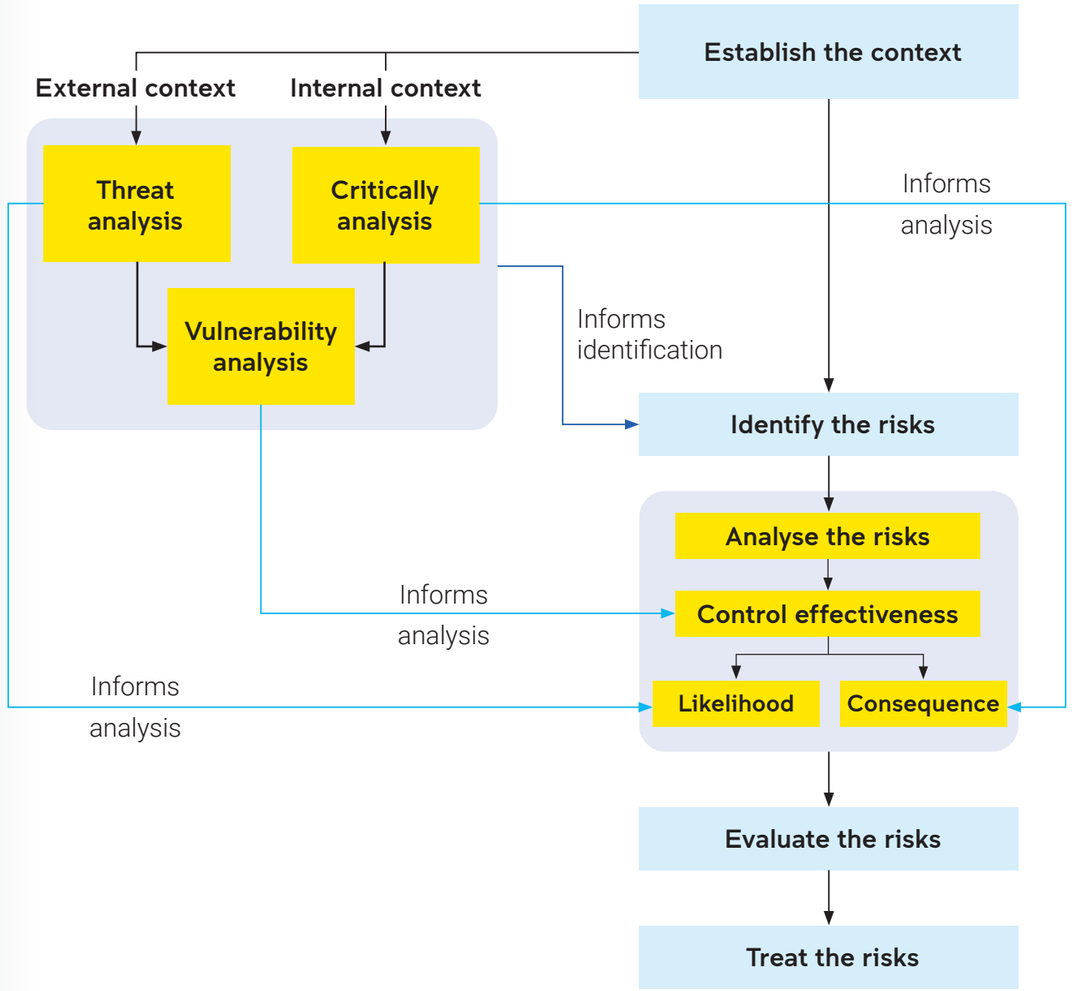
For the reasons set out in 4.1.3 and 4.1.5, identification of security risks relating to Data Standards should align with the PSPF and ISO/IEC 27005 (Information technology — Security techniques — Information security risk management). ISO/IEC 27005 states that "the purpose of risk identification is to determine what can happen to cause a potential loss, and to gain insight into how, where and why the loss can happen." It goes on to note that "risk identification should include risks whether or not their source is under the control of the organisation, even though the risk source or cause is perhaps not evident."

The standard then deals with the approach in a number of steps, also aligning with the approach in the policies and standards set out in Section 4.1:

1. **Identification of assets**
   This has the input of the scope and boundaries for the risk assessment to be conducted including identifying the constituents, their owners, location, and function. It has the action of identifying the assets within the established scope. This has the output of a list of assets to be risk-managed, and a list of business processes related to assets and their relevance.
2. **Identification of threats**
   This step is discussed in the UNSW Threat Report.
3. **Identification of existing controls**
   This has the input of documentation of controls and risk treatment implementation plans. It has the action of identifying existing and planned controls. This has the output of a list of all existing and planned controls, their implementation and usage status.
4. **Identification of vulnerabilities**
   This has the input of a list of known threats, lists of assets and existing controls. It has the action of identifying vulnerabilities that can be exploited by threats to cause harm to assets or to the organisation. This has the output of: a list of vulnerabilities in relation to assets, threats and controls; and a list of vulnerabilities that do not relate to any identified threat for review.
5. **Identification of criticality**
   this is a requirement, referred to above, which could rely on the BILs in PSPF Policy 8.
6. **Identification of consequences**
   This has the input of a list of assets, a list of business processes, and a list of threats and vulnerabilities, where appropriate, related to assets and their relevance. It has the action of identifying the consequences that losses of confidentiality, integrity and availability may have on the assets. This has the output of a list of incident scenarios with their consequences related to assets and business processes.

A summary of the approach is set out in Figure 1:

Figure 1: Approach based on HB 167: 2006



5.4 Evaluation of risks

There are "residual" risks that are inherent in sharing any confidential or sensitive data, and which cannot be reasonably expected to be fully mitigated through application of standards and risk frameworks. Factors relevant to determination of acceptable residual risks include (1) likelihood of occurrence of those residual risks and of material adverse impact if those risks are not fully mitigated, (2) cost and reasonable practicality of assessment and mitigation of all conceivable risks through imposition of technical and operational safeguards, (3) cost and reasonable practicality of creation and oversight of controls to assure that safeguards have been reliably and verifiably implemented, and (4) countervailing or offsetting benefit.

Where Shared Risks are addressed through government initiated action that imposes a regulatory burden upon other entities, further relevant factors include (1) whether the allocation by government fiat to the entity of the burden of managing that risk is fair (as between government, its agencies and the various entities sharing that risk), reasonable and proportionate to the risk, and (2) whether there is a significant mismatch between which entity bears the cost and effort of discharging that burden, and the entities (including government and its agencies) that derive a countervailing or offsetting benefit from that burden being discharged.

Where Shared Risk is being addressed it is difficult to predict and reliably quantify, because there is likely to be a significant mismatch between which CDR participants, and agencies, bear the cost and effort of discharging a burden and the participants, or agencies, that derive countervailing or offsetting benefit. Therefore, it is appropriate to exercise caution in (1) making a determination as to whether to create the burden, and (2) specifying which entity bears that burden.

This applies to the Shared Risk of loss of trust in the CDR (when attributable directly, or indirectly through contagion effects, to failures in safe handling of CDR data through the CDR system or resulting from uses or disclosures that are outside of reasonable consumer expectations as informed by consumer consents). In particular, allocation of the burden of mitigating this risk is difficult because of the diversity of interests of entities within the CDR system as to mitigation of this Shared Risk, and the fact that benefits in mitigating this risk accrue in substantial part outside of the entity mitigating the risk. The treatment of this risk thus requires caution.

Evaluation of the extent to which Data Standards can, and should, by their operation create burden upon entities that are required to apply those Data Standards to their operations also requires consideration of where Data Standards are the best-fit regulatory measure to address the relevant risks, including Shared Risks. In *Appendix 5B*, we further discuss how the Chair may evaluate whether to make Data Standards to address an issue, as compared to other regulatory measures being adopted, and within the context of the respective roles and functions of the Treasury, ACCC and OAIC.

One complexity with cross-sectoral expansion of the CDR is that the magnitude of the regulatory burden, the costs incurred by CDR participants in discharging that burden, and the magnitude and distribution of benefits, will substantially differ as between sectors, and as to use case scenarios within sectors.

This is one reason why the Risk Management Framework for Data Standards should assess risks for particular common use cases and associated data environments for handling CDR data to fulfil those use cases: see further Section 3.4.

5.5 The scope for risk treatments: Information security risks and operational risks of data participants

The current safeguards requirements for these environments in the Data Standards focus upon assessment, mitigation and management of information security risks, and not upon risks of inappropriate and unauthorised handling of CDR data. See *Appendix 5C*. Focus upon the high and/or extreme risk that consumer data will be subject to external security threat vectors. The sources of threat may be human adversaries and/or inadequate or failed internal processes, people or systems.

Often the most efficient way to mitigate these risks is deployment of technical safeguards and associated controls as to management of data environments and for structured evaluation as to whether outputs are safe to be allowed out of those controlled environments. Accordingly, 'technical' standards may assist with assessment, mitigation and management of operational risks, as well as cyber risk. A risk framework and risk management system for Data Standards should encompass technical means (safeguards and associated controls) for assessment, mitigation and management of operational risks.

Operational risks are more situationally specific. Operational risks of unsafe handling of CDR data, leading to harms, may be substantial because frameworks, systems and standards for operational risk management, because of situational diversity, generally are less prescriptive (standardised) as to specific safeguards and associated controls than their equivalents for data security (cyber risk) management. Diversity in scope of consumer consents, and in data handling for associated permitted use cases, means that more context specific (situational) risk management will often be prudent and appropriate. The importance of context is discussed in Section 5.2 above. As noted there, this includes the need to manage diversity in the scope and quality of consumer consents, making risk management more complicated.

Context (consent, data environment and use case) specific assessment may be significantly guided and aided by specification of an appropriate risk assessment framework which leads to development of risk management systems that address operational risks with the same rigour as is now expected of entities in their management of cyber risks associated with their handling of confidential or sensitive data. A risk-based approach to Data Standards would assist assessment of how and where risks of inappropriate and unauthorised handling and disclosure of CDR data may be addressed through less prescriptive measures that assure linkage between the scope and quality of data consents and the specification of operational processes and practices as implemented by data recipients.

A further contextual complexity arises when endeavouring to apply PSPF Policy 8 (Sensitive and classified data) in the context of development of a Risk Management Framework for Data Standards (see Section 4.2.2). The Chair, and The Treasury, may assess information sensitivity having regard the Shared Risk of unauthorised uses and disclosures of CDR data by other entities impacting public perceptions as to the trustworthiness of the CDR system, thereby undermining the objective of facilitating consumer transactions that are impeded by limited availability to consumers of data that relates to them and their transactions and activities, and current friction points as to transfers of consumer data. Clearly CDR data that is reasonably identifying of consumers and their transactions and activities should be classified as consumer consent-controlled data in relation to uses and disclosures, and therefore treated as sensitive personal information by CDR participants that handle this CDR data.

6. Privacy

1. Privacy is critical for an individual's dignity and autonomy. Dignity and autonomy entail the ability to make one's own choices and be free from unjustifiable control and manipulation by others.
2. Information privacy is not only about secrecy, but allowing people to share their data selectively according to their own preferences.
3. Beyond facilitating individuals' management of the disclosure and use of their personal information, information privacy requires protection against privacy harms. As the OAIC has argued, such a shift in focus will, 'support responsible innovation, economic development and other important societal objectives by promoting trust and confidence in government and commercial activities'.
4. Privacy is also interwoven with, and supports, rights such as the right to freedom from discrimination; equal access to markets and opportunities; autonomy; free will and individual dignity.
5. Consumer surveys indicate that Australian consumers are concerned about their privacy online. Attitudes revealed in these surveys include consumers' beliefs that companies should only collect information currently needed for their product or service and should allow them to opt out of certain types of collection, use and sharing.
6. However, some commentators believe there is a 'privacy paradox' in that consumers express these views but continue to use services with poor privacy terms, arguing that therefore consumers do not in fact value privacy as they claim.
7. The 'privacy paradox' argument is undermined by the facts that: it is practically impossible for most consumers to read all the privacy terms that apply to them; many privacy terms are designed to conceal and obfuscate the most concerning data practices; there is a lack of competition on privacy quality; and consumers often have no real choice about whether to use a particular service.
8. It is likely that most consumers do care about privacy, as they have expressly stated in surveys.
9. Harms from poor privacy practices include: combining data from different sources to reveal unexpected facts or inferences about a person; increased vulnerability to fraud and identity theft; undesirable secondary uses of data without consent; excluding consumers from knowledge about and participation in the handling and use of their data by others; and interference with individual decision-making.
10. Not all privacy risks can be solved by consent. Consumers may not be capable of making complex choices about information handling practices where those practices and their consequences are beyond their comprehension. Some practices are so inherently harmful that they should not be permitted even with consent.
11. Nor is de-identification of data a panacea. Even diligent de-identification efforts may fail and expose consumers to substantial harms. Data minimisation - avoiding the collection of unnecessary data - is therefore vital in reducing privacy risks, since the data, which is not collected, cannot be exposed to improper access or use.

6.1 The value and meaning of privacy

The foundation of what is protected by the right of privacy is human dignity.[99] In the context of the CDR, the relevant type of privacy is information privacy.[100] Information privacy is not just about keeping some personal information confidential or 'secret'. It is also about how people 'want to share (their data) selectively and make sure that it isn't used in harmful ways'. Information privacy is 'about modulating boundaries and controlling data flows'.[101] In other words, it is as much about data collection and use as it is about disclosure.

Thus the right to privacy is more than the right 'to be let alone'. Privacy has consistently been explained as critical for an individual's dignity and autonomy, which entails the ability to make one's own choices and be free from unjustifiable control and manipulation by others. Paul Sieghart has explained the links between privacy and information management, autonomy and power:

> *In a society where modern information technology is developing fast, many others may be able to find out how we act. And that, in turn, may reduce our freedom to act as we please – because once others discover how we act, they may think that it is in their interest, or in the interest of society, or even in our own interest to dissuade us, discourage us, or even stopping us from doing what we want to do, and seek to manipulate us to do what they want to do.*

Sieghart gave that explanation in 1976, but the UN Special Rapporteur on the Right to Privacy more recently highlighted the relevance of this description of the value of privacy in the present era, warning of the potential for manipulation once privacy is degraded:

> *Shorn of the cloak of privacy that protects him, an individual becomes transparent and therefore manipulable. A manipulable individual is at the mercy of those who control the information held about him, and his freedom, which is often relative at best, shrinks in direct proportion to the extent of the nature of the options and alternatives which are left open to him by those who control the information.*[102]

However, even a conception of privacy as regulating the handling of personal information through the information life cycle can miss the forest for the trees. In a submission to the Attorney-General's Department in the current review of the *Privacy Act*, the OAIC has argued that the *Privacy Act* needs a clearer focus on protecting against privacy harms, instead of just the management of personal information *per se*. Such a shift in focus will 'support responsible innovation, economic development and other important societal objectives by promoting trust and confidence in government and commercial activities'.[103] Potential privacy harms under the CDR scheme are explained further below.

> Further, privacy is often interwoven with other rights. By upholding privacy, other rights and values can also be enabled or supported.[104]

such as:

- freedom of speech / expression,
- freedom of association and movement,
- freedom of religion,
- freedom from discrimination,
- the right to a fair trial,
- equal access to markets and opportunities,
- autonomy / free will, and
- individual dignity.

As noted in the discussion of privacy harms in Section 6.4 below, in the context of the CDR scheme, privacy's role in enabling freedom from discrimination, equal access to markets and opportunities, autonomy and dignity are particularly relevant.

6.2 Consumer attitudes to privacy in Australia

Research indicates that most Australian consumers do not want their online or offline activities tracked and analysed, shared with other companies, and used for various commercial purposes unnecessary for the product or service they sought from the supplier. According to the 2020 Community Attitudes to Privacy Survey by the Office of the Australian Information Commissioner (OAIC), most Australians are uncomfortable with:

- businesses sharing their personal information with other Australian organisations - 72%; and
- online businesses keeping databases on what they have said and done online - 62%.[106]

The ACCC 2018 Roy Morgan survey indicated that most consumers surveyed considered it to be a misuse of their personal information if digital platforms:

- collect information about the consumer in ways the consumer would not expect - 83%;
- add to information about them with information gathered from other companies the consumer has dealt with - 81%;
- track their online behaviour when they are not logged in - 82%;
- monitor their offline activities like location and movement without the consumer's express consent, even when logged in - 86%.[107]

In the same survey, most consumers did *not* agree that they did not mind digital platforms collecting more information if the consumer would be more likely to be interested in the ads they receive (62%).

The Consumer Policy Research Centre survey showed that the majority of consumers:

- consider it unfair for a company to collect info about the consumer from other companies - 83%;
- found it unacceptable for companies to monitor their online behaviour to show them relevant advertisements and offers - 60%;
- consider it unfair for a company to use personal information to make predictions about the consumer - 76%;
- agreed that companies should only collect information currently needed for their product or service - 92%;
- agreed that companies should give them options to opt out of certain types of information collection, use and sharing - 95%;
- disagreed that, if they trust a company, they don't mind if the company buys information about them from database companies without asking the consumer - 81%.[108]

6.3 'Privacy paradox' debate

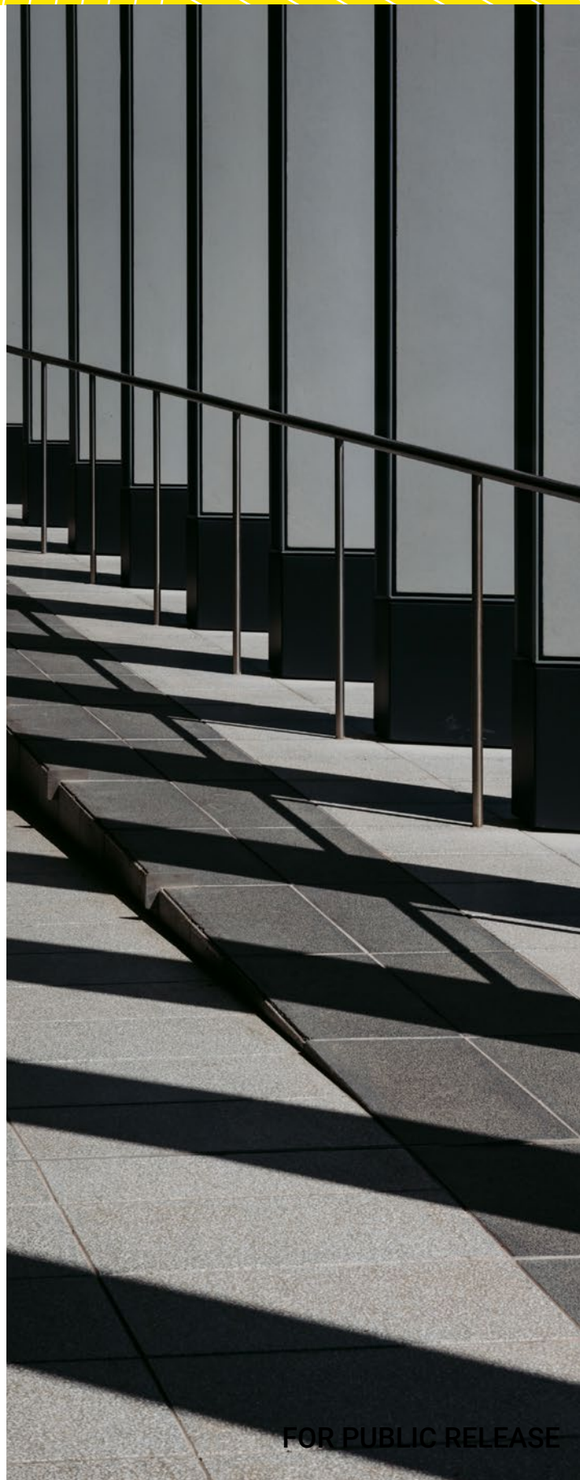
Some commentators have suggested that, while consumers might express these preferences for privacy when questioned for a survey, in reality consumers do not value privacy in this way - or do not value privacy as much as convenience or free services - since they continue to use services with poor privacy terms. This has often been referred to as the 'privacy paradox'.[109] These arguments at least implicitly rely on 'revealed preference theory': in essence, consumers are said to express one view while engaging in contradictory behaviours that reveal their true preferences.

However, there are strong arguments that it is inappropriate to rely on revealed preference theory in circumstances where the consumer does not have clear information about the nature of the available options (if any) or their consequences; and where the consumer has little choice but to accept the service in question.

Both of these factors are present in the case of many privacy terms. Research has demonstrated that it would be practically impossible for most consumers to read all privacy policies that apply to them, requiring an average of over six working weeks per year for the reading alone.[110] Privacy policies in general are now notorious for their vaguely-worded, open-ended clauses and their tendency to hide the most concerning data practices in the fine print, while headlining with reassurances of 'care' and 'trust' and obvious, uncontroversial uses of personal data.

