Office of the Australian Information Commissioner

Consumer Data Right Complaints and Reports Handling System

Privacy Impact Assessment

26 November 2020

HWL EBSWORTH
LAWYERS

Table of Contents

Executive Summary

1. The CDR Complaints and Reports Handling System: PIA Overview

1.1 The Information Commissioner and the Australian Competition and Consumer Commission (**ACCC**) are the regulators of the Consumer Data Right Scheme (the **CDR**). The Information Commissioner is required to handle certain complaints under the CDR. To enable the Information Commissioner to perform that function, the Office of the Australian Information Commissioner (**OAIC**) is implementing the Consumer Data Right Complaints and Reports Handling System (the **System**). The OAIC intends to implement a minimum viable product (**MVP**) for the System in the second half of 2020. The MVP will permit CDR consumers to make complaints, enquiries and reports via customised user forms hosted on the CDR website.

1.2 This Privacy Impact Assessment (**PIA**) Report:

(a) assesses any risks to individual privacy presented by the implementation of the MVP as described in the Project Description;

(b) considers compliance with the *Privacy Act 1988* (Cth) (**Privacy Act**), including the Australian Privacy Principles (**APPs**);

(c) seeks to inform stakeholders about the System, and illustrate the focus being given by the OAIC to identifying and mitigating privacy risks;

(d) sets out the information lifecycle which helps to highlight any privacy risks and areas for improvement in terms of risk mitigation; and

(e) considers any safeguards that the OAIC will have in place to secure personal information from loss or unauthorised access, modification or disclosure.

1.3 This PIA Report has been developed in accordance with the OAIC's Guide to Undertaking Privacy Impact Assessments.

2. Summary of Findings

2.1 HWL Ebsworth has identified privacy risks related to the MVP, and believes that these risks can be effectively mitigated by implementing the Recommendations set out in section 3 below. In particular, HWL Ebsworth considers that the OAIC should not proceed with the enquiries and reports handling functionality of the System as designed as these elements present a real risk of breach of APP 3.1. HWL Ebsworth recommends that Recommendations 4, 5, 6 and 7 be implemented prior to the MVP being released to the public.

3. Recommendations

3.1 This PIA Report makes the following recommendations.

Recommendation 1.
That the OAIC implement processes or governance arrangements to ensure that function creep does not occur. For example, the OAIC could consider implementing a regular review of the operation of the System and, in particular, the nature and scope of personal information collected (perhaps by reference to a sample of enquiries, reports and complaints) and the actual and proposed uses and disclosures of that personal information, to confirm that the uses and disclosures remain consistent with those anticipated at the outset.

Recommendation 1.

OAIC response

The OAIC accepts Recommendation 1 and will undertake to periodically review the operation of the System, at least once every 12 months.

This review will take into account the factors outlined in Recommendation 1.

The CDR Compliance and Enforcement Team will be responsible for conducting this review, specifically staff at the EL 2 and EL 1 Levels, as they will have general oversight over the day-to-day use of the System.

This review will include consideration of the technical aspects of the System, with assistance from internal ICT if/as required, as well as a review of the BAU processes and governance arrangements, to ensure the proposed uses and disclosures of personal information are consistent with those intended from the outset.

The OAIC notes that together with the ACCC, we have also prepared a joint CDR Governance Manual, which includes principles and processes for the management of all contacts received via the System, to ensure uses and disclosures are consistent with those anticipated from the outset.

In addition, the OAIC and ACCC have published a Consumer Data Right Information Sharing Plan.

This Information Sharing Plan has been developed in accordance with clause 4.2 of the CDR Memorandum of Understanding (**MoU**) and sets out the basis on which the OAIC and ACCC can share with each other CDR-related information (which may include personal information), in accordance with section 157AA of the *Competition and Consumer Act 2010* (Cth) (the **CCA**) and section 29 of the *Australian Information Commissioner Act 2010* (Cth) (**AIC Act**).

The OAIC is also developing an internal Guide to CDR matters received via the Online Front Door into Resolve, to assist staff in managing personal information received via the System, and then through Resolve. The Guide first sets out the end to end process for all CDR enquiries, complaints and reports from receipt via the System, and the following processes once enquiries and complaints are received into the OAIC's Resolve system.

In addition, the OAIC is developing a CDR Manual for staff, which provides practical information about the OAIC's CDR functions.

These documents will serve as a useful benchmark in the OAIC's review of the operation of the System, to compare whether personal information is being used and disclosed as originally intended.

Recommendation 2.

That the OAIC deliver privacy training to personnel who will access the System or handle personal information for the purposes of assessing, responding to or investigating enquiries, reports or complaints collected through the System. The training and any written guidance material about the use of the System should addresses at least the matters listed in paragraph [10.7] below.

This training could be included as a component of any broader training to be delivered to those staff in connection with the System. Noting that only two members of OAIC personnel will have access to

Recommendation 2.
the MVP, the OAIC may wish to defer delivery of the training until a time immediately prior to a wider range of staff having access to the System.
OAIC response
The OAIC accepts Recommendation 2. Privacy training for the System will be provided to all staff who will be authorised to access the System, closer to the launch of the full-scale product, and prior to any staff being granted access to the System. Training and written guidance for use of the System will take into account the matters listed in paragraph 10.7 of the PIA. The CDR Compliance and Enforcement Team, specifically EL 2 and EL 2 level staff, will be responsible for delivering this training. Materials are also being prepared to assist with this, including: • A CDR Service Desk Manual: Prepared by Cypha Interactive; • The Guide to CDR matters received via the Online Front Door into Resolve (also noted above under recommendation 1); and • An Internal CDR Manual. Each of the above documents will be finalised by January 2021. However, updates will be made pending changes to the System between the MVP and full-scale solution if/ as required. We have also confirmed with the relevant IT consultant that the System keeps a record of all users who are authorised to access the System, and a record of when they last logged in, so this information can be reviewed if/as required.

Recommendation 3.
That, when the OAIC next reviews its Privacy Policy, it include in that policy: (a) information about how the OAIC holds the personal information it collects. In the context of the System, this would require reference to cloud storage; and (b) reference to the OAIC's statutory functions under the CDR (in the context of identifying the purposes for which the OAIC collects, holds, uses and discloses personal information).
OAIC response
The OAIC accepts this recommendation. The CDR Team will work with our Privacy Officer to draft appropriate wording covering the above matters, for inclusion in the OAIC's Privacy Policy when this is next reviewed, or within 12 months of launching the System, whichever is first.

Recommendation 4.
That the OAIC not proceed with the enquiries and reports handling functionality of the System as designed as this PIA has concluded that there is a real risk that the OAIC will not comply with APP 3.1. That is, the OAIC should not collect solicited personal information in:

Recommendation 4.

(a) enquiries in relation to the CDR generally; or

(b) reports in relation to any business practice or behaviour relating to the CDR that are of concern.

It is open to the OAIC to redesign the System so that it will comply with APP 3.1, such as by soliciting personal information in a narrower range of enquiries and reports in relation to the CDR.

OAIC response

The OAIC does not accept this recommendation.

We note that the OAIC has sought external legal advice in relation to these matters. A copy of this advice was provided to HWL Ebsworth on 12 August 2020. Please note the OAIC provided this on the basis that it is confidential and the OAIC is not waiving any legal professional privilege in relation to the advice.

In the OAIC's view, the operation of the System would be authorised by subsection 10(2) of the AIC Act, as something 'convenient' to be done for or in connection with the performance of the Information Commissioner's statutory privacy functions. Further, in the OAIC's view the collection of personal information under the System would either be reasonably necessary for, or directly related to, one or more of the OAIC's functions or activities (being the operation of the System as authorised under subsection 10(2) of the AIC Act) for the purposes of APP 3.1.