Further, consumers often have little real choice but to use a given service, whether or not they are satisfied with what they understand of the privacy policy. Engagement with certain services is not optional, particularly when chosen by third parties, such as employers, landlords, schools, sports clubs, colleagues, and government agencies.

The consumer preferences expressed in major Australian surveys are entirely consistent with consumers preferring privacy while lacking the information, resources, and power necessary to fulfil those preferences and secure fairness in data practices.[111]



6.4 Potential privacy harms under the CDR scheme

The recognised types of activity which can lead to privacy harms include the following which are particularly relevant to the CDR scheme:[112]

- Aggregating or combining data can reveal facts about a person that are not readily known and that a person did not expect to be known when providing the data,
- Security vulnerabilities make people more susceptible to fraud and identity theft,
- Secondary use involves using information in ways a person does not consent to and might not find desirable, and
- Exclusion concerns the failure to allow people to know about the data that others have about them and participate in its handling and use.

Other categories of privacy harm are listed in *Appendix 6A*. Taking this taxonomy of privacy harms as a starting point,[113] we can see that utilisation of the CDR scheme as a whole by consumers has the potential to lead to privacy harms including:

- A fintech or Trusted Adviser could combine data (including data across different CDR sectors) which then reveals facts or generates inferences about a consumer that were not readily known, and that the consumer did not expect to become known,
- Security vulnerabilities in the technology underpinning data sharing could make people more vulnerable to fraud and identity theft, and associated financial loss and trauma,
- Any breach of confidentiality by any player would break the promise to keep a consumer's information confidential,
- Any secondary use of data gained by data recipients could involve use of data in ways the consumer did not consent to which could disadvantage the consumer, and
- To the extent that 'Action Initiation' is used (e.g. initiating an application for a loan or switching between retail energy plans), decisional interference could involve incursion into people's decisions regarding their private affairs.

There are also some broader societal impacts to be considered, such as the decisional interference for consumers *not* using the CDR scheme. For example, will consumers who do not have an app, or who do not want to share data via a fintech, suffer market exclusion or price discrimination, such as paying higher prices for their electricity or home loan or not being offered insurance cover? Market exclusion could further entrench disadvantages suffered by those on the wrong side of the digital divide.

Another broader social impact to consider will be the extent to which the CDR promotes the commodification of data. What in the scheme will prevent fintechs from asking people to effectively 'sell' their data, including by offering incentives in exchange for the consumer's 'consent' for their data to be collected or used in certain ways?

Many privacy scholars argue that privacy has a **social value** like free speech, or food safety: 'There would be a price at which some people would accept greater risks of tainted food. The fact that there is such a price doesn't mean that the law should allow the transaction'.[114] The creation of a 'data marketplace' raises similar ethical concerns.

6.5 Limitations of a 'notice and consent' model to mitigate privacy harms

As a general observation of the CDR as a consent-based scheme, it will be critical to appreciate that **not all privacy risks can be resolved by consent**.

The same observation can equally be made of de-identification. Both 'consent' and 'de-identification' are often posed as panaceas to all privacy risks. However, once privacy is understood as protecting a range of rights and values beyond just confidentiality, it becomes apparent that a more nuanced understanding of privacy risks – and potential solutions – is necessary.

Even diligent de-identification efforts may fail and expose consumers to substantial harms. Data minimisation - avoiding the collection of unnecessary data - is therefore vital in reducing privacy risks, since the data which is not collected cannot be exposed to improper access or use.

The OAIC has also argued that notice and consent mechanisms do 'not address the privacy risks and harms facing individuals in the digital age'. Notice and consent places 'an unrealistic burden of understanding the risks of complicated information handling practices on individuals', and it 'does not scale'.[115]

Professor Woodrow Hartzog writes that 'People are simply overwhelmed by the choices presented to them. The result is a threadbare accountability framework that launders risk by foisting it on people who have no practical alternative to clicking the 'I Agree' button'.[116]

Further, because one individual's actions can impact the privacy of other individuals or society at large, a privacy framework which focuses on enabling *individual* privacy management through notice and consent mechanisms is not 'capable of addressing these collective privacy concerns'.[117]

The OAIC has argued that consent should not be requested for routine, expected activities:

> *[R]eliance on consent should be targeted and limited to situations where individuals can and should validly exercise a choice, not expanded and used more broadly to permit data handling practices.*[118]

> *[I]t is important to preserve the use of consent for situations in which the impact on an individual's privacy is greatest, and not require consent for uses of personal information for purposes that individuals would expect or consider reasonable. Seeking consent for routine purposes may undermine the quality of consents obtained from consumers, and result in consent fatigue. It is also essential that consent be relied on only where an individual is actually being given meaningful control over their personal information.*[119]

Consent is thus not a panacea because (1) a valid, freely given, unambiguous, informed, specific consent is hard to get, and (2) some data uses are too unfair or harmful to allow even with consent.

6.6 CDR: Potential points of weakness

For the CDR, some potential points of weakness, at which privacy harms could be introduced for consumers, include the following in broad terms.

1. **Capacity to consent**
   For the purposes of ensuring that a customer has given a valid consent for a data exchange, it will be important to establish first that an entity has correctly identified the customer. Intertwined with this is the need to ensure that the customer has the *capacity* to provide (or withhold / revoke) their consent.

2. **Authentication of the customer**
   The following scenarios will be challenging as the CDR scheme expands beyond the financial sector:
   - joint accounts,
   - accounts in the name of a parent on behalf of a child (e.g. mobile phone accounts for teens),
   - determining who has parental authority for a child, and
   - determining who is an authorised representative for an adult with limited capacity.

3. **Validity of consent**
   How much do does the consumer understand? Is the consent freely given? Might the consumer be suffering from consent fatigue?

4. **Data minimisation**
   Whenever the minimum cluster of data for which a consumer can request access for a third party is significantly broader than the data required for the consumer's purpose, this may undermine data minimisation and unnecessarily expose further personal data to security and other risks.

5. **Fairness of the proposed activity**
   Proposals for a new 'fair and reasonable' test in privacy reforms being considered by the Attorney-General's Department as part of the Privacy Act Review.

6. **Accuracy and integrity of the data**
   This includes the accuracy, relevance and fairness of inferences as well as 'facts' revealed by the data.

7. **Re-identification of de-identified data**
   If an ADR sells or otherwise discloses CDR data which it has purportedly de-identified and that data is later re-identified and therefore connected to the consumer, the consumer's personal information will potentially be exposed to misuse well beyond the CDR system.

8. **Misuse of CDR data – by related actors**
   As the CDR scheme moves beyond just data sharing towards 'action initiation' (e.g. change contact details, make a payment, open a new account, close an account), it is necessary to consider how a bad actor, such as an abusive or controlling (ex)partner, could use the CDR scheme to deliberately hurt an individual, such as by:
   - finding out critical information such as home address,
   - determining patterns of behaviour from electricity usage,
   - switching off the power to the victim's home, and
   - cancelling a phone contract or insurance policy on which the victim relies.

9. **Misuse of CDR data – by unrelated bad actors**
   This is considered in the UNSW Threat Report.

10. **Misuse of CDR data – by ADRs and Trusted Advisers**
    As explained in Section 3, what the recipients do with the data affects trust in the overall CDR ecosystem.

11. **Utility of the CDR Privacy Safeguards**
    If the *Privacy Act 1988* (Cth) is amended as a result of the Attorney-General Department's consideration of privacy reforms, the Privacy Safeguards could become less rigorous than the Australian Privacy Principles.

12. **Development of the Data Standards**
    Because the Data Standards change frequently, there may be insufficient time to identify and assess changed risks with each iteration.

In the context of issues related to consent, the DSB prepared a Discussion Paper comparing requirements for consent across different existing and proposed regulatory frameworks as well as ISO/IEC 29100:2011. The mapping conducted in that Discussion Paper is set out in Table 2:

Table 2. Mapping of consent requirements from Data Standards Body Discussion Paper

ISO 29100:2011	OAIC Australian Privacy Principles	ACCC Rules Div 4.3	ACCC Digital Platforms Inquiry	GDPR Article 4
Freely given	Voluntary	a. Voluntary	Freely given	Freely given Article 7 (4)
		b. Express	Unambiguous	Unambiguous Article 7(2)
Informed Agreement	Implied / (Adequately) Informed	c. Informed	Informed	Informed Agreement Article 7(2)
Specific	Current and Specific	*Current and* d. Specific to purpose	Specific	Specific Article 6(1)(a)
		e. Time limited		
		f. Easily withdrawn		It shall be as easy to withdraw as to give consent. Article 7 (3)
				Provable that the individual related to the PII is the one granting consent. Article 7 (1)
			Additional data collection settings must be turned off by default	
	The individual has the capacity to provide consent.			It shall be proven that the individual has capacity to provide consent. Article 7 (1)

The benefits of the GDPR approach in resolving some of the gaps in the consent framework for the CDR are evident from the table. In particular, for the GDPR, it must be proven that the individual consenting is the one related to the relevant information and that they have capacity to provide consent. These would deal with the first two weaknesses listed above.

7. Privacy Impact Assessments

1. Six Privacy Impact Assessments (PIAs) have been conducted in respect of the CDR scheme at various stages since 2018.
2. However, these PIAs have not squarely and comprehensively addressed the impact of the substance of the Data Standards as such. This is likely to have been due to factors such as the exclusion of the Data Standards from terms of reference and some PIAs pre-dating the Data Standards.
3. The functions of the DSB have been assigned from a quasi-independent Commonwealth Corporate Entity (CSIRO) to a central Australian Government Department (Treasury). For Australian government agencies, such as the Chair, PIAs are required by law for any changes which may have 'high privacy risks'.
4. Each time the CDR scheme updates or evolves creates a fresh opportunity to deliver benefits to consumers; but also to potentially create privacy risks which should be assessed and where possible mitigated.
5. A PIA is a comprehensive tool for assessing the privacy impact of new initiatives, whether technical, policy or legislative ('projects').
6. PIAs are usually undertaken as part of a sound project management strategy, to assess whether it is safe to proceed to the implementation phase.
7. A failure to properly embed appropriate privacy protection measures may result in a breach of privacy laws, or prohibitive costs in 'retro-fitting' a system to ensure legal compliance or address community concerns about privacy.
8. Both positive and negative privacy impacts from the project are assessed.
9. Negative impacts can be a legal compliance risk for the organisation; a reputational risk for the organisation; or a risk for individuals suffering a privacy-related harm.
10. Triggers for requiring a fresh PIA should include: the on-boarding of new sectors; the on-boarding of new data types; any new functionalities or features; and as part of the development process for new or significantly amended Data Standards. In our view, these expansions reflect many of the factors which the OAIC considers to pose inherently 'high privacy risks'.
11. We recommend that a PIA be conducted on draft Data Standards associated with each such expansion of the CDR scheme. The PIA should take a deliberately broad, holistic, 'scheme-wide' view, rather than focus on only one element such as the Data Standards.
12. The PIA should consider which of the risks can be resolved through careful crafting of the Data Standards, versus applying other levers.
13. Future PIAs should also include a review of which recommendations from previous PIAs were not followed or implemented, and why, helping to ensure that nothing has 'slipped through the cracks' over time.

7.1 Existing PIAs and concerns regarding adequacy

To date, six Privacy Impact Assessments (PIAs) have been conducted in respect of the CDR scheme at various stages since 2018. We note that some of the initial PIAs conducted in 2018 and 2019 pre-dated the release of the first production version of the Data Standards (v1.0.0) in September 2019. The PIAs have also tended to expressly limit their scope and naturally relate to particular stages of the CDR scheme. *Appendix 7A* outlines matters expressly within scope and expressly excluded from scope of the PIAs conducted to date. The result is that most of the PIAs have not squarely addressed the impact of the Data Standards as such.

This does not necessarily mean that there were errors, gaps or weaknesses in previous PIAs conducted on the CDR scheme at the time they were conducted. It would be difficult to determine whether any errors, gaps or weaknesses existed without effectively re-conducting each assessment from scratch. Even then, it should be borne in mind that any particular PIA will have been impacted by the circumstances in which it was conducted or commissioned. PIAs are often conducted, or commissioned, in less than perfect circumstances. What can be achieved in any particular PIA will be limited by factors including the Terms of Reference provided, the risk appetite of the organisation, the timeframe in which the assessment is to be conducted or completed, the budget available, the availability of internal teams or subject matter experts to provide input, the amount of detail available for review, the availability of external stakeholders including regulators or affected individuals to be consulted on the potential privacy impacts, and the client's willingness to engage with external stakeholders.

In any case, PIAs reflect an assessment conducted at a particular point in time. Therefore, to suggest now that fresh PIAs should be conducted on the CDR scheme is not in itself a suggestion that there were deficiencies in any of the previous PIAs conducted on the scheme. Instead, it is a reflection of the fact that the CDR scheme is evolving, and expanding out to different sectors.

7.2 The need for fresh PIAs

The DSB has relatively recently changed from a quasi-independent Commonwealth Corporate Entity (CSIRO) to a central Australian Government Department (Treasury). The DSB and the Chair are therefore now bound by the Australian Government Agencies Privacy Code (**AGA Privacy Code**).[120] This makes PIAs mandatory for any changes which amount to 'high privacy risk projects'. The OAIC has provided guidance on the factors it regards as giving rise to 'high privacy risk projects' under the AGA Privacy Code and a number of these are present in the CDR scheme overall, as explained below.[121]

It is important to note that there are two intersecting legal frameworks here. As discussed in Section 7.4, there are factors that determine what constitutes 'high privacy risk projects'; these are set by the OAIC. This is distinct from the Business Impact Level Tool in PSPF Policy 8, which was described in Section 4.1.3. Thus it is not necessarily the case that 'high privacy risk projects' will correspond with projects with potential for 'high' business impact level risks. However, the process of determining what gives rise to 'high privacy risk' in the CDR scheme (including the Data Standards) on an ongoing basis would be greatly assisted by the development and adoption of a Risk Management Framework for the Data Standards. This is because such a Framework, also drawing on Threat Modelling (see the UNSW Threat Report), provides a basis for understanding the likelihood and impact of (*inter alia*) privacy risks.

The Data Standards are intended to be, and in fact are, regularly amended. Each time the CDR scheme updates or evolves creates a fresh opportunity to deliver benefits to consumers; but also to potentially create privacy risks which should be assessed and where possible mitigated.

A number of the PIAs in 2019 had terms of reference which excluded, for example, the application of the CDR scheme other than its initial implementation in the banking sector. Later PIAs focussed on the expansion of the CDR to the energy sector in particular. The coverage of the Data Standards will soon expand beyond banking and energy to other sectors and thus create entirely new categories of Data Standards, which require a different assessment of the privacy impact as they will pose different risks to any Data Standards that have been assessed before. For instance, the data held by and valued by telecommunications companies is different to the data held by banks.

An analogy here is the safety testing of motor vehicles. When a brand new vehicle type is first developed, it will go through 'crash test dummy' safety testing. Over the years, changes will be made to that vehicle line. Some changes will be minor, such as a change in paint colour, which will not require fresh safety testing. But structural changes made to the design of a new model within the same vehicle line will potentially introduce new areas of safety risk, and therefore a fresh set of safety testing must be conducted.

As expansions are layered upon previous changes to the CDR scheme, it is occasionally necessary to step back and look at the whole, rather than just each change in isolation.

We recommend that a PIA be conducted on draft Data Standards associated with each such expansion of the CDR scheme, in order to consider what new privacy risks might arise. The PIA should take a holistic, 'scheme-wide' view, rather than focus on only one element such as the Data Standards. The PIA should include consideration of which of those risks can be resolved through careful crafting of the Data Standards, versus applying other levers.

An alternative analogy is that of the development over time of a building site. If it is proposed to build a single storey house on a site, various land use, environmental impact and engineering assessments will look at ensuring that the foundations will be stable, and that the structure and services will be suitable for the occupants of a single storey dwelling. Later on, a second storey may be added, and a fresh assessment will look only at the impacts of the incremental change of adding that second storey. Later again, an extension is made to change the footprint of the building, and again an assessment will be made only of the incremental impact of the proposed changes to the dwelling. But eventually, perhaps when a third story is proposed to be added, there is a point at which it is necessary to step back and look at the entire building in relationship to the site, to judge whether or not the site and the building's foundations and services are still fit for purpose to support the building and its occupants. What might have been suitable for a small number of occupants may no longer be suitable following years of incremental changes which impact on the stability of the original foundations, or the ability of the waste water systems to cope. Further, the collateral impact on neighbours may have been exponential, rather than incremental, as the house has grown over time.

A fair question though is whether, when the initial building was being designed and built, if it was already foreseen or even planned that there would eventually be new stories added to the building, should the initial assessment of the plans have been limited in its scope to only the initial phase of the project?

7.3 PIAs explained

7.3.1 What is a PIA and what does it measure?

A PIA is a comprehensive tool for assessing new initiatives, whether technical, policy or legislative. Together, we refer to these as 'projects' in the broadest sense.

PIAs are usually undertaken as part of a sound project management strategy, to assess whether it is safe to proceed to the implementation phase of a significant initiative. A failure to properly embed appropriate privacy protection measures may result in a breach of privacy laws, or prohibitive costs in 'retro-fitting' a system to ensure legal compliance or address community concerns about privacy.

At a minimum, a PIA:

› *is a written assessment of an activity or function that:*

  a. *identifies the impact that the activity or function might have on the privacy of individuals; and*

  b. *sets out recommendations for managing, minimising or eliminating that impact.*[122]

In practice, PIAs also typically assess impacts on, or risks for, the organisation/s involved in the project.

Privacy impacts from a project can be positive or negative. Negative privacy impacts (i.e. risks) to arise from a project can be categorised as either:

› **A legal compliance risk for the organisation** – i.e. non-compliance with the applicable privacy law/s,

› **A reputational risk for the organisation** – i.e. not meeting customer / stakeholder / community expectations about personal information handling, even if the law allows the activity, and/or

› A **risk for affected individuals of suffering a privacy-related harm** because of the project.

What is meant by a *privacy-related* harm in the context of the CDR is discussed in Section 6.4.

7.3.2 When are PIAs required by law?

The conduct of a PIA is mandated by law, under a Privacy Code which has the status of a statutory instrument, when Australian government agencies, such as the Chair, are considering 'high privacy risk' projects.[123] An obligation to conduct a PIA may also be inherent in the agency's obligations under APP 1 in the Australian Privacy Principles in the Schedule to the Privacy Act 1988. The OAIC has found the Australian Federal Police in breach of both the Privacy Code and APP 1 for failure to conduct a PIA on a 'high privacy risk' project.[124]

In *Appendix 7B*, we outline circumstances in which PIAs are expected but not required by the OAIC and predicted changes as to when PIAs will come to be required by law.

7.3.3 What should a PIA achieve?

A PIA should be enabling. It should offer a roadmap to achieve the project objectives, in a way which also respects and protects privacy. A PIA report should describe and de-mystify the initiative, identify and analyse the privacy implications, and make recommendations for minimising privacy intrusion, and maximising privacy protection – while ensuring the initiative's objectives are met.

This will typically involve examining a particular project in terms of:

› compliance with the Australian Privacy Principles (APPs) under the *Privacy Act 1988* (Cth) and/or other privacy laws (e.g. the CDR Privacy Safeguards), and

› community or stakeholder expectations (testing the project will have a 'social licence').

In that sense, a PIA can be considered to cover both law and ethics.

7.3 PIAs explained (continued)

PIAs should examine both:

- End-to-end **data flows** for a project; i.e. ensuring the proposed collection, use and disclosure of personal information will be lawfully authorised; and
- End-to-end **data governance** at the organisation/s involved in the project, including ensuring data quality, pathways for applicants to seek access to and/or correction of the personal information held about them, retention and destruction of personal information, and the proposed management of privacy complaints and data breaches.

PIAs should therefore assess both project / program / system design, and the policies, procedures and governance supporting rollout and implementation.

Benefits of conducting a PIA

A PIA is a practical and pragmatic tool that can provide numerous benefits, such as:

- Enhancing the legitimacy of the project:
  - Gaining public / stakeholder trust for the organisation,
  - Developing a 'social licence' for the handling of personal information as part of the project, and
  - Demonstrating accountability and transparency, by providing a record that can be shared with project partners, privacy regulators, or customers and other stakeholders.
- Offering an early warning system of potential privacy problems:
  - Identifying gaps in processes or practices,
  - Identifying potential stakeholder concerns or 'myths' to be addressed,
  - Helping to ensure compliance with legal obligations,
  - Identifying risk, and taking effective action to mitigate risk, and
  - Avoiding inadequate solutions, unnecessary costs, potential harms to individuals or reputational risks for the organisation.
- Improving project outcomes:
  - Determining early who will be responsible for what,
  - Facilitating collaboration between different parts of the business, and
  - Educating and raising privacy awareness amongst employees.