In forming this view, we have had regard to Part IVD of the CCA as a whole, and in particular to the fact that Part IVD establishes the CDR as a co-regulatory scheme.

Recommendation 5.

That the OAIC amend the privacy notice to be used in connection with the enquiry user form to:

(a) specifically refer to Part IVD of the CCA, under which the ACCC and the OAIC have regulatory functions;

(b) more comprehensively address the matters in each of APP 5.2(g) and (h); and

(c) state that personal information included in that form will be collected by the OAIC in the first instance, and that personal information will be disclosed to the ACCC if it is best placed to respond to the enquiry;

Suggested amendments to give effect to this recommendation are shown in Schedule 3. This recommendation should be implemented prior to public release of the MVP.

OAIC response

The OAIC accepts Recommendation 5 and will amend the privacy notices to incorporate the wording in Schedule 3, prior to the public release of the MVP.

Recommendation 6.
That the OAIC amend the privacy notice to be used in connection with the report user form to: (a) specifically refer to Part IVD of the CCA, under which the ACCC and the OAIC have regulatory functions; (b) more comprehensively address the matters in each of APP 5.2(g) and (h); and (c) state that personal information included in that form will be collected by the OAIC in the first instance, and that personal information will be disclosed to the ACCC if it is best placed to respond to the report. Suggested amendments to give effect to this recommendation are shown in Schedule 3. This recommendation should be implemented prior to public release of the MVP.
OAIC response
The OAIC accepts Recommendation 6 and will amend the privacy notices to incorporate the wording in Schedule 3, prior to the public release of the MVP.

Recommendation 7.
That the OAIC amend the privacy notice to be used in connection with the complaint user form to more comprehensively address the matters in each of APP 5.2(g) and (h). Suggested amendments to give effect to this recommendation are shown in Schedule 3. This recommendation should be implemented prior to public release of the MVP.
OAIC response
The OAIC accepts Recommendation 7 and will amend the privacy notices to incorporate the wording in Schedule 3, prior to the public release of the MVP.

4. PIA Methodology

4.1 This PIA has been undertaken in accordance with the ten step process for undertaking a PIA recommended by the OAIC in its Guide to Undertaking Privacy Impact Assessments.

Project Description

5. Background

5.1 The CDR is a data portability reform implemented by the *Treasury Laws Amendment (Consumer Data Right) Act 2019* (Cth) (the **Treasury Laws Amendment Act**). The scheme provides Australians with the right to safely access data about them, held by businesses, and direct that the information be transferred to trusted third parties of their choice.[1] It also requires businesses to provide public access to information on specified products that they offer.[2] The CDR is intended to provide consumers (**CDR consumers**) with efficient and convenient control over their data to lead to increased competition across the Australian economy.[3]

5.2 The Treasury Laws Amendment Act establishes the CDR through amendments to the *Competition and Consumer Act 2010* (Cth) (the **CCA**), the Privacy Act and the *Australian Information Commissioner Act 2010* (Cth) (the **AIC Act**). The amendments include the introduction of new Part IVD of the CCA, with the following objects:[4]

(a) 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:

(i) to themselves for use as they see fit; or

(ii) to accredited persons for use subject to privacy safeguards; and

(b) to enable any person to efficiently and conveniently access information in those sectors that:

(i) is about goods (such as products) or services; and

(ii) does not relate to any identifiable, or reasonably identifiable, consumers; and

(c) as a result of the matters in paragraphs (a) and (b), to create more choice and competition, or to otherwise promote the public interest.

5.3 The CDR operates under a multi-regulator model including the ACCC, the OAIC and a new Data Standards Body.[5] The ACCC has rule-making responsibilities and is required to establish the required functionality of the CDR across each sector.[6] It sets accreditation criteria and processes for data recipients, manages the accreditation register and takes enforcement action in relation to serious or systemic breaches of the CDR.[7] The Information Commissioner is responsible for advising the ACCC on privacy impacts and enforcing the CDR privacy standards. The Information Commissioner will also handle complaints from individuals and small to medium enterprises about possible 'privacy safeguard breaches', and may direct them to a relevant external dispute resolution body.

5.4 The Explanatory Memorandum to the Treasury Laws Amendment (Consumer Data Right) Bill 2019 (Cth) (**Explanatory Memorandum**) recognised that ensuring the privacy and confidentiality of CDR data which relates to a CDR consumer was a key element of the CDR. Accordingly, the Treasury Laws Amendment Act implemented a set of CDR specific privacy safeguards, modelled on the existing Australian Privacy Principles (**APPs**).[8] In describing the

[1] Australian Competition and Consumer Commission, *Consumer Data Right Rules made by ACCC* (Web Page, 5 February 2020) < https://www.accc.gov.au/media-release/consumer-data-right-rules-made-by-accc>.
[2] Office of the Australian Information Commissioner, Consumer Data Right, *Compliance and Enforcement Policy* (Web Page, 8 May 2020) < https://www.oaic.gov.au/consumer-data-right/compliance-and-enforcement-policy/>.
[3] Australian Government, 'ACCC/OAIC Compliance and Enforcement Policy for the Consumer Data Right' (2020) 2.
[4] *Australian Information Commissioner Act 2010* (Cth) s 56AA.
[5] The Australian Government the Treasury, Consumer Data Right Overview (2019) 9.
[6] Ibid 10.
[7] Ibid.
[8] Explanatory Memorandum, *Treasury Laws Amendment (Consumer Data Right) Bill 2019* (Cth) 2.11.

CDR privacy safeguards, the Explanatory Memorandum noted the importance of CDR consumers having the ability to inquire or complain about the manner in which their CDR data is being handled by a CDR participant.[9] It recognised that the CDR is consumer driven and if a consumer is not satisfied that their data is being treated in compliance with the consumer data rules, the consumer should have a clear avenue to raise this with the data holder or accredited entity in possession of the consumer's CDR data.[10]

5.5 The OAIC proposes to implement the System. The System involves the delivery of an online interface hosted on the CDR website through which a CDR consumer can lodge a complaint, report or enquiry about the CDR. It will include a service desk component which facilitates the management of information received from CDR consumers. The System will provide a specific avenue for CDR consumers to raise concerns about how their data is treated. It will also provide a tool through which the OAIC and ACCC can facilitate the performance of their statutory responsibilities as well as efficiently manage complaints, reports and enquiries about the CDR received from CDR consumers.

Statutory Framework

5.6 The Treasury Laws Amendment Act extends the scope of paragraph 9(1)(b) of the AIC Act, which provides for the Information Commissioner's privacy functions, to include functions conferred by Part IVD of the CCA. A summary of those functions is at Schedule 1.

5.7 Under section 56ER of the CCA, the Information Commissioner is authorised to conduct an assessment of whether a CDR participant or designated gateway for the CDR is maintaining and handling the CDR data in accordance with the privacy safeguards or the consumer data rules (to the extent they relate to the privacy safeguards or the privacy or confidentiality of the CDR data).

5.8 Section 56ES of the CCA extends the application of Part IIIC of the Privacy Act (which deals with notification of eligible data breaches) so that it applies to an accredited data recipient, or designated gateway, that holds a CDR consumer's CDR data in a corresponding way to the way that Part applies to an entity that holds an individual's personal information.

5.9 Section 56ET of the CCA extends the regulatory powers of the Information Commissioner under Part V of the Privacy Act. Part V deals with the powers of the Information Commissioner to investigate complaints made by individuals about an act or practice that may be an interference with the individual's privacy, and to investigate certain acts or practices on the Commissioner's own initiative.