7.4 When PIAs should be conducted for the CDR scheme

A Privacy Impact Assessment is mandatory for 'high privacy risk' projects conducted by Australian government agencies. In relation to the CDR scheme, we suggest it is necessary to take a view of the scheme overall, rather than particularising how any particular app or use case or set of technical standards will work.

There are a number of elements to the expansion of the CDR scheme to new sectors (energy, telecommunications etc), which in our view reflect many of the factors which the OAIC considers to pose an inherently 'high' level of privacy risk. (See further discussion of PIAs in *Appendix 7C* for the full list of 'high risk' factors.)

For the CDR scheme overall, those elements will or could include:

- handling large amounts of personal information,
- handling personal information of individuals with particular needs,
- handling personal information in a way that could have a serious consequence for an individual or a group of individuals, and/or
- the following activity-based risk factors:
  - using or disclosing personal information for secondary purposes,
  - using or disclosing personal information for profiling or behavioural predictions,
  - using personal information for automated decision-making,
  - systematic monitoring or tracking of individuals, and
  - data matching (linking unconnected personal information) or data linkage.

We recommend that a PIA be conducted on the draft Data Standards for each expansion of the CDR scheme to a new sector, in order to consider what new privacy risks might arise. The PIA should take a holistic, 'scheme-wide' view, rather than focus on only one element such as the Data Standards. The PIA should consider which of those risks can be resolved through careful crafting of the Data Standards.

Appendix 7C provides more detailed recommendations about developing and embedding a PIA Framework.

7.5 Framing the scope of PIAs on the CDR scheme in future

Triggers for requiring a fresh PIA should include:

- The on-boarding of new sectors,
- The on-boarding of new data types,
- Any new functionalities or features,
- As part of the development process for new or significantly amended Data Standards

In the context of the CDR, since the development of the Data Standards is not of itself a process which involves the handling of personal information, it could be tempting to find that the standards-creation activity is not worthy of examination for privacy impacts. However, this would be to take an overly narrow view of the role played by the Data Standards in the overall CDR ecosystem.[125]

We also recommend that each time there is a significant change to the CDR scheme, such as when it is to be expanded to a new sector of the economy, or a significant change in Data Standards, that is the point in time to conduct a deliberately wide review of the entire ecosystem. The scope of the PIA at that point should include first an audit of how the system is already operating (i.e. a privacy audit of how things have been working in 'business as usual' mode), and then consideration of what new risks might be introduced if or when the proposed new sector is brought on board.

While we suggest that it is not necessary to second-guess the analysis and findings of all past PIAs (see Section 7.1 above), it can be worth looking at the recommendations made in previous PIAs. A review of which recommendations were not followed or implemented, and why, can be a useful jumping off point for a new PIA. This could help ensure that nothing has 'slipped through the cracks' over time.

The scope of any future PIA should be deliberately broad, to avoid some of the general or 'typical' problems with PIAs, such as:

- Treating a PIA as only a legal compliance check,
- Reviewing elements in isolation,
- Failure to test the technology or functionalities being assessed,
- Failure to test for necessity, legitimacy and proportionality of any personal information-handling activities – instead the public interest objectives (and the likelihood of achieving them) must be considered when balanced out against any privacy-invasive impacts,
- Failure to consider customer expectations and the role of social licence in gaining trust, or
- Failure to think about the full range of mitigation levers

The scope of new PIAs – in other words, what should be included in any Request For Quotation, initiating brief or terms of reference when commissioning a new PIA – should encompass:

- A description and assessment of the end-to-end data flows, both for lawfulness of the data flows, and to measure against the 'necessity, legitimacy and proportionality' metrics promoted by the OAIC.
- Testing of technology or functionalities involved, to ensure they do what is claimed of them.
- A description and assessment of the data governance at the organisation/s involved, including ensuring data quality, pathways for applicants to seek access to and/or correction of the personal information held about them, retention and destruction of personal information, and the proposed management of privacy complaints and data breaches.
- Assessment of project / program / system design, and the policies, procedures and governance supporting rollout and implementation.
- Consideration of any legal compliance risk for each category of participating organisation – i.e. non-compliance with the applicable privacy law/s by each player in the CDR ecosystem. A PIA should not only be about assessing *Treasury's* compliance with the Privacy Act or the CDR Privacy Safeguards; it should consider each category of entity such as data holders and data recipients as well.
- Consideration of any reputational risks for each category of participating organisation, as well as for the public acceptance of the CDR overall – i.e. assess the risk of not meeting customer / stakeholder / community expectations about personal information handling, even if the law allows the activity.
- Consideration of any risks to affected individuals of suffering a privacy-related harm because of the project.
- A review of any outstanding recommendations from past PIAs, if they are still relevant.
- Consideration of how current or likely future proposals for law reform might impact on the Scheme or on categories of participating entities, such as the current review of the Privacy Act; and
- Development of recommendations to mitigate risks to any participating organisation, and to mitigate negative privacy impacts for individuals, and/or to strengthen privacy-preserving or privacy-enhancing outcomes.

The Chair should also consider the capabilities required to conduct a PIA, having regard to the nature and size of the project; the range of expertise required; and the likely need for external assessors where the impact of the project is very substantial. Our recommendations on the capabilities required to conduct a PIA are included in *Appendix 7D.*

Glossary

ACCC is the Australian Competition and Consumer Commission

Accountable Authority has the meaning given in the PGPA Act. The Accountable Authority of the Department of the Treasury (designated to perform the functions of the DSB) is the Secretary.

Accredited Data Recipient (ADR) has the same meaning as accredited data recipient in CCA s 56AK.

Action Initiation refers to the recommendation that the CDR should enable third parties to initiate actions beyond read-only requests for data sharing.

AGA Privacy Code refers to Privacy (Australian Government Agencies - Governance) APP Code 2017.

Authorised means within the scope of legal requirements and permissions, including statutory requirements and the terms of any policy or notice provided to affected persons and any relevant consumer consent, and not an act or practice that is otherwise misleading or deceptive.

Availability is the property that data or information is accessible and useable upon demand by an authorised person.

BIL is a reference to the Business Impact Levels tool in PSPF Policy 8.

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

Chair means the Data Standards Chair.

CSO means a Chief Security Officer (a role within the PSPF).

Confidentiality is the property that data is not made available or disclosed to unauthorised persons or unauthorised processes or for use in an unauthorised manner. Disclosure of data within an entity for use in an unauthorised manner is an adverse event that affects confidentiality of that data, even where there is no disclosure to persons or entities external to that entity.

Consumer Data Right (CDR) is established in CCA Part IVD.

CDR data has the same meaning as in CCA s 56AI.

CDR ecosystem refers to the network of Data Holders, ADRs, Trusted Advisers, CDR consumers and CDR data.

CX refers to Customer Experience.

Data Holder has the same meaning as data holder in CCA s 56AJ.

Data minimisation principle means the principle that personal data shall be limited to that which is necessary for the purpose for which it is processed. That is the entity handling the personal data should identify the minimum amount of data necessary to fulfill the relevant purpose, and hold no more than that data.

Data Standards refers to data standards issued by the Chair in accordance with the provisions of Division 6 of CCA Part IVD.

Data Standards Body (DSB) is a secondary statutory structure contemplated in Subdivision C of Division 6 of CCA Part IVD. The Department of the Treasury is currently appointed as the DSB.

DTA means the Digital Transformation Agency.

Information Security Manual (ISM) has the meaning given in PSPF Policy 11. The purpose of the ISM is to outline a cybersecurity framework that organisations can apply, using their risk management framework, to protect their information and systems from cyber Threats. The ISM is intended for Chief Information Security Officers, Chief Information Officers, cybersecurity professionals and information technology managers.

Integrity is the property that data has not been altered or destroyed in an unauthorised manner.

Likelihood means the probability that a given threat event is capable of exploiting a vulnerability to cause harm.

OAIC is the Office of the Australian Information Commissioner.

Operational safeguards are operational or administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect CDR data and to manage the conduct of an entity's personnel in relation to permitted use and disclosure and protection of that information.

PGPA refers to the *Public Governance, Performance and Accountability Act 2013* (Cth).

PIA means a Privacy Impact Assessment.

Privacy Safeguards are set out in CCA Pt IVD Div 5.

Pt IVD refers to Part IVD of the CCA.

PSPF refers to the Protective Security Policy Framework.

Risk refers to the effect of uncertainty on objectives.

Risk management refers to the implementation of security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

Risk Management Framework has the same meaning as that term in the Risk Policy. It is a structured process for identifying and analysing risks, vulnerabilities to threats, likelihood of threats, and likelihood and impact of harms. That process is intended to be used to determine whether, when, how, and to what extent particular risks and vulnerabilities should be addressed through actions taken by an entity, and to guide an entity to establish a system of safeguards to mitigate risks and vulnerabilities, and associated controls to assure and verify that these safeguards operate reliably, such that residual risks (after operation of these safeguards and controls) of relevant harms are very low. See further Australian Standard AS ISO 31000:2018 Risk Management Guidelines at Section 5 - Framework.

Risk Policy refers to the Commonwealth Risk Management Policy.

Rules refers to the Consumer Data Rules made pursuant to CCA Part IVD Div 2A.

Safe handling of CDR data means handling of CDR data in a manner and for a purpose that is both secure and authorised.

Secretary means the Secretary of the Department of the Treasury.

Security risk assessment refers to the conduct of an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of CDR data held by an entity and other persons and entities for whom that entity is responsible.

Security standards are standards that address how an entity (1) ensures the confidentiality, integrity, and availability of CDR data that it creates, receives, maintains, or transmits; (2) protects against any reasonably anticipated threats and hazards to the security or integrity CDR data; (3) protects against uses or disclosures of CDR data that are not permitted; and (4) ensures compliance by its personnel, subcontractors and other persons and entities for whom that entity is responsible with the above.

Shared Risk has the same meaning as in the Risk Policy.

Technical safeguards are technology, and the policy and procedures for its use, that protect CDR data and manage the conduct of an entity's personnel in relation to permitted use and disclosure and protection of that information.

Threat is anything that has the potential to prevent or hinder the achievement of objectives or disrupt the processes that support them.[126]

Threat sources means the sources of the threats causing a negative impact on CDR data and stakeholders in CDR data, including CDR consumers. Threat sources may be Threat Actors or events.

Trusted Adviser has the same meaning as in Rule 1.10C.

UNSW Threat Report means Lyria Bennett Moses, Richard Buckland, Rahat Masood & Benjamin Turnbull, *Considerations for managing cyber threats to the Consumer Data Standards: A Report to the Data Standards Chair* (UNSW, 2022).

Vulnerabilities are flaws or weaknesses in a system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat event.

Appendices

Appendix 3A - Research on trust and attitudes to privacy

A multi-year, eight-nation research project by the World Economic Forum (**WEF**) and Microsoft sought to measure the impact of context on individuals' attitudes towards privacy and the use of their personal information.[127] Their research made two critical findings.

First, there are four types of factors which influence an individual's degree of trust in any given proposal to use their personal information:

1. the situational context – i.e. the nature of the proposal itself;
2. demographics – research has shown that an individual's gender, age, ethnicity and country of origin can each influence the value they place on privacy;
3. culture – local cultural norms also play a part; and
4. perceptions – about the strength of legal protections available, as well as about the individual's own level of confidence navigating technology.

From an organisational point of view, a player in the CDR ecosystem will only have control over the first of those four factors: the situational context.

Second, in terms of the situational context, there are seven variables that individuals consider, when determining whether they would accept any given scenario involving the use of their personal information. Interestingly, the single most important variable affecting the 'acceptability' of a scenario was not the type of data at issue, the way it was proposed to be used, the type of organisation or institution seeking to use it or even the pre-existing level of trust enjoyed by the particular organisation proposing the project – but the method by which the personal information was originally *collected*.

In terms of the method of collection, any given set of personal information may be broadly categorised as having been directly provided by the subject, indirectly provided via another party, observed, generated or inferred. An individual's ability to control how his or her personal information may be used depends on both an awareness of the collection and control over that collection. As awareness and control over the point of collection lessen, so too does trust in the subsequent use of that data. Understanding how personal information is *collected* therefore becomes critical to understanding the likely community expectations around the *use* of that data.

Further, the WEF research found that the type of entity proposing the project – i.e. the sector the organisation is in, such as healthcare, finance, government etc – turned out to be the *least* important of all the variables.

Therefore, trust in data-related projects is specific to the use case and the design of each project, as well as the type of customers to be affected, far more than it is about underlying levels of trust in particular organisations or sectors.

So – how can an organisation gain its social licence to use personal information, for a particular use case? How can CDR players *build* trust in their projects?

In addition to addressing the variables highlighted in the WEF research, the Chair and the DSB should consider the importance of transparency. Qualitative research conducted in New Zealand on behalf of the Data Futures Partnership found that being transparent about how data is proposed to be used is a crucial step towards community acceptance.[128]

In particular, customers and citizens expect clear answers to eight key questions:

Value

- What will my data be used for?
- What are the benefits and who will benefit?
- Who will be using my data?

Appendices

Protection

- Is my data secure?
- Will my data be anonymous?
- Will the minimum amount of personal data be collected to fulfil this purpose?

Choice

- Can I see and correct data about me?
- Will I be asked for consent?
- Could my data be sold?

The answers to those questions will be different for every project and have almost nothing to do with the pre-existing level of trust enjoyed by any particular entity or brand.

Therefore, CDR players should ask not whether customers trust *them*; they should ask whether they have designed each data project to incorporate the elements needed to make those projects *trustworthy.*

Appendix 4A - PSPF

PSPF Principles

1. Security is everyone's responsibility. Developing and fostering a positive security culture is critical to security outcomes.
2. Security enables the business of government. It supports the efficient and effective delivery of services.
3. Security measures applied proportionately protect entities, people, information and assets in line with their assessed risks.
4. Accountable authorities own the security risks of their entity and the entity's impact on shared risks.
5. A cycle of action, evaluation and learning is evident in response to security incidents.

PSPF Outcomes

- **Governance**

  Each entity manages security risks and supports a positive security culture in an appropriately mature manner ensuring:
  - clear lines of accountability,
  - sound planning,
  - investigation and response,
  - assurance and review processes,
  - proportionate reporting.
- **Information**
  - Each entity maintains confidentiality, integrity and availability of all official information.
- **Personnel**
  - Each entity ensures its employees and contractors are suitable to access Australian Government resources, and meet an appropriate standard of integrity and honesty.
- **Physical**
  - Each entity provides a safe and secure physical environment for their people, information and assets.

Relevant PSPF Policies

PSPF Policy 1, which establishes that the Accountable Authority (including the Secretary of the Department of the Treasury) is answerable for the security of their entity including the management of security risks.

PSPF Policy 2, which requires the Accountable Authority to appoint a Chief Security Officer (CSO) to be responsible for the security of the entity and empowered to make decisions about protective security planning, practices and procedures. This policy also requires the Accountable Authority to ensure personnel and contractors (including, here, those working on Data Standards) are aware of their collective responsibility to foster a positive security culture.

PSPF Policy 3, which concerns security planning and security risk management as part of the wider risk management framework (see HB 167: 2006). This policy requires each entity to have a 'security plan' that details the:

- security goals and strategic objectives of the entity, including how security risk management intersects with and supports broader business objectives and priorities,
- threats, risks and vulnerabilities that impact the protection of an entity's people, information and assets (the limitation here to the entity's people, information and assets is discussed in Section 4.2.2),
- entity's tolerance to security risks,
- maturity of the entity's capability to manage security risks,
- entity's strategies to implement security risk management, maintain a positive risk culture and deliver against the PSPF.

PSPF Policy 4, concerning security maturity monitoring.

PSPF Policy 5, concerning security reporting (including on key risks to the entity's people, information and assets).

PSPF Policy 7, Security Governance.

PSPF Policy 8, concerning information holdings and sensitivity and security classification.

PSPF Policy 10, concerning safeguarding data from cyber threats (including implementation of the "Essential Eight" (a PSPF maturing rating of 'Managing' corresponds to Maturity Level Two for each of the Essential Eight).

PSPF Policy 11, requires entities to ensure that "their" ICT systems meet the security requirements under the ISM.

Appendix 5A - Systemic risk of cross-sectoral expansion of the CDR system

Risk of instances of mishandling or other unauthorised collection, use or disclosure of CDR data is likely to increase with cross-sectoral expansion of the CDR system.

A number of factors are likely to contribute to this growing systemic risk:

Firstly, the range of possible data recipients and data intermediaries is expanding beyond Australian financial services providers that have experience in implementing three lines of defence and like business, prudential and technological risk assurance risk assurance frameworks and measures in order to comply with regulatory requirements.

As compared to financial services sector-regulated entities,[129] many entities likely to enter the cross-sectoral CDR system will have lower levels of organisational data maturity in assessing, mitigating and managing residual technology, security and other operational risks, and in tracking and assurance of data provenance (was the data of appropriate quality and collected, used and disclosed only as authorised?) and decision provenance (was the decision appropriate to the data, and reliably and verifiably attributable to fair and reasonable analysis of that data?).

Participants with lower levels of data maturity may align systems and documented practices and practices with regulated requirements, but fail to ensure that controls and safeguards are effective to reliably assure both (1) compliance with mandatory requirements, and (2) mitigation of other risks of harms that are not addressed by mandatory requirements, including

Appendices

identification and mitigation of risks that particular uses and disclosures of data may fall within the letter of the permissioning framework but not be consistent with reasonable consumer expectations, as informed by relevant permissioning notices and consents.

Through lower levels of organisational maturity, instances of mishandling or other unauthorised collection, use or disclosure of CDR data are more likely to occur.

Second, assessment, mitigation and management of technology, security and other operational risks, and tracking and assurance of data provenance and decision provenance, is:

- simpler when CDR data is being handled for a like-for-like product or service comparison and possible switch within a sector,
- more complex as relevant products or services for which CDR data is being used within a sector become more heterogenous, and
- more complex again when the services compared are cross-sectoral.

For example, to provide a service as to specification and pricing of options for household energy capture and storage options including solar and electric vehicle, a service provider may obtain a customer's consent to access CDR data sets that include bank transaction statements (energy and fuel spend data); gas statements and gas meter data; electricity statements and electricity meter data; and other data sets identifying of particular customers or their households (i.e. Google StreetView and Google Maps images used to analyse roof surfaces as to suitability for solar panel installations).

Integration and analysis of diverse data sets is more likely to require use of and disclosures by a CDR data participant to subcontractors to that participant (that should only be acting as data processors of derived CDR data, with relevant data remaining controlled by, and only used at the direction of, the relevant data participant.

Third, increases in heterogeneity of data sets and in number of separate entities within a data ecosystem controlled by a particular data recipient and involving sharing of derived CDR data, raise risks of unauthorised uses and disclosures of derived CDR data.

Systemic risks are higher in data ecosystems where incentives operating at the enterprise level – that is, incentives (either positive, through financial benefit, or to avoid penalties and sanctions) upon individual participants as to identification and mitigation of risk of harms to those participants or their customers - do not closely align with the preconditions that need to be satisfied to ensure sustainable trustworthiness (as perceived by consumers) at the system level.

The prospect of operation of misleading and deceptive conduct and unfair contract terms provisions of Australian Consumer Law and possible enforcement action by the ACCC is often sufficient incentive for entities to ensure congruence between their data handling acts and practices and their consumer terms that are the permissioning mechanism for those acts and practices. However, a broader range of entities will participate in the CDR system following sectorial expansions of the CDR scheme.

With anticipation of lower levels of data maturity of some incoming data participants, coupled with risks of systemic harms to the CDR system that may be occasioned through consumer reaction to reports of poor or unreliable data handling by some CDR participants, it may be prudent to consider more prescriptive criteria as to appropriate data handling practices of CDR participants.

More prescriptive criteria could be implemented through accreditation criteria, or through data standards.

The key selection criteria should be ensuring that requirements as to responsible data governance are sufficiently clearly stated to create appropriate incentives for data participants to specify, implement and verify reliable operation of safeguards to mitigate risks of mishandling or other unauthorised collection, use or disclosure of CDR data. Attributes of *safeguards* reasonably required to mitigate risks of mishandling or other unauthorised collection, use or disclosure of CDR data need to be specified with sufficient particularity to enable appropriate *controls* to address those risks to be specified, implemented and tested.