5.10 Section 56ET of the CCA provides:

> Breaches to which this section applies
>
> (1) This section applies to a breach (a privacy safeguard breach) of any of the following:
>
> (a) one or more of the privacy safeguards;
>
> (b) the consumer data rules to the extent that those rules relate:
>
> (i) to one or more of the privacy safeguards; or
>
> (ii) to the privacy or confidentiality of CDR data;
>
> (c) section 26WH, 26WK or 26WL or subsection 26WR(10) of the *Privacy Act 1988*, as they apply because of section 56ES of this Act;
>
> in relation to the CDR data of:

[9] Ibid 1.308.
[10] Ibid.

(d) a CDR consumer who is an individual; or

(e) a small business (within the meaning of the Privacy Act 1988) carried on by a CDR consumer for the CDR data.

(2) This section also applies to a breach of section 56ED (privacy safeguard 1).

5.11 Subsection 56ET(3) provides that the object of section 56ET is as follows:

> The object of this section is for Part V of the *Privacy Act 1988* to apply to an act or practice:
>
> (a) of a CDR participant or designated gateway; and
>
> (b) that may be:
>
> (i) a privacy safeguard breach relating to CDR data covered by subsection (1); or
>
> (ii) a breach of section 56ED (privacy safeguard 1);
>
> in a corresponding way to the way that Part applies to an act of practice of an organisation, person or entity that may be an interference with the privacy of an individual or a breach of Australian Privacy Principle 1.
>
> Note: That Part is about investigations of interferences with privacy etc.

5.12 To achieve this objective, subsection 56ET(4) provides that Part V of the Privacy Act, and any other provision of that Act that relates to that Part, also apply in relation to: a CDR participant for CDR data; or a designated gateway for CDR data as if certain substitutions and modifications were made. For example, a reference to an interference with the privacy of an individual is to be taken to be a reference to a privacy safeguard breach relating to the CDR data or a CDR consumer who is an individual or a small business carried on by a CDR consumer for the CDR data.

5.13 Accordingly, the Information Commissioner is empowered to investigate complaints received in relation to privacy safeguard breaches under the CDR in accordance with the procedures in Part V of the Privacy Act (as modified by the CCA). Pursuant to section 25 of the AIC Act, the Information Commissioner may delegate any of her functions or powers to a member of staff of the OAIC, with certain exceptions (including the power to make determinations under section 52 of the Privacy Act).

Implementation of the System

5.14 The OAIC and the ACCC have developed a Memorandum of Understanding for the CDR (**MoU**). The purposes of the MoU include ensuring that the parties are well-prepared to work together in executing their CDR complaint-handling, investigation, enforcement and other functions; and allowing for the exchange of relevant information and documents to the extent permitted by relevant legislation.

5.15 Under clause 4.1 of the MoU, the parties have committed to cooperate to develop appropriate processes and protocols to undertake work in connection with the CDR, with a view to ensuring that the parties will be able to work effectively together. The processes and protocols may cover matters including information exchange to facilitate the parties' duties under the CCA, including audit, enforcement, complaints handling and reporting, and any other relevant duties. One of those protocols is the CDR Information Sharing Plan. That plan states that the parties are likely to need to share information:

> For enforcement related activities: The Parties each have responsibilities under the CCA and the CDR rules to take enforcement action where appropriate and are developing a joint audit and assessment programme in relation to CDR audit and assessment functions. Given this, the Parties will at times need to share information about the conduct of CDR participants, and

information about audits and assessments, investigations and litigation (noting that there may be legal impediments to sharing this information).

To triage CDR matters appropriately: The Australian Government has a 'no wrong door' policy for CDR complaint handling. This policy aims to provide a seamless experience for consumers by ensuring complaints are managed by the appropriate Party. To facilitate this, the Parties are developing an internal complaint handling system for automatic triage and allocation. However, the Parties may still need to transfer to each other complaints and reports that have been misdirected or have been received via alternate channels.