Controls assessed through testing and verification consistent with ASAE 3150 (Assurance Engagements on Controls) and like standards may only be effective to address relevant risks if the safeguards to be verified by those controls are appropriately comprehensive. Assurance through verification of controls depends upon appropriate scoping of safeguards that are then to be the subject matter of controls.

The CDR regulatory framework may reasonably be described as prescriptive as to both scope and level of detail of mandated CDR data assurance measures that data participants must implement to address the privacy safeguards and assure information security. High level of prescription carries risk that less data mature participants may see compliance with detailed requirements as ensuring that their practices in handling of CDR data are appropriately trustworthy, as well as legally compliant.

This may lead to a **reference frame problem**. Where complex requirements are stated at a level of detailed prescription, less data mature entities may regard addressing the list of regulated requirements with controls and safeguards addressing each of those requirements as implementation of a comprehensive risk management program. The list of regulated requirements becomes the reference frame for cataloguing of risks to be mitigated and managed, leaving exposure to risks outside that reference frame. Compliance with in-scope detailed requirements may be addressed through safeguards and assured through controls, but out-of-scope pre-conditions to reliable trustworthiness in process and practices for handling of derived CDR data by a data participant and other entities with whom that data participant interworks in handling of derived CDR data may not be addressed through (non-mandated) safeguards and associated controls tested through assurance engagement on controls.

Appendix 5B - Criteria for risk-based assessment by the Chair about coverage and framing of Data Standards

The Chair is *empowered* to make one or more data standards about:

- the format and description of CDR data;
- the disclosure of CDR data;
- the collection, use, accuracy, storage, security and deletion of CDR data;
- de-identifying CDR data, including so that it no longer relates to an identifiable person, or a person who is reasonably identifiable: section 56FA CCA.

The Chair is *mandated* by Rule 8.11 of the Rules to make standards in relation to a subset of those matters (**the Rule 8.11 standards subset**).

This mandated subset principally relate to:

- the form and content of instructions that CDR consumers and CDR participants respectively give in order to initiate processing of CDR data and production of derived CDR data by data participants,
- processes, formats and protocols for presentation of CDR data, and communication of CDR data, in response to requests,
- processes for authentication and validation of requests and responses,
- pathways for passage of requests and CDR data content, between data participants,
- measurement, monitoring and reporting of systems as to security, performance and availability in relation to the above.

The Chair is therefore otherwise empowered, but not required, to make Data Standards as to each and any ADR's processes and practices in collection, use, accuracy, storage, security and deletion of CDR data.

Data Standards complement and supplement:

- mandatory requirements for data recipients to implement privacy safeguards as stated in sections 56EA to 65EM (Div 5 of Part IVD) of the CCA, and Rules 7.2 to 7.16 of Part 7 (Rules relation to privacy safeguards) and Schedule 2 (Steps for privacy safeguard 12 – security of CDR data held by ADRs) of the Rules,
- mandatory requirements for data recipients to attain and maintain accreditation under section 56CA of the CCA and Rules 5.1 to 5.34 of Part 5 (Rules relating to accreditation) and Schedule 1 (Default conditions on accreditations) of the Rules.

Appendices

The Chair may wish to determine the scope of activities in making Data Standards, and ordering of the priority of those activities, having regard to:

1. the statutory imperative to make and maintain the Rule 8.11 Data Standards subset,
2. the Chair's assessment as to the level of need (risk of adverse impact, and level of adverse impact), if a possible, other within-scope, Standard is *not* made: that is, the counter-factual.

That assessment might be made having regard to:

1. likelihood of efficient operation of (1) market forces in a particular CDR sector, to lead to a desired outcome without a standard being made, (2) other controls and safeguards within the CDR regulatory framework, to address the identified concern, and (3) other behavioural incentives and incentives, such as adverse media or consumer opprobrium, that affect decisions of CDR participants and that may obviate any imperative for a relevant standard to be made,
2. best fit of CDR standards-making activity with complementary mechanisms under the CDR framework, and activities of the ACCC and OAIC as other CDR regulators, to the extent that the respective regulators are empowered to use those mechanisms. Those other mechanisms include amendment to Rules; amendment to accreditation criteria, and issue of guidelines and guidance issued by the ACCC, OAIC or Chair,
3. availability of resources to draft, consult about, make and maintain other within-scope standards that the Chair might elect to propose, and prioritisation of scarce regulatory resources to address assessed level of need.

In determining whether to propose other within-scope standards, the Chair's assessment, made in consultation with other regulators including the ACCC and the OAIC, as to the counter-factual should include assessment as to the level of risk and possible impact of

1. harms that CDR consumers may suffer if Data Standards are (1) not made, and then (2) not complied with.
2. adverse effect upon the number of potential CDR consumers willing to consent to service providers using the CDR framework, due to loss of perceived trustworthiness of the CDR framework.

This adverse effect would lead to benefits foregone for potential CDR consumers, and for the Australian economy, as information symmetries between incumbent service providers and consumers would then continue to restrict informed selection by consumers of best fit services and to impede switching by consumers between service providers.

Accordingly, this adverse effect is a form of systemic or societal harm to the ongoing sustainability of the CDR system itself. Privacy safeguard principles and the data minimisation principle operate to confine the nature and extent of permissions that may be sought. The current Rules expand upon the principles to include control assurance requirements as to compliance with permissions and as to ensuring information security. The current Rules state detailed requirements for an ADR to implement a formal controls assessment program in relation to information security (paragraph 1.6 of Schedule 2, including specific information security control requirements (1) to (6) in Part 2 of Schedule 2). However, and as noted in Section 2 of this report, the current Rules do not create a substantive legal requirement:

- that an accredited entity implement a data management program to ensure that data environments are appropriately controlled,
- that an accredited entity take active steps to ensure that outputs allowed to egress those data environments are appropriately assessed and controlled by the data recipient to ensure that uses of those outputs are reliably and verifiably confined to reasonable expectations of the CDR consumer, as informed by relevant permissioning notices and consents.

The current Data Standards create guardrails as to form, content and some aspects of the customer experience as to permissioning requests for CDR data to pass through the CDR system, and as to presentation and information security of CDR data passing through the CDR system and into data environments controlled by participants (and other entities for whom they are responsible).

The current Data Standards do not address the characteristics of a data management program to ensure that data environments are appropriately managed, or that outputs allowed to egress those data environments are appropriately assessed and controlled by the data recipient to ensure that uses of those outputs are reliably and verifiably confined to reasonable consumer expectations, as informed by relevant permissioning notices and consents.

If it is accepted that regulated entities should be required to develop data management programs to better assess, mitigate and manage risks as to safe use of CDR data that are not information security risks already addressed by required CDR data assurance measures, the question then arises as to the relative roles of changes to accreditation criteria or changes to data standards.

Rule 5.12 of Part 5—*Rules relating to accreditation etc.* of the Rules states a general obligation of an accredited person to "take the steps outlined in Schedule 2 which relate to protecting CDR data from, among other things, (i) misuse, interference and loss; and (ii) unauthorised access, modification or disclosure", subject to:

1. specific exceptions and conditions for different designated sectors, as stated in sector Schedules, and
2. streamlined accreditation under rule 5.5.

The Default conditions on accreditations, for accredited persons without streamlined accreditation, include preparation and provision to the Data Recipient Accreditor of:

1. an assurance report for each reporting period, being for a person with unrestricted accreditation—a report that is made in accordance with (i) ASAE 3150; or (ii) an approved standard, report or framework; and for a person with sponsored accreditation, an assessment of its capacity to comply with Schedule 2 that is made in accordance with any approved requirements; and
2. an attestation statement for each reporting period, being for a person with unrestricted accreditation—a statement in the form of a responsible party's statement on controls and system description that is made in accordance with ASAE 3150; and for a person with sponsored accreditation—a statement about its compliance with Schedule 2 that is made in accordance with any approved requirements.

Schedule 2—*Steps for privacy safeguard 12—security of CDR data held by ADRs* expressly relates only to privacy safeguard 12 as stated in subsection 56EO(1) of the CCA and elaborated in rule 7.11 and paragraph 5.12(1)(a) of the Rules.

Information security capability of a data recipient is not solely limited to technical capability to detect and mitigate risks of *external* security threats to CDR data as managed within information technology systems of a data recipient and other entities for whom it is accountable. *Information security capability* means ability to manage security of a CDR data environment in practice through the implementation and operation of processes and controls, and includes the ADR being able to allocate adequate budget and resources, and provide for management oversight. Controls to be implemented following the steps in Schedule 2 Part 1, and including the *Minimum information security controls* in Schedule 2 to the Rules, must be informed by an information security policy that details:

1. an accredited person's information security risk posture to address its assessed exposure and potential for harm to the ADR's information assets, including CDR data that it holds, from security threats to its CDR data environment and its operating environment, and
2. how its information security practices and procedures, and its information security controls, are designed, implemented and operated to mitigate those risks.

The boundaries of information technology systems used for, and processes that relate to, the management of CDR data (CDR data environments) must be assessed, defined and documented, and subject to the controls.

However, compromises to safe handling of CDR data within those CDR data environments, or through allowing outputs to egress those CDR environments that are not properly assessed as within scope of relevant customer authorisation, would not appear to fall within *information security controls* as addressed in Schedule 2 to the Rules. New data standards could address the characteristics of a data management program to ensure that data environments are appropriately managed and that outputs allowed to egress those data environments are appropriately assessed and controlled by the data recipient.

Appendices

Appendix 5C - Operation of the Privacy Safeguards in relation to management by ADRs of their data environments

ADRs are required to manage received CDR data in data environments that are operated in accordance with Rule 7.2, Rule 7.11 and Schedule 2.

There is complexity, and associated uncertainty, as to coverage of these rules in relation to ADRs ensuring that CDR data is used only within the scope of authorisations granted by relevant consents, as distinct from ADRs ensuring information security of CDR data.

This complexity is outlined below.

Privacy safeguard 1—*open and transparent management of CDR data* (section 56ED) requires each CDR entity:

1. to manage CDR data in an open and transparent way,
2. to take such steps as are reasonably in the circumstances to implement practices, procedures and systems that will ensure that the CDR entity complies with Part IVD of the CCA and the Rules,
3. to have and maintain a clearly expressed and up-to-date policy that is about the CDR entity's management of CDR data, is in a form approved in accordance with the consumer data rules, and which contains information specified for inclusion in subsections 56ED(4), (5) and (6), relevantly including:
    a. the classes of CDR data that is or may become held by (or on behalf of) the CDR entity as an ADR, and how such CDR data is held or is to be held;
    b. the purposes for which the CDR entity may collect, hold, use or disclose such CDR data with the consent of a CDR consumer for the CDR data;
    c. the circumstances in which the CDR entity may disclose such CDR data to a person who is not an accredited person.

Rule 7.2 - Rule relating to privacy safeguard 1—open and transparent management of CDR data in sub-Rule (4) relevantly requires further levels of detail as to content mandated for inclusion within the CDR policy of an ADR.

This mandate as to transparency operates in two principal ways.

Firstly, an ADR must publish a statement of record as to the matters required to be addressed. This creates a regulatory incentive to ensure that the treatment of each matter required to be addressed is described in a way that is not misleading or deceptive (including not misleading through omission of material qualification or creation of an incorrect inference.

Publication of an enduring statement of record is a relevant incentive that increases likelihood of compliance by ADRs, because comprehensiveness of matters to be addressed in this statement creates substantial risk of enforcement and adverse findings if the stated treatment of any matter is incorrect or misleading by omission or reasonable inference.

However, a CDR policy is not likely to be read, or if read, fully comprehended, by most CDR customers.

Accordingly, the CDR policy is not an appropriate mechanism for scoping permissions conferred through consent as to CDR data handling by an entity, both (1) within the narrower ambit of purposes for which the CDR entity may collect, hold, use or disclose such CDR data (as required by section 56ED(5)(b) to be addressed in the CDR policy), and (2) within the broader and more complex ambit of safeguards and associated controls to assure that CDR data is used and disclosed only for such purposes, which are only partially addressed within the listed matters in Rule 7.2(4),

Second, this mandate as to transparency operates to create a substantive obligation that a CDR entity must *take such steps as are reasonable in the circumstances to implement practices, procedures and systems that will ensure that the CDR entity complies with Part IVD and the Rules*: subsection 56ED(2)(a).

Steps to ensure that a CDR entity complies with Part IVD and the Rules should include practices, procedures and systems to address ensuring both (1) that CDR data is used only within the scope of authorisations granted by relevant consents, and (2) information security of CDR data.

However, the substantive obligation is stated in terms analogous to Australian Privacy Principle 11.1 — security of personal information, which states "If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information: (a) from misuse, interference and loss; and (b) from unauthorised access, modification or disclosure".

The scope of operation of subsection 56ED(2)(a) (*practices, procedures and systems that will ensure that the CDR entity complies with Part IVD and the Rules*) is clearly wider than *security* of CDR data. This construction is supported by comparison of subsection 56ED(2)(a) with section 56EO of the CCA (Privacy safeguard 12--*security of CDR data, and destruction or de-identification of redundant CDR data*). Section 56EO:

1. closely parallels scope of treatment of APP 11.1 (requiring a CDR entity who is an ADR or a designated gateway for CDR data to take steps to protect the CDR data from misuse, interference and loss; and unauthorised access, modification or disclosure), but
2. defines the scope of steps required as the steps specified in the Rules, and not (as per APP 11.1) as an open class of *such steps as are reasonable in the circumstances.*

As explained elsewhere in this report and the accompanying information security review, there are now mature frameworks and standards for assessing:

- means,
- likelihood,
- appropriate steps to mitigating, and
- management of residual risks,

of compromise to information security of confidential and environment-controlled data sets.

Rule 7.11 and Schedule 2—Steps for privacy safeguard 12—*security of CDR data held by ADRs of the Rules* specify particular steps that accredited persons must take to give effect to their obligation to comply with section 56EO. Specification of these steps creates substantive safeguards for which controls must be designed and implemented and assessed through testing and verification consistent with ASAE 3150 (*Assurance Engagements on Controls*) and like standards.

While noting the potential scope of operation of subsection 56ED(2)(a) (to require an accredited entity to develop practices, procedures and systems that ensure that the accredited entity complies with Part IVD and the Rules, potentially including steps to ensure that CDR data is used only within the scope of authorisations granted by relevant consents), absence of specification of particular steps that the accredited entity must take to give effect to their obligation to comply with subsection 56ED(2)(a) creates risk that some accredited entities will not design and implement practices, procedures and systems that ensure only duly authorised (as well as secure) handling of CDR data within data environments that they control.

Further, without specification of particular steps that the accredited entity should take to give effect to the obligation to ensure that CDR data is used only within the scope of authorisations granted by relevant consents, the entity may also fail to develop and implement controls that are then tested and verified consistent with ASAE 3150 (*Assurance Engagements on Controls*) and like standards.

One possible solution would be development of Data Standards which address attributes of a data handling programme that ADRs should implement to ensure that CDR data is used only within the scope of authorisations granted by relevant consents.

Appendix 6A - Privacy harms taxonomy

Leading privacy scholar Professor Daniel Solove has categorised 16 types of activity which can lead to privacy harms:[130]

- Surveillance can chill expression and political activity, give too much power to the watchers, and make people feel creepy and inhibited,
- Interrogation can be too prying and coercive,
- **Aggregation or combining data can reveal facts about a person that are not readily known and that a person did not expect to be known when providing the data,**
- Identification can inhibit one's ability to be anonymous or pseudonymous,
- **Insecurity makes people more vulnerable to fraud and identity theft,**

Appendices

- **Secondary use involves using information in ways a person does not consent to and might not find desirable,**
- **Exclusion concerns the failure to allow people to know about the data that others have about them and participate in its handling and use,**
- Breach of confidentiality is breaking the promise to keep a person's information confidential,
- Disclosure involves the revelation of truthful information about a person,
- Exposure involves revealing another's nudity, grief, or bodily functions,
- Increased accessibility is amplifying the accessibility of people's personal information,
- Blackmail is the threat to disclose personal information,
- Appropriation involves the dissemination of certain information about a person to serve the aims and interests of another,
- Distortion consists of the dissemination of false or misleading information about individuals,
- Intrusion concerns invasive acts that disturb a person's solitude, and
- Decisional interference involves incursion into people's decisions regarding their private affairs.

Appendix 6B - Advantages of a proactive 'privacy by design' approach

As a general observation of the CDR as a consent-based scheme, it will be critical to appreciate that **not all privacy risks can be resolved by consent**.

The same observation can equally be made of de-identification. Both 'consent' and 'de-identification' are often posed as panaceas to all privacy risks. However, once privacy is understood as protecting a range of rights and values beyond just confidentiality, it becomes apparent that a more nuanced understanding of privacy risks – and potential solutions – is necessary.

This is where a 'Privacy by Design' approach comes into play. The Privacy Commissioner has stated that:

'Underpinning the accountability requirements in APP 1.2, is a 'privacy by design' approach to information management'.[131]

'Privacy by design' has become an internationally accepted framework for protecting privacy.[132] Privacy by design is built around seven key principles:[133]

1. **Proactive not reactive, preventative not remedial**: Take a proactive approach, anticipating risks and preventing privacy-invasive events before they occur.
2. **Privacy as a default setting**: Automatically protect personal information in IT systems and business practices as the default.
3. **Privacy embedded into design**: Embed privacy into the design of any systems, services, products and business practices. Entities handling personal data should ensure that privacy becomes one of the core functions of any system or service.
4. **Full functionality: positive-sum not zero-sum**: Incorporate all legitimate interests and objectives in a 'win-win' manner, not through a 'zero-sum' (either/or) approach. This will avoid unnecessary trade-offs, such as privacy versus security, demonstrating that it is possible to have both.
5. **End-to-end security – full lifecycle protection**: Put in place strong security measures throughout the 'lifecycle' of the information involved. Process personal information securely and then destroy it securely when you no longer need it.
6. **Visibility and transparency – keep it open**: Ensure that whatever business practice or technology you use operates according to the stated promises and objectives and is independently verifiable. Make people fully aware of the personal information being collected, and for what purpose.
7. **Respect for user privacy – keep it user centric**: Keep the interest of individuals paramount in the design and implementation of any system or service. This can be done by offering strong privacy defaults and user-friendly options, as well as ensuring appropriate notice is given.

In our experience, the above seven principles alone are too high-level to offer practical application. One approach to bridging the gap between those principles and influencing actual product or system design is to use the eight Privacy Design Strategies, following the work of Professor Jaap-Henk Hoepman.[134]

A simplified outline of the eight Privacy Design Strategies is included in the Appendix. However, each design strategy can and should be fleshed out, within the context of the CDR, to pose a series of questions for relevant teams. For example, the 'Inform' privacy design strategy may be summarised as:

Individuals should be provided with clear and meaningful privacy communications about their information and privacy rights.

In the context of the CDR, this strategy might lead to additional design questions such as:

- *How might we develop education and awareness raising opportunities to encourage consumers to consider their privacy before sharing their CDR data?*
- *What role should Data Holders play in this?*
- *What role should ADRs play in this?*
- *What role should a new category of 'trusted advisors' play in this?*
- *What could the Data Standards say about this?*
- *How might we leverage the flexibility of app design to deliver 'just in time' privacy communications to individuals?*

We wish to stress that Privacy by Design thinking is not just about the design of technology, but the design of the entire ecosystem in which a piece of technology is supposed to work, including legal protections, transparency and messaging.

We also note that, in addition to privacy *compliance* training, the OAIC has outlined its expectation that organisations should also train staff in privacy *risk management*, including in how to identify high risk projects and when to conduct a PIA.[135]

We recommend that personnel involved in the policy, legislative framework and Data Standard-settings aspects of the CDR be trained in 'privacy by design' and the eight privacy design strategies, as well as PIA methodology for identifying and mitigating privacy risks. In particular, personnel should be reminded to consider abuse cases, not just use cases, for any particular aspect of the CDR. The training should include:

- The meaning and value of privacy,
- Legal obligations under privacy law and the CDR Privacy Safeguards,
- What 'privacy impact' and 'privacy harms' mean for individuals,
- The role of Privacy Impact Assessment in addressing such matters,
- How to identify privacy risks, including via mapping data flows, testing against relevant privacy principles, and considering abuse cases,
- Utilising the eight Privacy Design Strategies to mitigate privacy risks.

Using hypothetical scenarios as part of the training experience can be particularly effective. As the CDR scheme moves beyond just data sharing towards 'action initiation' (e.g. change contact details, make a payment, open a new account, close an account), training exercises could include teasing out how a bad actor, such as an abusive or controlling (ex)partner, could use the CDR scheme to deliberately hurt an individual, such as by:

- finding out critical information such as home address,
- determining patterns of behaviour from electricity usage,
- switching off the power to the victim's home,
- cancelling a phone contract or insurance policy on which the victim relies.

Such training should also encourage co-design, and encourage teams to think broadly about solutions. Uplifting capabilities for teams in how to apply the eight different Privacy Design Strategies helps teams understand that privacy is not always (or only) solvable through designing yet more privacy toggles, asking for customers' consent, or implementing de-identification. We recommend that such training also be offered to players in the CDR ecosystem, i.e. Data Holders, ADRs, and Trusted Advisers.

Appendices

Appendix 6C - Adoption of 'privacy by design' principles

Canada:

Ann Cavoukian, Information & Privacy Commissioner of Ontario, Canada, 'Privacy by Design: The Seven Foundational Principles' (2009, revised 2011).

https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

Australia

'Privacy by Design', OAIC (Web Page).

https://www.oaic.gov.au/privacy/privacy-for-organisations/privacy-by-design

USA

Edith Ramirez, 'Privacy By Design and New Privacy Framework of the U.S. Federal Trade Commission' (Conference Paper, Hong Kong Privacy by Design Conference, 13 June 2012).

https://www.ftc.gov/sites/default/files/documents/public_statements/privacy-design-and-new-privacy-framework-u.s.federal-trade-commission/120613privacydesign.pdf

Singapore

Singapore Personal Data Protection Commission, 'Guide to Data Protection By Design for ICT Systems' (Guidance Report, 2019) 6.

https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Data-Protection-by-Design-for-ICT-Systems-(310519).ashx?la=en

Hong Kong

Hong Kong PCPD, 'Data Protection Authorities Issue Co-signatory Letter to Voice Out Global Privacy Expectations of Video Teleconference Providers' (Media Release, 21 July 2020) 2.

https://www.pcpd.org.hk/english/news_events/media_statements/press_20200721.html

https://www.pcpd.org.hk/english/news_events/media_statements/files/VTC_Open_Letter_upload_updated.pdf

South Korea

Korea Internet & Security Agency, 'Guide on "General Data Protection Regulation" for Korean Enterprises' (Guidance Report, 11 July 2017) 53.

https://www.privacy.go.kr/eng/news_event_list.do [PDF page 56/80]

UK

'Data protection by design and by default', *Information Commissioner's Office* (Web Page).

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-le-processing/accountability-and-governance/data-protection-by-design-and-by-default/#:~:text=What%20is%20data%20protection%20by,protection%20into%20your%20processing%20activities

'Guide to the GDPR: Data protection by design and by default', *Information Commissioner's Office* (Web Page).

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

Data Protection Act 2018 (UK) s 57.

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

57 Data protection by design and default

1. Each controller must implement appropriate technical and organisational measures which are designed—
   a. to implement the data protection principles in an effective manner, and
   b. to integrate into the processing itself the safeguards necessary for that purpose.
3. The duty under subsection (1) applies both at the time of the determination of the means of processing the data and at the time of the processing itself.
4. Each controller must implement appropriate technical and organisational measures for ensuring that, by default, only personal data which is necessary for each specific purpose of the processing is processed.
5. The duty under subsection (3) applies to
   a. the amount of personal data collected,
   b. the extent of its processing,
   c. the period of its storage, and
   d. its accessibility.
5. In particular, the measures implemented to comply with the duty under subsection (3) must ensure that, by default, personal data is not made accessible to an indefinite number of people without an individual's intervention.

Appendices

GDPR

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1 art 25.

https://gdpr-info.eu/art-25-gdpr/

Art. 25 GDPR

Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.[2] That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.[3] In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.
3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.

India

The Personal Data Protection Bill 2019 s 22.

http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf

22

1. Every data fiduciary shall prepare a privacy by design policy, containing
   a. (a) the managerial, organisational, business practices and technical systems designed to anticipate, identify and avoid harm to the data principal;
   b. (b) the obligations of data fiduciaries;
   c. (c) the technology used in the processing of personal data is in accordance with commercially accepted or certified standards;
   d. (d) the legitimate interests of businesses including any innovation is achieved without compromising privacy interests;
   e. (e) the protection of privacy throughout processing from the point of collection to deletion of personal data;
   f. (f) the processing of personal data in a transparent manner; and
   g. (g) the interest of the data principal is accounted for at every stage of processing of personal data.
2. Subject to the regulations made by the Authority, the data fiduciary may submit its privacy by design policy prepared under sub-section (1) to the Authority for certification within such period and in such manner as may be specified by regulations.
3. The Authority, or an officer authorised by it, shall certify the privacy by design policy on being satisfied that it complies with the requirements of sub-section (1).
4. The privacy by design policy certified under sub-section (3) shall be published on the website of the data fiduciary and the Authority.

Appendices

Appendix 7A - PIAs conducted to date and limitations on scope

Consumer Data Right Draft PIA[136]

What was expressly inside the scope of that PIA

[Page 3]

- Detailed analysis of the risks involved with the implementation of the CDR and mitigation strategies, to support better management of those risks.
- Reflects the privacy impact analysis conducted as part of the development of the CDR policy including the outcomes of stakeholder consultations on privacy and information security issues.

What was expressly stated to be outside the scope

[Page 105]

- General Privacy Act reform was outside the scope of this project, which was focussed on data portability and provides rights to business customers as well as individuals.

Whether any mention is made of the Consumer Data *Standards* (as opposed to Consumer Data Rules)

Data Standards were referred to in:

- Regulatory framework governing the Consumer Data Right.
- Consultations on the Consumer Data Right Rules and Standards.
- Risk Mitigation: CDR Specific.

Regulatory framework governing the Consumer Data Right	Under the CDR, data must be provided in a format and in a manner which complies with the **Standards**. While the **Standards** may apply differently across sectors, it is important that the manner and form of the data coming into the CDR system be consistent within and between designated sectors, as far as is practicable. This will promote interoperability, reduce costs of accessing data and lower barriers to entry by data driven service providers – promoting competition and innovation [Page 21]
Consultations on the Consumer Data Right Rules and Standards	Consultations are ongoing in relation to the ACCC's development of the Rules; and the development of the consumer data right technical standards by the interim **Data Standards Body** (the Data61 branch of the CSIRO) Data61 is developing technical standards with the benefit of advice from an Advisory Committee which includes industry, FinTech, privacy and consumer representatives. Three industry working groups have been established that are open to all interested parties: on APIs Standards; Information Security; and User Experience. The standards are being developed transparently and iteratively through GitHub. [Page 40-41]
Risk Mitigation CDR Specific	A2. Information security standards: Data security and transfer standards will be developed by the **Chair**, setting out minimum requirements that must be met. [Page 78]

Privacy Impact Assessment – Consumer Data Right – March 2019[137]

What was expressly inside the scope of that PIA

[Page 9]

- Detailed analysis of the threats involved with the implementation of the CDR and mitigation strategies, to support better

management of those threats.

- This PIA takes a different approach, more akin to a security Threat and Risk Assessment.
  - Assesses the CDR regime using first principles of risk assessment.
  - Reflects that the CDR regime incorporates its own Privacy Safeguards which are stronger than the APPs in a number of ways.

[Page 10]

- Based on the proposed regulatory framework for the CDR, incorporating key design decisions as part of rulemaking and standard setting processes, and public feedback on the first version of the PIA.

What was expressly stated to be outside the scope

- Assessment of threats at the group level, as in many cases this would increase the likelihood and/or severity attached to those threats in a way that would not provide meaningful information to a reader seeking assess the level of a given privacy threat. [Page 63].
- The privacy impacts table and analysis in this section does not take into account any of the risk mitigation strategies in the CDR framework. [Page 63].
- Reputational damage to the CDR system itself [Page 111].
  - This was considered outside the scope of this PIA which focusses on harm to individuals.
- General Privacy Act reform was outside the scope of this project, which was focussed on data portability and provides rights to business customers as well as individuals [Page 128].

Whether any mention is made of the Consumer Data *Standards* (as opposed to Consumer Data Rules)

Data Standards were referred to in:

- Regulatory framework governing the Consumer Data Right.
- Consultations on the Consumer Data Right Rules and Standards.
- Risk Mitigation CDR Specific.

Regulatory framework governing the Consumer Data Right	Under the CDR, data must be provided in a format and in a manner which complies with the **Standards**. While the **Standards** may apply differently across sectors, it is important that the manner and form of the data coming into the CDR system be consistent within and between designated sectors, as far as is practicable. This will promote interoperability, reduce costs of accessing data and lower barriers to entry by data driven service providers – promoting competition and innovation [Page 33]
Consultations on the Consumer Data Right Rules and Standards	Consultations are ongoing in relation to the ACCC's development of the Rules; and the development of the consumer data right technical standards by the interim **Data Standards Body** (the Data61 branch of the CSIRO) Data61 is developing technical standards with the benefit of advice from an Advisory Committee which includes industry, FinTech, privacy and consumer representatives. Three industry working groups have been established that are open to all interested parties: on APIs Standards; Information Security; and User Experience. The standards are being developed transparently and iteratively through GitHub. [Page 52]
Risk Mitigation CDR Specific	A2. Information security standards: Data security and transfer standards will be developed by the **Chair**, setting out minimum requirements that must be met. [Page 93]

Appendices

Maddocks PIA (December 2019)[138]

What was expressly inside the scope of that PIA

[Page 15-16]

- Undertake a "point in time" analysis and consider only the initial implementation of the CDR regime, if it was to be implemented by the versions of the CDR Act, and the Open Banking Designation, Draft Rules, and Draft Data Standards, as at 23 September 2019.
- Following the publication of the revised Draft Rules in August 2019, we noted that many of the risks we had previously identified had been further mitigated and accordingly we revised our draft analysis and draft recommendations.

What was expressly stated to be outside the scope

[Page 16]

- The application of the CDR regime other than its initial implementation in the banking Sector; or
- Any possible future versions of the Open Banking Designation, the Draft Rules and the Draft Data Standards.

Whether any mention is made of the Consumer Data *Standards* (as opposed to Consumer Data Rules)

Data Standards were referred to in:

- Summary of Findings [Page 6]
- Recommendations:
  - Recommendation 1: Further updates to this PIA [Page 7-8].
  - Recommendation 2: Further guidance on operation of the CDR regime [Page 8-9].
  - Recommendation 3: Further consideration of the Draft Rules [Page 9].
  - Recommendation 5: Draft Data Standards.
- Project Description
  - 9. Overview of the Consumer Data Right [Page 20].
  - 12. Draft Rules (proposed rules – August 2019) [Page 24].
  - 13. Draft Data Standards (July 2019 working draft) [Page 25-26].
  - 16. Information flows between the CDR Consumer and a Data Holder [Page 35-36].
  - 17. Information flows involving the ACCC's broader ICT system for the CDR regime (including the Accreditation Register) [Page 37-38].
  - 18. Information flows between the Data Holder and the ADR [Page 41].

4. Summary of Findings [Page 6]	4.1.5 Privacy risk associated with the complexity of the **Draft Data Standards** (including because of the use of language which does not make it easy to determine which parts of the **Draft Data Standards** are binding legal requirements); 4.1.9 lack of clarity around the legal obligations of Data Holders about their required interactions with the Accreditation Registrar, including testing to ensure compliance with the **Draft Data Standards**;
Recommendation 1: Further updates to this PIA [Page 7-8]	A proposed criteria for the trigger of PIA reconsideration is changes to the legislative framework (including the Draft Rules or **Draft Data Standards**) that would impact on the application of the Privacy Safeguards and/or APPs, or remove or reduce any privacy mitigation strategies in the legislative framework identified in this PIA Report, or which would introduce new privacy risks
Recommendation 2: Further guidance on operation of the CDR regime [Page 8-9]	Further guidance could also be provided: 2.7 about the required treatment of redundant data, including the technical requirements for de-identification in accordance with the Draft Rules and **Draft Data Standards**; and
Recommendation 3: Further consideration of the Draft Rules [Page 9	Recommend ACCC should be asked to consider whether the Draft Rules should be further amended before finalisation to: 3.1 include a process for testing a Data Holder's compliance with the **Draft Data Standards** (including when, how, and how often, testing will occur), possibly also including assessment of a Data Holder's security in relation to the transmission of CDR Data;
Recommendation 5: Draft Data Standards	We recommend that the **Draft Data Standards** should be recast into language that will allow CDR Participants to easily distinguish which parts of **Draft Data Standards** are binding legal requirements. Further, we recommend that as the **Draft Data Standards** change and are updated, there needs to be adequately detailed version control to allow for easy identification of any changes to the Draft Data Standards (to ensure the consistent implementation of the **Draft Data Standards** by all CDR Participants).
Project Description 9. Overview of the Consumer Data Right [Page 20]	9.4 The CDR regime will be implemented via a framework that consists of: › 9.4.3 **Data Standards** to be made under the Rules, pursuant to section 56FA in the CDR Act, which will be drafted and administered by the Chair of a new Data Standards Body;
Project Description 12. Draft Rules (proposed rules – August 2019) [Page 24]	12.3 The Draft Rules must be read in conjunction with: › 12.3.4 **Data Standards** made in accordance with section 56FA in the CDR Act (currently the Draft Data Standards); and
Project Description 13. Draft Data Standards (July 2019 working draft) [Page 25-26]	Content not included in PIA.
Project Description 16. Information flows between the CDR Consumer and a Data Holder [Page 35-36]	16.3 The CDR Consumer may use the direct request service to request that the Data Holder disclose their CDR Data directly to themselves. The Data Holder must then provide the requested CDR Data to the CDR Consumer (in human-readable form), unless the Data Holder refuses to disclose the CDR Data as permitted by the Draft Rules. These circumstances are those where the Data Holder considers the refusal to be necessary to prevent physical or financial harm or abuse, or as otherwise specified in the **Draft Data Standards**. 16.7 Further, the Data Holder's Consumer Dashboard must have a function that: 16.7.5 as part of the process for withdrawing authorisation, displays a message relating to the consequences of the withdrawal in accordance with the **Data Standards**. ***Request by ADR on behalf of the CDR Consumer*** 16.10 If an ADR makes a request on behalf of a CDR Consumer, there is no current authorisation for the Data Holder to disclose the requested CDR Data and the Data Holder reasonably believes that the request was made by an ADR on behalf of an eligible CDR Consumer, the Data Holder must ask the CDR Consumer to authorise the disclosure of the requested CDR Data to the ADR. This must be done in accordance with the Division 4.4 of the Draft Rules (Authorisations to disclose CDR Data) and the **Draft Data Standards**. ***Can a Data holder refuse to disclosure CDR data?*** 16.13 The Data Holder may also refuse to disclose CDR Data in response to a valid request in circumstances set out in the **Draft Data Standards**. 16.14 If the Data Holder decides to refuse a valid request in accordance with the **Draft Data Standards**, the Data Holder must inform the ADR. Additionally, a Data Holder may refuse a request in the circumstances set out in the **Draft Data Standards**. The **Draft Data Standards** provide for refusal to be given in certain circumstances, including during periods of time when the digital channels for the Data Holder are the target for a distributed denial of service or equivalent form of attack, or there is a significant increase in traffic from a poorly designed or misbehaving ADR.

FOR PUBLIC RELEASE

Appendices

Project Description 17. Information flows involving the ACCC's broader ICT system for the CDR regime (including the Accreditation Register) [Page 37-38]	17.2 The Draft Rules provide that a database containing a list of Data Holders will form part of the Accreditation Register. This database will contain information about each Data Holder, including each brand name under which the Data Holder offers products and a hyperlink to the relevant web site address of the Data Holder and to their CDR Policy. We understand that Data Holders will also be required to undertake a process of testing to ensuring that their ICT systems include a direct request service and an accredited person request service, and will allow the transfer of CDR Data to ADRs, in accordance with the requirements of the Draft Rules and **Draft Data Standards**. 17.3 The Accreditation Register will also hold information about ADRs who have completed the accreditation process. We understand that applicants seeking accreditation will need to undergo a process of testing to ensuring that their ICT systems will allow the making of requests to Data Holders, and for the receipt of CDR Data from Data Holders, in accordance with the requirements of the Draft Rules and **Draft Data Standards**. 17.6 All transactions between the Accreditation Register and/or the ACCC's broader ICT system for the CDR regime, will be made in a manner consistent with the Draft Rules and the technical requirements in the **Draft Data Standards**. ***What is the Accreditation Register?*** 17.8 We also understand that the ACCC is currently undertaking further work to determine the necessary requirements for: 17.8.1 the Accreditation Register API to be included in the **Data Standards** (i.e., the API that will allow CDR Participants to find the details of registered Data Holders and ADRs);
Project Description 18. Information flows between the Data Holder and the ADR [Page 41]	18.2 CDR Data disclosed by the Data Holder to the ADR must be disclosed in machine-readable form, and the transfer must occur in accordance with the **Draft Data Standards** (which include a number of minimum requirements, including in relation to security).

KPMG Privacy Impact Assessment - Consumer Data Right in the Energy Sector (June 2020)[139]

What was expressly inside the scope of that PIA

[Page 14]

- Impact on an individual consumer's privacy, to the extent that the Priority Energy Datasets concern Generic Product Data.
- Considered the impact of data flowing from the Tailored Product Data dataset.

What was expressly stated to be outside the scope

[Page 14]

- The data flows between the CDR Consumer and Accredited Person;
- The direct data flows between the CDR Consumer and Data Holder;
- The data flows in relation to the ACCC's Register of Accredited Persons and its broader CDR information and communication technology system;
- Did not consider issues in relation to the Generic Product Data in the energy CDR.

Whether any mention is made of the Consumer Data *Standards* (as opposed to Consumer Data Rules)

Data Standards were referred to in:

- Analysis of Privacy Impacts and Risks [Page 7].
- Recommendation 3: Matters for the energy rules to address [Page 8].
- Recommendation 7: Priority Energy Datasets [Page 10].

Analysis of Privacy Impacts and Risks [Page 7]	Takes into account the privacy protections that have been built into the CDR legislative framework to date (as further detailed in the Rules, and supported by the **Consumer Data Standards**, CX Standards and CDR Privacy Safeguard Guidelines).
Recommendation 3 Matters for the energy rules to address [Page 8]	Need to be supported by appropriate changes to the CDR Privacy Safeguard Guidelines, **Consumer Data Standards**, CX Standards and CX Guidelines
Recommendation 7: Priority Energy Datasets [Page 10]	Recommend that Priority Energy Datasets identifies as clearly as possible what classes of information are in scope and what are out of scope and that the **Consumer Data Standards** explain what types of data will be included within the scope of each class of information identified in the Designation Instrument

Maddocks update 3 to Consumer Data Right Regime: Privacy Impact Assessment (September 2021)[140]

What was expressly inside the scope of that PIA

[Page 18]

- Proposed changes to the Rules as described in Part D [Project Description].

Part D Project Description [Page 19-32]

Section 1: Access Changes	13. Introduction of disclosure of CDR Data to Trusted Advisers › Obligations of ADRs, › Obligations of Trusted Advisers, › Data Standards. 14. Introduction of disclosure of CDR insights to non-accredited persons › Obligations of ADRs, › Data Standards. 15. Introduction of a sponsored level of accreditation › Sponsorship arrangements, › Obligations of Sponsors, › Obligations of Affiliates. 16. Introduction of disclosure of CDR Data to CDR Representatives › CDR Representative Arrangements, › Obligations of CDR Principals.
Section 2: Joint Account Changes	17. Proposed changes to joint accounts › Types of disclosure options, › Default disclosure option, › Disclosure option management system, › Managing consumer data requests, › Consumer dashboards, › Notifications to JAHs, › Protection for JAHs.

Appendices

What was expressly inside the scope of that PIA

[Page 18]

› Does not include consideration of any possible future versions of the Rules or the Data Standards.

Whether any mention is made of the Consumer Data *Standards* (as opposed to Consumer Data Rules)

Data Standards were referred to in:

› Recommendation 2: Transfer of CDR Data [Page 8].

› Recommendation 4: Transparency for CDR Consumers [Page 9].

› Recommendation 5 Classes of Trusted Advisers [Page 9-10].

› Recommendation 8: Transparency regarding CDR Insights [Page 10-11].

› Project Description:

  › 13. Introduction of disclosure of CDR Data to Trusted Advisers – Data Standards [Page 20].

  › 14. Introduction of disclosure of CDR Insights to non-accredited persons – Data Standards [Page 21].

  › 17. Proposed changes to joint accounts - Notification to JAHs [Page 32].

Recommendation 2 Transfer of CDR Data [Page 8]	We recommend that Treasury consider whether it is appropriate to amend the **Data Standards**, and/or ensure that appropriate guidance is provided, so that it is clear that all CDR Data (including CDR Insights) must be appropriately encrypted in accordance with Schedule 2 to the Rules, from the time the data leaves the ADR's CDR data environment until it reaches the recipient's IT environment.
Recommendation 4 Transparency for CDR Consumers [Page 9]	We recommend that Treasury consider whether it would be appropriate to continue, in consultation with the **Data Standards** Body, to conduct consumer research on what is the best way to present a CDR Consumer with information on the implications of providing a disclosure consent which permits the disclosure of their CDR Data to Trusted Advisers (and therefore outside of the CDR regime), to ensure that CDR Consumers are provided with an adequate amount of information before providing their consent, but balancing this against the risk of "information overload" for the CDR Consumer. We suggest this could be achieved by expanding proposed Rule 8.11(1A) to require the **Data Standards** to include provisions that cover ensuring that CDR Consumers are made aware that if they provide a TA disclosure consent, their CDR Data will leave the CDR system. We also recommend that Treasury consider whether the Rules should allow the **Data Standards** to specify different standards for obtaining consent to disclose CDR Data to Trusted Advisers, depending on whether: › the CDR Consumer is an individual or sole trader and consenting to disclosure of their CDR Data; and › the CDR Consumer is a company or other business and is consenting to disclosure of CDR Data about their business.

Recommendation 5 Classes of Trusted Advisers [Page 9-10]	We recommend that further guidance be provided about what constitutes the 'reasonable steps' that an ADR is required to take to establish that a Trusted Adviser falls within a class of persons to which CDR Data can be transferred. For example, we suggest that it might be best practice for the Rules, or the **Data Standards**, to require the ADR to: › obtain evidence that the Trusted Adviser falls within a class specified in proposed Rule 1.10C(2); or › check a public register for the relevant class of Trusted Adviser.
Recommendation 8 Transparency regarding CDR Insights [Page 10-11]	We recommend that Treasury consider amending the proposed Rules to specify that **Data Standards** must be made to ensure that, in addition to the fact that the CDR Data will leave the CDR system, the CDR Consumer is made aware of the implications and consequences of their CDR Data leaving the CDR system (such as that their data will be afforded fewer privacy protections). Additionally, we recommend that Treasury consider: › whether different rules should be able to apply for CDR Consumers who are individuals or sole traders, and for CDR Consumers who are businesses; › providing clear and detailed guidance to the market to ensure that potential recipients of CDR Insights understand that they must not seek to pressure a CDR Consumer to consent to the disclosure of their CDR Insight; › whether (through the **Data Standards**) CDR Consumers should be made aware of the implications and consequences of their CDR Data leaving the CDR system; › working with the **Data Standards Body** to develop appropriate **Data Standards** (in consultation with industry and informed by consumer research), to ensure that CDR Consumers fully understand what it is they are consenting to in relation to their CDR Insights; and › CDR Consumers should be required to be shown the particular CDR Insight before it is disclosed (as opposed to simply being provided with an explanation of the CDR Insight or the purpose for its disclosure), so that they can decide not to provide their consent if they do not wish it to be disclosed. For example, CDR Insights in relation to verifying credits and debits on an account may potentially disclose information which an individual CDR Consumer may be uncomfortable about disclosing. We also recommend that Treasury consider requiring that further consumer research be conducted on whether CDR Consumers understand the difference between a one-off versus an ongoing use and disclosure consent in relation to CDR Insights, and based on this research, determine whether it would be appropriate for the Rules and/or **Data Standards** to prescribe how such consent must be sought from CDR Consumers.
Project Description 13. Introduction of disclosure of CDR Data to Trusted Advisers – Data Standards [Page 20]	13.7 Proposed Rule 8.11(1)(c)(iv) will require the **Chair** to make one or more **Data Standards** about the consumer experience data standards for disclosure of CDR Data to Trusted Advisers.

Appendices

Project Description 14. Introduction of disclosure of CDR Insights to non-accredited persons – Data Standards [Page 21]z	14.7 Proposed Rule 8.11(1)(c)(v) will require the **Chair** to make one or more **Data Standards** about the consumer experience data standards for disclosure of CDR Insights. 14.8 Additionally, proposed Rule 8.11(1A) will require the **Data Standards** for obtaining authorisations and consents, and withdrawal of authorisations and consents, that relate to obtaining insight disclosure consents, to include provisions that cover: › 14.8.1 how the Accredited Person can meet the requirement to explain a CDR Insight in accordance with proposed Rule 4.11(3)(ca) (proposed Rule 8.11(1A)(a)); and › 14.8.2 ensuring that the CDR Consumer is made aware that their data will leave the CDR system when it is disclosed (proposed Rule 8.11(1A)(b)).
Project Description 17. Proposed changes to joint accounts - Notification to JAHs [Page 32]	17.14 A Data Holder must give, in accordance with the **Data Standards** and through its ordinary means of contacting JAHs: › 17.14.1 JAH As a notification if: a. one or more JAH Bs have not given their approval for disclosure within the specified timeframe; or b. a JAH B has withdrawn an approval previously given; and › 17.14.2 JAH Bs a notification if a JAH A has given, amended or withdrawn an authorisation, or that the authorisation has expired. 17.15 Data Holders must provide these notifications to JAHs as soon as practicable after an event specified in paragraph 17.14 above occurs, unless the JAH has selected an alternative schedule of notifications. 17.16 Proposed Rule 4A.13(3) will require Data Holders to, in accordance with any **Data Standards**: › 17.16.1 provide for alternative notification schedules (including reducing the frequency of notifications or not receiving notifications); and › 17.16.2 give each JAH a means of selecting such an alternative, and of changing a selection.

Maddocks update 4 to Consumer Data Right Regime: Privacy Impact Assessment (November 2021)[141]

What was expressly inside the scope of that PIA

[Page 10]

› Proposed changes to the Rules and the proposed amendments to the *Competition and Consumer Regulations 2010* (Cth) (CDR Regulations), insofar as they relate to the energy sector

› Only considered the energy-specific amendments in version 40 of the draft Rules, and the exposure draft of version 4 of the CDR Regulations (with a further minor amendment notified to us by Treasury on 21 October 2021).

Part D – Project Description [Page 11-14]

8. Overview

1. Definition of SR Data.
2. Definition of Retail Data Holders.
3. CDR Consumers making requests for SR Data.
4. Responding to SR Data Requests by CDR Consumers.
5. Accredited persons making requests for SR Data.
6. Responding to SR Data Requests by Accredited Persons.
7. Restrictions on the use of SR Data.
8. Managing unsolicited SR Data.
9. Record-keeping obligations.
10. Dispute resolution provisions.

What was expressly inside the scope of that PIA

[Page 10]

› Does not include consideration of any possible future versions of the Rules or the Data Standards

Whether any mention is made of the Consumer Data *Standards* (as opposed to Consumer Data Rules)

Yes – Data Standards refer to the data standards made under s 56FA of the *Competition and Consumer Act 2010* (Cth).

Data Standards were referred to in:

› Recommendation 2 [Page 7].

› Project Description:

  › CDR Consumers making requests for SR (Shared Responsibility) Data [Page 12].

  › Responding to SR Data Requests by CDR Consumers [Page 12].

  › Responding to SR Data Requests by Accredited Persons [Page 13].

  › Record keeping obligations [Page 14].

› Risks associated with the role and obligation of AEMO [Page 16].

Appendices

Recommendation 2 [Page 7]	We recommend that, before commencement of the amendments to the Rules, Treasury confirm that the **Data Standards** do (or will) prohibit Retail Data Holders from disclosing information to AEMO about CDR Consumers if that information would allow AEMO to identify one or more CDR Consumers for the data held by AEMO
Project Description *CDR Consumers making requests for SR (Shared Responsibility) Data* [Page 12]	8.5 Proposed Rule 1.22(2) means that SR Data Requests can only be made by a CDR Consumer to a Primary Data Holder, using the Primary Data Holder's direct request service. However, CDR Consumers in the energy sector will not be able to make Direct to Consumer Requests as proposed Rule 8.5 of Schedule 4 provides that Part 3 of the Rules does not apply in relation to energy sector data. 8.6 Proposed Rule 1.19 means that if a CDR Consumer can make an SR Data Request to a Primary Data Holder, the CDR Consumer is not eligible to make or initiate a SR Data Request for that SR Data to the Secondary Data Holder. 8.7 In the energy sector, this means that CDR Consumers will only be able to make SR Data Requests to Retail Data Holders, and not to AEMO. 8.8 Proposed Rule 1.20(1) effectively requires Retail Data Holders to provide a Consumer Data Request Service for any SR Data. Additionally, proposed Rule 1.21 requires Retail Data Holders to provide a Consumer Dashboard (in accordance with Rule 1.15) in relation to an SR Data Request as if the Retail Data Holder held the requested SR Data. 8.9 Additionally, proposed Rule 1.20(2) requires Secondary Data Holders to, in respect of SR Data, provide an online service that: › 8.9.1 can be used by the Primary Data Holder to request any SR Data needed to respond to an SR Data Request from the Secondary Data Holder; › 8.9.2 enables the requested SR Data to be disclosed to the Primary Data Holder in machine-readable form; and 8.9.3 conforms with the **Data Standards**.
Project Description *Responding to SR Data Requests by CDR Consumers* [Page 12]	8.10 In accordance with proposed Rule 1.22(3), a Retail Data Holder must, using the online service provided by AEMO, and otherwise in accordance with the **Data Standards**, request AEMO to disclose any SR Data that the Retail Data Holder needs to respond to a SR Data Request made by a CDR Consumer. 8.11 Relevantly, if AEMO chooses: › 8.11.1 to disclose the requested SR Data to the Retail Data Holder, it must do so in accordance with any relevant **Data Standards** (proposed Rule 1.22(4)); or › 8.11.2 not to disclose the requested SR Data to the Retail Data Holder, it must notify the Retail Data Holder of its refusal (proposed Rule 1.22(5)).

FOR PUBLIC RELEASE

Project Description *Responding to SR Data Requests by Accredited Persons* [Page 13]	8.14 Proposed Rule 1.23(3) means that Retail Data Holders must comply with Rule 4.5 (asking CDR Consumer for authorisation to disclose CDR Data) as if the Retail Data Holder were the Data Holder for any SR Data covered by the SR Data Request. 8.15 If the CDR Consumer authorises the disclosure of the relevant SR Data, proposed Rule 1.23(4) will require the Retail Data Holder to, using the online service provided by AEMO and otherwise in accordance with the **Data Standards**, request AEMO to disclose any SR Data that the Retail Data Holder needs to respond to a SR Data Request made by a CDR Consumer. 8.16 Relevantly, if AEMO chooses: › 8.16.1 to disclose the requested SR Data to the Retail Data Holder, it must do so in accordance with any **relevant Data Standards** (proposed Rule 1.23(5)); or › 8.16.2 not to disclose the requested SR Data to the Retail Data Holder, it must notify the Retail Data Holder of its refusal (proposed Rule 1.23(6)).
Project Description *Record-keeping obligations* [Page 14]	8.22 It is proposed that Rule 9.3(1) will be amended to require: 8.22.1 Retail Data Holders to keep and maintain records that explain: a. any requests for SR Data made by the Retail Data Holder under proposed Rule 1.23(4); and b. responses to those requests received under proposed Rules 1.23(5) or (6); and 8.22.2 AEMO to keep and maintain records that explain: a. any requests for SR Data received under proposed Rule 1.22(3) or proposed Rule 1.23(4); b. any responses to requests, given under proposed Rules 1.22(4) or (5) or proposed Rules 1.23(5) or (6); and c if they have refused to disclose SR Data, the reasons relied upon to refuse to disclose the SR Data, including any provision of the Rules or **Data Standards**.
Risks associated with the role and obligation of AEMO [Page 16]	***Potential Privacy Risk*** AEMO may receive personal information from a Retail Data Holder in connection with a Consumer Data Request, which results in AEMO holding CDR Data from which a CDR Consumer could be identified This is because it is possible that a Retail Data Holder may provide AEMO with information about the CDR Consumer in the course of assisting a Retail Data Holder to fulfil a Consumer Data Request, or respond to a CDR Consumer's complaint or dispute. Many of the proposed amendments to the Rules (and CDR Regulations) have been drafted on the basis that AEMO will not hold CDR Data from which a CDR Consumer could be identified. ***Existing mitigation strategies*** It is intended that the **Data Standards** will provide that Retail Data Holders must not provide any personal information to AEMO. If AEMO is required to provide assistance after providing CDR Data to a Retail Data Holder in fulfilment of a Consumer Data Request (e.g. by assisting a Retail Data Holder to respond to a CDR Consumer's complaint or dispute), it is intended that a 'transaction identifier' will be used to enable AEMO to identify the relevant CDR Data (i.e. AEMO will not require a CDR Consumer's personal information). If AEMO receives personal information from a Retail Data Holder, AEMO will need to comply with the Privacy Act and any relevant obligations under the National Energy Legislation in respect of that personal information. ***Gap analysis and Recommendations*** In the unlikely event that AEMO receives personal information about a CDR Consumer from a Retail Data Holder (for example, when a Retail Data Holder is seeking assistance to resolve a complaint or dispute under the CDR regime), it is arguable that AEMO may, depending on the nature of the information, then be able to identify one or more CDR Consumers for the data that AEMO holds. If this risk eventuates, AEMO may hold CDR Data from which a CDR Consumer could be identified, but it would not be subject to all of the obligations of a Data Holder. Recommendation: We recommend that, before commencement of the amendments to the Rules, Treasury confirm that the **Data Standards** do (or will) prohibit Retail Data Holders from disclosing information to AEMO about CDR Consumers if that information would allow AEMO to identify one or more CDR Consumers for the data held by AEMO.

FOR PUBLIC RELEASE

Appendices

Appendix 7B - When PIAs are required for other entities

When PIAs are expected by the regulator, rather than legally required?

Although not explicitly mandated by law for entities which are not within the scope of the Privacy Code, the OAIC certainly nonetheless *expects* PIAs to be conducted for 'high privacy impact' activities. (Note the OAIC uses the language of 'privacy impact', whereas the Privacy Code uses the term 'privacy risk'.)

The OAIC has found a number of private sector organisations in breach of APP 1, for failure to conduct a PIA on a 'high privacy impact' project.[142] This is because the 'accountability principle', APP 1, requires entities to take proactive steps to establish and maintain 'practices, procedures and system' to ensure compliance with the other APPs. APP 1 implicitly promotes a 'privacy by design' approach to ensure that privacy compliance is included in the design of information systems and practices from their inception. It does this by requiring all entities to take reasonable steps to implement practices, procedures and systems to ensure compliance with the APPs and any binding registered APP code.

Conducting PIAs is seen as a key way to ensure the entity meets the requirements of APP 1, and thus complies with the other APPs.

For example, the OAIC's Determination against 7-Eleven highlighted that PIAs are an essential element of compliance with APP 1. The OAIC noted that a PIA could have identified 'options for avoiding, minimising or mitigating adverse privacy impacts (including by identifying potential alternatives for achieving the goals of the project without collecting such information)'. In a Determination against Flight Centre following on from a data breach, the OAIC noted that a PIA could have helped to prevent the data breach.[143]

Predicted changes as to when PIAs will be required by law

PIAs may soon be mandatory for all entities regulated by the Privacy Act. The Privacy Act is currently undergoing a review and reform process. In late 2019, the Government agreed to review and reform the Privacy Act.[144] On 25 October 2021, the Attorney General's Department released a Discussion Paper containing numerous proposals to amend the Privacy Act.[145]

Proposal 11.1 recommends the creation of a list of 'restricted practices', which while not prohibited will require additional steps from organisations to identify and mitigate privacy risks. While not explicitly saying so, this proposal could mean the introduction of mandatory PIAs for certain activities, for *all* entities (not just Australian government agencies). Such a reform would be in line with the OAIC's expectations, and international privacy laws such as the European General Data Protection Regulation (GDPR).

Appendix 7C - PIA methodology

Developing a PIA Framework

In our experience, there are a number of matters which need to be considered, in order to develop a successful PIA framework, such that PIAs become embedded into an organisation's standard risk assessment methodology.

Align with enterprise risk management framework – or go broader

When assessing the level of privacy risk posed by a project, a PIA should align with the commissioning organisation's risk management framework, which may include a risk rating methodology, risk appetite statement, and/or categorisation of business impacts.

A PIA should include, for any particular privacy impact identified, an assessment as to:

- the *likelihood* of the risk eventuating (e.g. from 'rare' to 'almost certain'), as well as
- what *consequence* (e.g. from 'insignificant' to 'catastrophic') might arise for:
  - one or more affected individuals, and/or
  - business impacts for the organisation.

In the context of federal government agencies, the Protective Security Policy Framework (PSPF) incorporates consideration of impacts on both individuals and the organisation from 'compromise of the information'. These include for example impacts on:

- safety of an individual, or those associated with the individual
- legal compliance by the organisation.

However that risk framework is, as the descriptors suggest, based on scenarios involving 'compromise of the information'. This is because the PSPF is primarily concerned with the *security* of information.

Yet privacy considerations must extend much further than unauthorised disclosure, or a data breach. A PIA will need to consider privacy impacts on individuals even when the system works *exactly as planned.* Considering the nature of some of the most significant technology project failures, from Cambridge Analytica to the Australian Government's 'robodebt' program, the failures were not about the technology itself failing, or about failures of information security, but the terrible consequences of human decisions made to allow the collection, use and disclosure of personal information in the first place.

(See Section 6.4 for our explanation of the privacy harms which should be considered in a PIA.)

Clarify what constitutes a 'project' to be assessed

Settling what constitutes a 'project' to be assessed under the PIA Framework will be important. Should it be every activity which will involve handling personal information? (The Privacy Code for example defines ***handling personal information*** as 'dealing with personal information in any way, including managing, collecting, holding, using or disclosing personal information'.)

Or should a project be confined to each activity which will *change* the way personal information will be handled? Or only every ICT project?

In the context of the Data Standards, the definition of what will constitute a 'project' should reflect that some projects, such as developing Data Standards, will not actually involve handling personal information – but other CDR players who will operate under those Data Standards will be handling personal information in accordance with the Data Standards, so the process of developing Standards *should* be considered a project worthy of assessment, in our view.

Build in gateways or triggering mechanisms

It will also be important to ensure there is clarity around the triggering points for application of the PIA Framework. For example, it may be necessary to have triggers spread across:

- business case development,
- change management processes,
- procurement processes,
- budget approval processes,
- ICT project initiation, etc.

Ensuring that the triggering points encompass all manner of activities is important, as the Australian Federal Police (AFP) discovered. The OAIC found the AFP in breach of APP 1 and the Privacy Code for failing to conduct a PIA on the use of new software.[146] Even though the AFP had policies, guidance and a procedure for conducting PIAs, the adoption of Clearview AI technology by members of one unit bypassed all the normal procedures for assessing privacy risks of new projects. Because individual officers set up free 'trial' accounts to use the facial recognition software, no funding or procurement processes were involved, and therefore nothing triggered a privacy impact assessment.[147]

Appendices

Triage according to inherent risk

A common problem is a PIA Framework which captures all projects, and all types of changes, and then applies the same risk assessment methodology to everything. In reality, some projects are obviously and inherently more likely to create negative privacy impacts or compliance risks than others, and the most comprehensive form of privacy impact assessment should be left for the more inherently impactful projects.

Thus while we recommend taking a broad approach to defining the types of activities which will constitute a 'project' for the purpose of triggering application of a PIA Framework, this does not mean that every single project will require a PIA to be conducted.

In particular, in the context of the developments of the Consumer Data Standards, if the standards are being constantly refined and revised every few weeks, there will not be sufficient time to conduct a PIA on every new iteration.

Instead, the PIA Framework should enable projects to be very quickly assessed against some threshold criteria, and sorted into inherently low, medium or high risk categories. Only the 'high risk' projects will typically need a comprehensive PIA. Medium risk projects would typically require some review and advice from a privacy advisor, while low risk projects may only need informal advice.

Determine what constitutes a high risk project

The Privacy Code notes that 'a project may be a high privacy risk project if the agency reasonably considers that the project involves any new or changed ways of handling personal information that are likely to have a significant impact on the privacy of individuals'.[148] The OAIC has issued guidance on the types of factors that may point to the potential for a high privacy risk project.[149] These are if a project will involve:

- handling large amounts of personal information,
- handling sensitive information,
- sensitivities of the context in which the project will operate,
- handling personal information of individuals with particular needs,
- handling personal information in a way that could have a serious consequence for an individual or a group of individuals, or
- any of the following activity-based risk factors:
- using or disclosing personal information for secondary purposes,
- disclosing personal information outside your agency,
- using or disclosing personal information for profiling or behavioural predictions,
- using personal information for automated decision-making,
- systematic monitoring or tracking of individuals,
- collecting personal information without notification to, or consent of, the individual,
- data matching (linking unconnected personal information) or data linkage, and
- developing legislation which seeks to engage the required or authorised by law exception to the APPs.

Settle who should conduct the PIA

A PIA Framework should establish who should perform what tasks in a PIA process. How this should be developed will depend on the availability of specialist privacy advisors within the organisation, their location (e.g. is there one central privacy team or are there pockets of privacy expertise across different business lines), as well as the extent to which project managers have the skills to themselves assess privacy risk and develop solutions.

A project manager, loosely defined, may be able to answer a questionnaire about compliance with privacy requirements, but would not typically develop findings or recommendations about addressing privacy impacts. Someone with privacy subject matter.

expertise will be needed to complete the assessment and write up the PIA Report. However, this will need to be a collaborative effort, as the project manager will need to answer questions about the nature of the project.

Develop the PIA methodology

The OAIC has guidelines available on the 'how' of conducting a PIA.[150]

Map out what should happen with a PIA Report

A PIA Framework should clarify what should happen with completed PIA reports, including:

- who needs to complete the risk rating methodology;
- who needs to approve the PIA Report as completed;
- who needs to be provided with a copy of the completed PIA Report;
- when and where the PIA Report is to be published (noting that the Privacy Code requires all PIAs to be at least *listed* on a published register; publication of each actual PIA Report is discretionary);[14]
- in relation to any risks rated as 'high' or above, where or to whom must these be reported (including in any project or enterprise risk register, and/or reported to the project sponsor, the Board, an Audit & Risk Committee, or the senior leadership team);
- in relation to any risks rated as 'high' or above, who has the power to stop the project from proceeding until something else has happened (i.e. the risks have been lowered through additional controls, or the risks have been formally accepted); and
- in relation to any risks rated as 'high' or above, who has the power to accept those risks.

Socialise the framework

Once a PIA Framework has been settled, it will be important to socialise the framework so that all staff know that it exists, and when it applies.

Limitations / challenges with PIAs as a methodology for assessing consumer data standards

A common problem we have observed with the commissioning or conduct of PIAs of public sector activities is an overly narrow framing, whether deliberately via terms of reference or otherwise. This can lead to a number of failures.

Treating a PIA as a legal compliance check

Despite the definition of PIAs from the Privacy Act making clear that they are about measuring and mitigating "*the impact* that the activity or function might have on the privacy of *individuals*", many PIAs are conducted as if they are simply a compliance check against the APPs. They test whether the agency commissioning or conducting the activity will comply with the APPs, without asking what impact the activity will have on individuals.

Similarly, PIAs in relation to the CDR should not only examine compliance against the Privacy Safeguards, which in any case only apply to certain players in the CDR ecosystem. The privacy impacts on individuals should be the primary focus.

A simple example of how looking for privacy impacts is broader than simply reviewing compliance with data privacy laws is in relation to body scanning technology. When first trialled at airports in the wake of the 11 September 2001 terrorist attacks, full body scanners offered screening officials a real-time image of what a passenger looks like naked. Despite the image not being visible to anyone else, and the image not being recorded, and no other 'personal information' being collected by the technology (and thus the technology posed no difficulties complying with the Privacy Act), the visceral reaction by the public against the invasion of their privacy was immediate. The technology was as a result re-configured to instead show screening officers an image of a generic outline of a human body, with heat maps showing where on any given passenger's body the security staff should pat down or examine for items of concern.

Appendices

Reviewing elements in isolation

PIAs which focus on one element of a project or program, rather than the whole ecosystem, will often miss the point.

An example is the PIA of the COVIDSafe app,[151] which did not examine compliance, or risks posed, by the State and Territory health departments which would actually be accessing and using the identifiable data collected by the app. Each of those health departments was covered by a different part of the patchwork of privacy laws in Australia (and in the case of SA and WA, no privacy laws.) The scope of the PIA was limited to the federal Department of Health's compliance with the federal Privacy Act. The PIA Report's authors noted this limitation in their report, along with the lack of time available to consult with either State and Territory privacy regulators, civil society representatives or other experts.

As noted above, a PIA should examine not just a piece of technology in isolation, but the design of the entire ecosystem in which the technology is supposed to work, including legal protections, transparency and messaging, which together influence how well users understand how the technology works. In the context of the CDR, how well users understand how an app works makes a difference to their level of trust, because they can make more informed decisions for themselves.[152]

Also in the context of the CDR, since the development of *standards* is not of itself a process which involves the handling of personal information, it could be tempting to find that the Data Standards-creation activity is not worthy of examination for privacy impacts. However, this would be to take an overly narrow view of the role played by the Data Standards in the overall CDR ecosystem.

Failure to test the technology itself

Again the PIA of the COVIDSafe app[153] is an example. This PIA turned out not to be a review of the *app* at all. The reviewers could not test the app's functionality, let alone test whether assertions made about the data flows were correct. The terms of reference for the PIA were simply whether the Department of Health could lawfully participate in the proposed data flows.

Failure to test for necessity, legitimacy and proportionality

As noted above, a PIA should not only be about assessing one potential vector for privacy harm such as the compromise of personal information.

The OAIC has made clear that a PIA should assess:

- whether the objective of an activity is a **legitimate** objective;
- whether or not the proposal (in terms of how it will handle personal information) is **necessary** to achieve that objective; and
- whether or not any negative impacts on individuals are **proportionate** to the benefits or achievement of the objective.[154]

In particular, a PIA should identify 'potential alternatives for achieving the goals of the project' which could be less privacy-invasive.

The OAIC's determination against 7-Eleven offers a good example. While finding that the company's objective of 'understanding customers' in-store experience' was legitimate, the covert collection of biometrics to achieve that objective was neither necessary nor proportionate to the benefits. (The store had implemented facial recognition technology without notice or consent to test who was answering its in-store customer satisfaction surveys.)

In the Clearview AI case, the OAIC further established that the tests of 'necessity, legitimacy and proportionality' are to be determined with reference to 'any public interest benefits' of the technology; the *commercial* interests of the entity are irrelevant.[156]

The PIA of the COVIDSafe app offers another example of a failure to test for proportionality. A proper assessment of privacy impacts on individuals should involve balancing benefits against risks. If a PIA cannot test whether the benefits will *actually* or even *likely* be achieved, no judgment can be made about whether or not the privacy risks are outweighed by the benefits. Had the PIA reviewers been able to test the functionality of the app, and had they therefore been able to determine that – as later became apparent – the app did not work on iPhones[157] and had other technical problems,[158] then a judgment could have been made much sooner that the benefits did not outweigh the risks to privacy at all.

Failure to consider customer expectations and the role of social licence in gaining trust

Public trust, and therefore uptake of the CDR, is not as simple as asking: Do you trust this organisation (e.g. this bank / telco / energy retailer / fintech)?'

It is about asking: 'Do you trust *this particular way* your data is going to be used *for this particular purpose*, can you see that it will deliver benefits (whether those benefits are personally for you or for others), and are you comfortable that those benefits outweigh the risks for you?'

(See further discussion in Sections 3.3-3.4 about what influences public trust in technology design and Section 6.2 on community attitudes towards privacy.)

When this more complex set of questions is recognised as the basis of consumer sentiment, it becomes apparent how important it is to assess each different data use proposal on a case-by-case basis, because the nature of the proposal, and its context, will make each value proposition unique. That means the balancing of benefits and risks from a privacy point of view needs to be considered afresh for every different project.

Failure to think about the full range of mitigation levers

Privacy by Design thinking is not just about the design of technology, but the design of the entire ecosystem in which a piece of technology is supposed to work, including legal protections, transparency and messaging, which combine to influence how well users understand how an app works. How well users understand how an app works makes a difference to their level of trust, because they can make more informed decisions for themselves.[159]

Comparing two different COVID-related apps offers a good example of how different levers may be pulled to mitigate privacy risks.

Levers to address privacy risks can include:

- technology design,
- technology configuration (i.e. choosing which settings to use when implementing off-the-shelf technology),
- legislation,
- policy (including policy, procedures, protocols, standards, rules etc),
- governance,
- public communications,
- user guidance, and
- staff training.

The development of the federal government's COVIDSafe app was rightly lauded for including strong, bespoke legal privacy protections (such as prohibiting use for law enforcement purposes) developed very early on, yet the app itself had design flaws which could leak data to bad actors. By contrast the NSW government's 'Covid Safe Check-in' app did not have specific legal protections until months after its launch, but the simplicity of the NSW app's design, and the fact that it put the user in complete control of when the app was used – instead of the COVIDSafe 'always on' design – made it the superior app, for utility and some aspects of user trust.

Failure to follow the recommendations

This should be self-evident: simply conducting a PIA is not enough. Unless findings and recommendations to mitigate privacy risks are followed, the assessment can be nothing more than a smokescreen, offering a veneer of respectability to a project.[161]

In particular, a PIA may result in a recommendation to pause, stop or abandon a project entirely. Project teams should be prepared for this possibility.

Appendices

Appendix 7D - The capabilities required to conduct a PIA

The OAIC provides the following advice about identifying who should conduct a PIA, including the desirability of external assessors in some circumstances:[162]

> "Generally, whoever is managing the project would be responsible for ensuring the PIA is carried out. The nature and size of the project will influence the size of the team needed to conduct the PIA, and how much the team needs to draw on external specialist knowledge.
>
> A PIA is unlikely to be effective if it is done by a staff member working in isolation. There could be a team approach to conducting a PIA, making use of the various 'in-house' experts available, such as the privacy officer or equivalent, and outside expertise as necessary. A range of expertise may be required, including information security, technology, risk management, law, ethics, operational procedures and industry-specific knowledge. Seeking external input from experts not involved in the project can help to identify privacy impacts not previously recognised.
>
> Some projects will have substantially more privacy impact than others. A robust and independent PIA conducted by external assessors may be preferable in those instances. This independent assessment may also help the organisation to develop community trust in the PIA findings and the project's intent.
>
> The team conducting the PIA needs to be familiar with the Privacy Act, any other legislation or regulations that might apply to personal information handling (for example, state or territory legislation), and the broader dimensions of privacy."

We would add further to that advice about the 'range of expertise', and suggest that ideally, a privacy assessment team will also be diverse, and have a 'range of lived experience'. This is because part of the task of a PIA is to look not only at legal compliance, but at the privacy impacts, or potential harms, which could be suffered by individuals.

Sometimes people in positions of privilege, such as senior managers, technical experts or lawyers experiencing career success who are predominantly white, male and middle class, may struggle to imagine privacy harms that they have never personally experienced, such as discrimination, harassment, stalking, or family violence.

By way of example, data about a person's home address, or increasingly geolocation data which can reveal patterns of behaviour including physical location, is often collected and exposed by organisations in a fairly casual fashion. Yet for some individuals, the exposure of their location data could lead to very serious harm. Taking a strict legal approach to assessing privacy risk will not assist the PIA assessor to identify the heightened privacy risks in such data, because privacy laws in Australia do not yet recognise location data as 'sensitive' in the way that, for example, medical records are.

We also suggest that a diverse set of skills is needed to conduct a robust privacy risk assessment. Legal and analytical skills are certainly needed, and so is the ability to understand how data might be collected, collated and presented to system users and third parties. However, 'soft' skills like imagination and empathy are also required.

Endnotes

[1]Under *Competition and Consumer Act 2010* (Cth) (**CCA**) s 56AC.

[2]CCA Pt IVD Div 5. The Privacy Safeguards largely replace the Australian Privacy Principles (APPs) from the *Privacy Act 1988* (Cth) in respect of data holders' and Accredited Data Recipients' dealings with CDR data: CCA s 56EC.

[3]CCA s 56BA; more generally CCA Pt IVD Div 2A.

[4]CCA s 56FA.

[5]ISO 31000:2009 – Principles and Guidelines on Implementation, ISO/IEC 31010:2009 – Risk Management – Risk Assessment Techniques
[6]Lyria Bennett Moses, Richard Buckland, Rahat Masood & Benjamin Turnbull, *Considerations for managing cyber threats to the Consumer Data Standards: A Report to the Data Standards Chair* (UNSW, 2022) ("UNSW Threat Report").

[7]The Protective Security Policy Framework (PSPF) is established in the Attorney-General's Directive on the Security of Government Business (October 2018).

[8]UNSW Threat Report.

[9]Lyria Bennett Moses, Richard Buckland, Rahat Masood & Benjamin Turnbull, Considerations for managing cyber threats to the Consumer Data Standards: A Report to the Data Standards Chair (UNSW, 2022).

[10]UNSW Threat Report, Section 3.

[11]ACCC, Assurance Strategy Consumer Data Right, Version 1.1 (28 August 2019).

[12]Data61 – Consumer Data Standards Security Profile (CDS-SP) – Galexia Review https://consumerdatastandards.gov.au/sites/consumerdatastandards.gov.au/files/uploads/2018/12/gal563_data61cds_final_20181219.pdf.

[13]PSPF Policy 3, Annex A.

[14]Australian Government Treasury, Consumer Data Right Overview (September 2019).

[15]Under CCA s 56AC.

[16]See CCA s 56AA.

[17]CCA Pt IVD Div 5. The Privacy Safeguards largely replace the Australian Privacy Principles (APPs) from the Privacy Act 1988 (Cth) in respect of data holders' and Accredited Data Recipients' dealings with CDR data: CCA s 56EC.

[18]CCA s 56BA; more generally CCA Pt IVD Div 2A. https://www.legislation.gov.au/Details/F2022C00187

[19]CCA s 56FA.

[20]CCA ss 56EC(1), 56FD(3).

[21]Each of which is described more fully in the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019.

[22]CCA ss 56AK, 56CA.

[23]The Commonwealth Industrial Scientific and Research Organisation (CSIRO) is a Commonwealth Company, and a Corporate Entity (CE) for the purposes of Finance Law, especially the Public Governance, Performance, and Accountability Act (PGPA) 2013

[24]This is explained further in Section 7.

[25]Australian Government, 'Future Directions for the Consumer Data Right: Final Report' (October 2020).

[26]Australian Government, 'Government Response to the Inquiry into Future Directions for the Consumer Data Right'' (December 2021). [27]Australian Government, 'Future Directions for the Consumer Data Right: Final Report' (October 2020), Recommendation 4.1.

[28]Australian Government, 'Future Directions for the Consumer Data Right: Final Report' (October 2020), Recommendations 5.1-5.2.

[29]Australian Government, 'Future Directions for the Consumer Data Right: Final Report' (October 2020), Recommendation 4.5.

[30]Australian Government, 'Government Response to the Inquiry into Future Directions for the Consumer Data Right'' (December 2021) p 29.
[31]CCA s 56FA(1).

[32]CCA s 56FA(3).

[33]CCA s 56FA(3).

[34]CCA s 56FA(3).

[35]Rule 8.11(2).

[36]The Rules currently require the Chair to make Standards about eight listed categories of matters (Rule 8.11(1)) and require each Data Standard to indicate that it is binding (Rule 8.11(2)).

Endnotes

[37]The Chair must comply with the Rules when making the Standards, must make a Standard if the Rules so require, and must specify a Standard is binding if the Rules so require: s 56FA(2),(3).

[38]CCA s 56FD.

[39]CCA s 56FE(1),(2).

[40]CCA s 56BL.

[41]CCA s 56EY(1)(b)(ii).

[42]CCA s 56GC(1).

[43]The individual Rules that require compliance with certain Data Standards do not seem to require that these be binding Data Standards - that is, it seems that participants may be able to rely on their good faith compliance with any Data Standard with which a Rule requires compliance, to claim protection from liability.

[44]'The scope of the committee's scrutiny function is formally defined by Senate standing order 24, which requires the committee to scrutinise each bill introduced into the Parliament as to whether the bills, by express words or otherwise: (i) trespass unduly on personal rights and liberties; (ii) make rights, liberties or obligations unduly dependent upon insufficiently defined administrative powers; (iii) make rights, liberties or obligations unduly dependent upon nonreviewable decisions; (iv) inappropriately delegate legislative powers; or (v) insufficiently subject the exercise of legislative power to parliamentary scrutiny.': Senate Standing Committee for the Scrutiny of Bills, Scrutiny Digest 4 / 2019, vii.

[45]Senate Standing Committee for the Scrutiny of Bills, Scrutiny Digest 4 / 2019, pp 29-31 https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Scrutiny_of_Bills/Scrutiny_Digest/2019; Senate Standing Committee for the Scrutiny of Bills, Scrutiny Digest 5 / 2019, pp 82-83 https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Scrutiny_of_Bills/Scrutiny_Digest/2019.

[46]Standing Committee for the Scrutiny of Bills, Scrutiny Digest 5 / 2019, pp 82-83 https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Scrutiny_of_Bills/Scrutiny_Digest/2019.

[47]'Statements of Compatibility', Australian Government Attorney-General's Department (Web Page, 8 June 2022) <https://www.ag.gov.au/rights-and-protections/human-rights-and-anti-discrimination/human-rights-scrutiny/statements-compatibility#what-must-a-statement-of-compatibility-contain>. See also *Legislation Act 2003* (Cth) s 42.

[48]CCA s 56BA.

[49]One of the situations in which an instrument will be a 'legislative instrument' is 'if: (a) the instrument is made under a power delegated by the Parliament; and (b) any provision of the instrument: (i) determines the law or alters the content of the law, rather than determining particular cases or particular circumstances in which the law, as set out in an Act or another legislative instrument or provision, is to apply, or is not to apply; and (ii) has the direct or indirect effect of affecting a privilege or interest, imposing an obligation, creating a right, or varying or removing an obligation or right' (Legislation Act 2003 (Cth) s 8(4)). However, even in such a case, the instrument is not a legislative instrument 'if it is declared by an Act not to be a legislative instrument' (s 8(6)(a)), and Part IVD declares that the Data Standards are not a legislative instrument (CCA s 56FA(4)).

[50]For example, in its 2020 Annual Report, the Parliamentary Joint Committee on Human Rights expressed concern about the absence of SoCs in relation to COVID-19 related instruments. Given the human rights implications of COVID-19 related laws and instruments, the Committee noted it would have been appropriate for a SoC to be provided despite the fact that a number of them were exempt from disallowance. The Committee's concern has been communicated to ministers and heads of departments in writing: Parliamentary Joint Committee on Human Rights, Annual Report 2020 (Report, 13 May 2021) 21 par 3.24. https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Human_Rights/Annual_Reports/Annual_Report_2020.

[51]Convention on the Rights of Persons with Disabilities, arts 4, 5, 9 and 12 https://www.info.dfat.gov.au/Info/Treaties/treaties.nsf/AllDocIDs/636560118784755BCA25726C0007D2AC.

[52]Convention on the Rights of Persons with Disabilities, art 12 https://www.info.dfat.gov.au/Info/Treaties/treaties.nsf/AllDocIDs/636560118784755BCA25726C0007D2AC

[53]Explanatory Memorandum, par 1.265.

[54]Explanatory Memorandum par 1.266.

[55]See Digest 5/19. The Chair has established and maintained the Data Standards Advisory Committee (DSAC) to support the Chair in accordance with the Rules. The Terms of Reference for the DSAC include the provision of "relevant … expert … advice on the design and implementation of relevant CDR Data Standards, especially with regard for: (i) Industry expectations and practice; (ii) Legal and regulatory requirements; (iii) Technical specifications; (iv) CDR rule-making; and (v) Policy expectations." While the DSAC may therefore consider some impacts on consumers' interests while advising on such matters, such consideration would not be a substitute for human rights scrutiny of the kind described in this section.

[56]CCA s 56FD(1),(2); s 56FE.

[57]See CCA s 56EE(3), indicating Rules can make exceptions to general anonymity principle in s 56EE(1).

[58]Rule 4.4(3)(b), 4.5.

[59]Rules 1.7(1), 8.11(1)(d). See further ss 56EF(1), 56FA(1)(a).

[60]CCA s 56EF(1), Rule 4.11(1).

[61]CCA s 56ED(7) note re Rules referring to Standards on privacy policies; s 56EH (collection notices in accordance with the Rules); s 56EM (disclosure notices in accordance with Rules); Rule 1.15(1)(ba).

[62]Rule 1.15(1)(ba), requiring information specified in the Standards.

[63]Rules 4.10(1)(a), 4.22 specifically require participants to have regard to any consumer experience guidelines developed by the Data Standards Body.

[64]Rules 4.10(1)(a), 4.22 specifically require participants to have regard to any consumer experience guidelines developed by the Data Standards Body.

[65]CX Guidelines, pp 39, 41.

[66]Rule 7.5(1)(e); CCA s 56EO(2). Note that, although Rule 4.16 requires that the CDR consumer be given the option to require deletion rather than de-identification of redundant data (potentially in contradiction of CCA s 56EO(2)), the ADR might take advantage of its apparent entitlement to sell de-identified CDR data under Rule 7.5(1)(e) before it becomes redundant.

[67]Rule 7.5(1)(aa),(1)(e).

[68]ACCC v Google LLC (No 2) [2021] FCA 367; 391 ALR 346.

[69]ACCC, 'Digital Platforms Inquiry: Final Report' (2019) 401-422.

[70]ACCC v Google LLC (No 2) [2021] FCA 367; 391 ALR 346.

[71]ACCC, 'Digital Platforms Inquiry: Final Report' (2019) 401-422.

[72]Rules 4.10(1)(a), 4.13, 8.11(1)(a),(b).

[73]ACCC, 'Digital Platforms Services Inquiry: Discussion Paper for Interim Report No. 5: Updating competition and consumer law for digital platform services' (February 2022) https://www.accc.gov.au/system/files/Digital%20platform%20services%20inquiry.pdf.

[74]CCA s 56FA(1)(d); Rule 7.5(1)(aa),(2).

[75]Rule 1.17(2),(3).

[76]Christine O'Keefe et al, 'The De-identification Decision-making Framework' (CSIRO Data61, 18 September 2017) https://publications.csiro.au/rpr/download?pid=csiro:EP173122&dsid=DS1.

[77]Rule 7.5(1)(e); CCA s 56EO(2). Note that, although Rule 4.16 requires that the CDR consumer be given the option to require deletion rather than de-identification of redundant data (potentially in contradiction of CCA s 56EO(2)), the ADR might take advantage of its entitlement to sell de-identified CDR data under Rule 7.5(1)(e) before it becomes redundant.

[78]See Luc Rocher, Julien M Hendrick and Yves-Alexandre de Montjoye, 'Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models' (2019) 10 *Nature Communications* 3069; 'Consent and Privacy: A Discussion Paper Exploring Potential Enhancements to Consent under the Personal Information Protection and Electronic Documents Act' (Discussion Paper 2016) 15–16 (risk of re-identification increases over time). See also Joseph A Cannataci, 'Report of the Special Rapporteur on the Right to Privacy to the General Assembly of the United Nations' (Advanced Unedited Report, A/73/45712, 17 October 2018) [61]-[67]; Chris Culnane and Kobi Leins, 'Misconceptions in Privacy Protection and Regulation' (2019) 36 Law in Context 49; Yves-Alexandre de Montjoye, Cesar A Hidalgo, Michel Verleysen and Vincent D Blondel, 'Unique in the Crowd: The Privacy Bounds of Human Mobility' <www.nature.com/articles/srep01376>.

[79]Rule 7.5(1)(e); CCA s 56EO(2).

[80]Rule 8.11(1)(c).

[81]See Attorney-General's Department, 'Tools for Assessing Compatibility with Human Rights' (Website) https://www.ag.gov.au/rights-and-protections/human-rights-and-anti-discrimination/human-rights-scrutiny/tools-assessing-compatibility-human-rights.

[82]'Notifiable data breaches statistics', Office of the Australian Information Commissioner (Web Page) <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics>.

[83]OAIC, Australian Community Attitudes to Privacy Survey 2020 (Survey Report, September 2020). <https://www.oaic.gov.au/engage-with-us/research/australian-community-attitudes-to-privacy-survey-2020-landing-page>.

[84]World Economic Forum, Rethinking Personal Data: Trust and Context in User-Centred Data Ecosystems (Industry Agenda, May 2014), <http://www3.weforum.org/docs/WEF_RethinkingPersonalData_TrustandContext_Report_2014.pdf>.

[85]Data Futures Partnership, A Path to Social Licence: Guidelines for Trusted Data Use (Guidelines, August 2017). <https://aisp.upenn.edu/wp-content/uploads/2019/08/Trusted-Data-Use_2017.pdf>.

[86]Relevant research on Australian consumers' expectations regarding, and attitudes to, privacy in the digital environment is outlined in Section 6.2.

[87]CCA s 56FJ.

Endnotes

[88]Element Four of the Risk Policy.

[89]See Australian Government Department of Finance, General Duties of Officials (RMG 203) [19-22], https://www.finance.gov.au/government/managing-commonwealth-resources/general-duties-officials-rmg-203.

[90]Australian Government Digital Transformation Agency, Digital and ICT Investments, https://www.dta.gov.au/help-and-advice/digital-and-ict-investments.

[91]Available at https://dta.govcms.gov.au/help-and-advice/digital-and-ict-investments/digital-and-ict-investment-oversight-framework.

[92]See Australian Government Department of Prime Minister and Cabinet, *Regulator Performance Guide* (July 2021): "Regulatory functions may include administering (e.g. providing approvals making operational rules about, handling complaints on), monitoring, promoting compliance with and enforcing regulation".

[93]Available at https://www.standards.org.au/getmedia/f132c974-1ecb-4601-884d-f1e10610fbf3/Data-Digital-Standards-Landscape.pdf.aspx.

[94]Data61 – Consumer Data Standards Security Profile (CDS-SP) – Galexia Review https://consumerdatastandards.gov.au/sites/consumerdatastandards.gov.au/files/uploads/2018/12/gal563_data61cds_final_20181219.pdf.

[95]Australian Government Department of Finance, Comcover Information Sheet, Understanding and Managing Shared Risk (2016).

[96]See CCA s 44AAL.

[97]Laura Brodsky and Liz Oakes, 'Data sharing and open banking', McKinsey & Company, 5 September 2017, https://www.mckinsey.com/industries/financial-services/our-insights/data-sharing-and-open-banking.

[98]Maturity of processes and practices, and associated governance structures and assurance controls, is more widely understood and implemented in relation to management of external threat vectors to information security than it is in relation to design and assessment of such elements in relation to privacy of personal information about individuals and good practice in management of confidential and sensitive information, such as CDR data, within organisations or data ecosystems that organisations either control or should otherwise exercise responsibility. One of the more developed frameworks for assessment of privacy maturity is the NZ Government Chief Privacy Officer's Privacy Maturity Assessment Framework, which includes self-assessment materials: see https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/privacy-maturity-assessment-framework-pmaf-and-self-assessments/, France's data protection authority, the Commission nationale de l'informatique et des libertés, in September 2021 proposed a like framework: https://www.cnil.fr/fr/la-cnil-propose-une-autoevaluation-de-maturite-en-gestion-de-la-protection-des-donnees. These frameworks require organisations to develop privacy management programs (as distinct from policies or plans), to ensure that processes and practices of data handling within organisations reliably and verifiably effect and assure implementation of stated policies and practices. See for example Office of the Privacy Commissioner of Canada (OPC), Getting Accountability Right with a Privacy Management Program, April 2012, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-compliance-and-training-tools/gl_acc_201204/; iab Canada, Privacy Management Program – A Practical Checklist for Compliance, https://iabcanada.com/content/uploads/2017/05/IABCanadaPrivacyChecklist.pdf; Manitoba Ombudsman, Guidelines for Implementing a Privacy Management Program for Privacy Accountability in Manitoba's Public Sector, https://www.ombudsman.mb.ca/uploads/document/files/privacy-management-program-guidelines-en.pdf and as an example of implementation by a government agency, Canada Revenue Agency, Privacy Management Framework, https://www.canada.ca/en/revenue-agency/corporate/security/privacy-management-framework.html.

[99]See the judgment of Chief Justice Gleeson in Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd [2001] HCA 63 [43]. The basis of privacy in human dignity was echoed in the extensive discussion of the right of privacy in the Indian Supreme Court decision Justice K. S. Puttaswamy (Retd.) and Anr. vs Union Of India And Ors (Writ Petition (Civil) No 494 of 2012) [28] - [40]. The Business Impact Levels Tool also recognises a sub-category of impact in respect of the potential impact on individuals of compromised information as 'Dignity or safety of an individual (or those associated with the individual)'.

[100]As opposed to territorial privacy or bodily privacy, for example.

[101]Daniel Solove, 'The Myth of the Privacy Paradox' (2020) 89(1) The George Washington Law Review 23.

[102]Joseph A Cannataci, Privacy and Data Protection Law: International Development and Maltese Perspectives (Norwegian University Press, 1986) 60.

[103]OAIC, Submission to Law Reform, Parliament of Australia, Privacy Act Review – Issues Paper (11 December 2020) 23 [1.13].

[104]OAIC, Submission to Law Reform, Parliament of Australia, Privacy Act Review – Issues Paper (11 December 2020) 50 [3.60].

[106]OAIC, 'Australian Community Attitudes to Privacy Survey 2020' (September 2020) 28-37.

[107]Roy Morgan, 'Consumer Views and Behaviours on Digital Platforms: Final Report prepared for Australian Competition & Consumer Commission' (November 2018) 17-23.

[108]Consumer Policy Research Centre, 'CPRC 2020 Data and Technology Consumer Survey' (2020).

[109]See Patricia A Norberg, Daniel R Horne and David A Horne, 'The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors' (2007) 41 Journal of Consumer Affairs 100.

[110]Aleecia M McDonald and Lorrie Faith Cranor, 'The Cost of Reading Privacy Policies' (2008) 4(3) I/S: *A Journal of Law and Policy for the Information Society* 543, 561, 563.

[111]Explained further in Katharine Kemp, 'Concealed Data Practices and Competition Law: Why Privacy Matters' (2020) 16 European Competition Journal 628, 664-665; Daniel J Solove, 'The Myth of the Privacy Paradox' (2021) 89 George Washington Law Review 1.

[112]Daniel J Solove, 'Professor Solove's Taxonomy of Privacy", Privacy + Security Academy', TeachPrivacy (Web Page, 2018) <https://www.privacysecurityacademy.com/wp-content/uploads/2018/02/Handout-Foundations-and-Themes-Professor-Soloves-Taxonomy-of-Privacy-01.pdf>.

[113]See Section 2.1 above regarding the Future Directions for the CDR Inquiry Report recommendation that the DSB develop a Risk Matrix and Risk Taxonomy.

[114]Daniel Solove, 'The Myth of the Privacy Paradox' (2020) 89(1) The George Washington Law Review 29.

[115]AIC, Submission to Law Reform, Parliament of Australia, Privacy Act Review – Issues Paper (11 December 2020) 70-71.<https://www.oaic.gov.au/engage-with-us/submissions/privacy-act-review-issues-paper-submission/>.

[116]Woodrow Hartzog, 'What is Privacy? That's the Wrong Question' (2021) 88 The University of Chicago Law Review 1684. <https://lawreview.uchicago.edu/sites/lawreview.uchicago.edu/files/08_ESSAY_HARTZOG.pdf>.

[117]OAIC, Submission to Law Reform, Parliament of Australia, Privacy Act Review – Issues Paper (11 December 2020) 25. https://www.oaic.gov.au/engage-with-us/submissions/privacy-act-review-issues-paper-submission/.

[118]OAIC, Submission to Law Reform, Parliament of Australia, Privacy Act Review – Issues Paper (11 December 2020) 9. https://www.oaic.gov.au/engage-with-us/submissions/privacy-act-review-issues-paper-submission/.

[119]OAIC, Submission to Law Reform, Parliament of Australia, Privacy Act Review – Issues Paper (11 December 2020) 76. https://www.oaic.gov.au/engage-with-us/submissions/privacy-act-review-issues-paper-submission/.

[120]Privacy (Australian Government Agencies — Governance) APP Code 2017, cl 12.

[121]See further PIA explanation in Section 7.4, for the factors which could make CDR standard development a 'high privacy risk' activity.

[122]Privacy Act 1988 (Cth) s 33.

[123]The conduct of a PIA for all 'high privacy risk projects' is a requirement of clause 12(1) of the Australian Government Agencies Privacy Code 2017 (the Privacy Code), which commenced on 1 July 2018. The Privacy Code is a statutory instrument made by the Australian Information Commissioner under s.26G of the Privacy Act. Clause 15 of the Privacy Code also requires agencies to maintain a publicly accessible register of all PIAs undertaken (irrespective of their risk level). See further section 7.4 on the meaning of 'high privacy risk'.

[124]Commissioner Initiated Investigation into the Australian Federal Police [2021] AICmr 74

[125]See Section 2.4 regarding risks perceptions concerning the Data Standards and the substantial impact of the Data Standards on human rights.

[126]HB 167-2006 Security risk management, Definitions and glossary.

[127]World Economic Forum, Rethinking Personal Data: Trust and Context in User-Centred Data Ecosystems (Industry Agenda, May 2014), https://www3.weforum.org/docs/WEF_RethinkingPersonalData_TrustandContext_Report_2014.pdf.

[128]Data Futures Partnership, A Path to Social Licence: Guidelines for Trusted Data Use (Guidelines, August 2017). <https://aisp.upenn.edu/wp-content/uploads/2019/08/Trusted-Data-Use_2017.pdf> .

[129]Under s912A(1)(h) of the Corporations Act 2001, Australian financial services (AFS) licensees, and responsible entities that are dual regulated by ASIC and APRA, are legally obliged to have adequate risk management systems. ASIC has issued Regulatory Guide 259 Risk management systems of responsible entities, March 2017, which details steps that AFS licensees should take to implement enterprise risk assessment, governance and management: https://download.asic.gov.au/media/el3luwdz/rg259-published-27-march-2017-20220328.pdf. Many licensees then use line of activity specific risk management frameworks and standards to address specific forms of risk, including in management of confidential or sensitive data, in management of the subset of that data that is personal information about individuals. A number of independent reviews of risk management of AFS licensees have identified that licensees are significantly more mature in their assessment and management of financial risks than in dealing with non-financial risks. See for example the analysis and findings of the Prudential Inquiry into the Commonwealth Bank (CBA) FInal Report, April 2018, often referred to as the Laker Report: https://www.apra.gov.au/sites/default/files/CBA-Prudential-Inquiry_Final-Report_30042018.pdf.

Endnotes

[130]Daniel J Solove, 'Professor Solove's Taxonomy of Privacy", Privacy + Security Academy', TeachPrivacy (Web Page, 2018) <https://www.privacysecurityacademy.com/wp-content/uploads/2018/02/Handout-Foundations-and-Themes-Professor-Soloves-Taxonomy-of-Privacy-01.pdf>.

[131]Commissioner Initiated Investigation into the Australian Federal Police (Privacy) [2021] AICmr 74 (26 November 2021) [78].

[132]Examples of the acceptance of 'privacy by design' principles by regulators and policymakers in various jurisdictions are provided in Appendix 6C.

[133]The Seven Principles of Privacy by Design originated in work by the then Privacy Commissioner for Ontario in Canada, Dr Ann Cavoukian (see https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf), and have since been adopted by privacy regulators worldwide, including in Australia; see the OAIC at https://www.oaic.gov.au/privacy/privacy-for-organisations/privacy-by-design.

[134]See https://www.cs.ru.nl/J.H.Hoepman/.

[135]In finding that the Australian Federal Police had breached APP 1, the OAIC determined that the AFP should have implemented comprehensive staff training about how to identify privacy risks, the responsibilities for conducting threshold assessments and PIAs, and clear pathways and triggers for functional areas to consult with appropriate legal and technical experts, before engaging in new or changed personal information handling practices. See Commissioner Initiated Investigation into the Australian Federal Police (Privacy) [2021] AICmr 74 (26 November 2021) [78].

[136]The Treasury, 'Draft Privacy Impact Assessment: Consumer Data Right' (Consumer Data Right: Privacy Impact Assessment, The Treasury, December 2018).

[137]The Treasury, 'Privacy Impact Assessment: Consumer Data Right' (Consumer Data Right: Privacy Impact Assessment, The Treasury, March 2019).

[138]Maddocks, 'Consumer Data Right Regime' (Consumer Data Right: Privacy Impact Assessment, The Treasury, 29 November 2019).

[139]KPMG, 'Consumer Data Right in the Energy Sector: Supplementary Privacy Impact Assessment for the Commonwealth Department of Treasury' (Consumer Data Right: Privacy Impact Assessment, The Treasury, 25 May 2020).

[140]Maddocks, 'Update 3 to Consumer Data Right Regime: Privacy Impact Assessment' (Consumer Data Right: Privacy Impact Assessment, The Treasury, 29 September 2021).

[141]Maddocks, 'Update 4 to Consumer Data Right Regime: Privacy Impact Assessment' (Consumer Data Right: Privacy Impact Assessment, The Treasury, 29 October 2021).

[142]Commissioner Initiated Investigation into 7-Eleven Stores Pty Ltd [2021] AICmr 50; Commissioner Initiated Investigation into Clearview AI, Inc. [2021] AICmr 54.

[143]Flight Centre Travel Group (Privacy) [2020] AICmr 57.

[144]Australian Government, Regulating in the digital age: Government Response and Implementation Roadmap for the Digital Platforms Inquiry (Report, 2019).

[145]Attorney-General's Department, Privacy Act Review (Discussion Paper, October 2021).

[146]Commissioner Initiated Investigation into the Australian Federal Police (Privacy) [2021] AICmr 74 (26 November 2021) at [78]; available at http://www6.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2021/74.html.

[147]In finding that the Australian Federal Police had breached APP 1, the OAIC determined that the AFP should have implemented comprehensive staff training about how to identify privacy risks, the responsibilities for conducting threshold assessments and PIAs, and clear pathways and triggers for functional areas to consult with appropriate legal and technical experts, before engaging in new or changed personal information handling practices. See Commissioner Initiated Investigation into the Australian Federal Police (Privacy) [2021] AICmr 74 (26 November 2021) at [78]; available at http://www6.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2021/74.html.

[148]Australian Government Agencies Privacy Code 2017 cl 12(2).

[149]'When do agencies need to conduct a privacy impact assessment?', OAIC (Web Page) <https://www.oaic.gov.au/privacy/guidance-and-advice/when-do-agencies-need-to-conduct-a-privacy-impact-assessment>.

[150]'Privacy impact assessments', OAIC (Web Page) <https://www.oaic.gov.au/privacy/privacy-impact-assessments>.

[151]Maddocks, 'The COVIDSafe Application: Privacy Impact Assessment' (Department of Health, 24 April 2020).

[152]Nathaniel Mott, 'Study Confirms Lack of Trust Undermined Contact Tracing Efforts', PCMag Australia (online at 21 June 2021) <https://au.pcmag.com/health-fitness/87782/study-confirms-lack-of-trust-undermined-contact-tracing-efforts>.

[153]Maddocks, 'The COVIDSAFE Application: Privacy Impact Assessment' (Department of Health, 24 April 2020).

[154]Commissioner Initiated Investigation into Clearview AI, Inc. [2021] AICmr 54 [177].

[155]Commissioner Initiated Investigation into 7-Eleven Stores Pty Ltd [2021] AICmr 50 [103].

[156]Commissioner Initiated investigation into Clearview AI, Inc. [2021] AICmr 54 [178]-[179].

[157]Ben Grubb, 'Half-baked: The COVIDSafe app is not fit for purpose on iPhones', The Sydney Morning Herald (online at 7 May 2020) <https://www.smh.com.au/technology/the-covidsafe-app-is-not-fit-for-purpose-on-iphones-20200506-p54qjk.html | https://www.smh.com.au/technology/the-covidsafe-app-is-not-fit-for-purpose-on-iphones-20200506-p54qjk.html>.

[158]'The flaws in the COVIDSafe app', The Saturday Paper (online at 11 July 2020) <https://www.thesaturdaypaper.com.au/news/health/2020/07/04/the-flaws-the-covidsafe-app/159378480010058#hrd>.

[159]Nathaniel Mott, 'Study Confirms Lack of Trust Undermined Contact Tracing Efforts', PCMag Australia (online at 21 June 2021) <https://au.pcmag.com/health-fitness/87782/study-confirms-lack-of-trust-undermined-contact-tracing-efforts>.

[160]Anna Johnston, 'What covid apps can teach us about privacy, utility and trust in tech design', SalingerPrivacy (Blog Post, 3 August 2021) <https://www.salingerprivacy.com.au/2021/08/03/covid-app-design/>.

[161]For example the PIA on the COVIDSafe app was touted as meaning that the app 'got the privacy tick'; see https://www.smh.com.au/politics/federal/the-coronavirus-tracing-app-gets-a-privacy-tick-but-it-will-test-australians-trust-20200426-p54nd2.html.

[162]OAIC, Guide to undertaking privacy impact assessments, September 2021, available at https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments.

FOR PUBLIC RELEASE