5.16 The OAIC has entered into a contract with Cypha Interactive Pty Limited (**Cypha**) for the design and implementation of the System, including the MVP. The contract was issued pursuant to a work order issued by the OAIC to Cypha in accordance with the Digital Marketplace Master Agreement dated 17 June 2020, which relates to the Digital Transformation Agency's Digital Marketplace Panel.

s 47E(d)

[redacted]

Information to be collected by the System

5.18 CDR consumers will be able to complete user forms available on the CDR website. The OAIC's website will direct CDR consumers to the user forms. CDR consumers will have to select whether they intend to make an enquiry, complaint or report in relation to the CDR. This selection will direct the consumer to one of three user forms, depending on which type of submission they select.

Enquiry User Form

5.19 Prior to electing to make an enquiry, a CDR consumer will be shown the following preliminary information about the enquiry user form:

CDR Enquiry Form

About this Form

You can use this form to submit an enquiry relating to the Consumer Data Right (CDR) scheme to the Australian Competition and Consumer Commission (ACCC) and/or the Office of the Australian Information Commission (OAIC).

A CDR enquiry is different to a CDR complaint or report. You can use the enquiries service to find out general information about the CDR Scheme, including the roles and functions of the ACCC and OAIC. For example, you may wish to understand more about your rights and/or obligations under the CDR scheme. This would be classified as a CDR enquiry.

Continue

5.20 The CDR consumer is then directed to the following privacy notice:

Handling your Enquiry

Under the Consumer Data Right, the ACCC and the OAIC are co-regulators.

Depending on the nature of your enquiry, the ACCC or OAIC may be best placed to respond. Therefore, information submitted in an enquiry may be provided to the ACCC, OAIC or both agencies.

Both the ACCC and the OAIC will handle your personal information in accordance with the Australian Privacy Principles.

If you have further questions about how we will handle your personal information, you can refer to the ACCC's privacy policy and/or the OAIC's privacy policy.

What will we do with your information?

The ACCC and/or the OAIC will use the information you have provided to assess and, where appropriate, respond to your enquiry.

Accessing your information

If you would like to access information about you that the ACCC holds, please email privacy@accc.gov.au

If you would like access to information about you that the OAIC holds, please contact the OAIC enquiries line at enquiries@oaic.gov.au.

Continue

5.21 After electing to continue, the CDR consumer is directed to the enquiry user form to provide the following information into free text fields:

(a) the details of their enquiry; and

(b) whether the consumer has contacted the ACCC or OAIC about their enquiry before and if applicable, their original reference number.

5.22 The remainder of the enquiry user form includes the following structured text questions:

(a) whether the CDR consumer requests a response to their enquiry;

(b) whether the CDR consumer has any documents that they wish to submit with their form. If a CDR consumer selects 'yes', a corresponding field will appear which will allow the consumer to select and upload files;

(c) the CDR consumer's contact information including:

(i) their preferred title from one of the following options:

(A) Mr;

(B) Ms;

(C) Mrs;

(D) Miss;

(E) Dr;

(ii) their given name;

(iii) their family name;

(iv) their preferred contact method including email, phone, post or other; and

(v) depending on which contact method a CDR consumer selects, a corresponding field will appear that requires the customer to provide their relevant contact information. This could include their phone number, email address, postal address or other. CDR consumers are only required to provide one method of contact.

5.23 The enquiry user form includes a note that the customer can use a pseudonym. Before submitting their enquiry form, the CDR consumer is asked to review the information they have provided and can elect to return to the form and change information provided prior to submission.

Report User Form

5.24 If a CDR consumer elects to make a report about the CDR, the following preliminary information will appear:

CDR Report Form

After consumer selects to "make a report"

About this Form

You can use this form to report information about business practices and behaviours relating to the Consumer Data Right (CDR) that are of concern to you.

Making a **report** is different to a complaint or an enquiry

Continue

5.25 A report is generally submitted if a CDR consumer has concerns about how data holders, accredited data recipients and other stakeholders are handling CDR data. The CDR consumer can redirect their submission to a complaint or enquiry via hyperlinks if required. If a customer selects next, they are directed to the following privacy notice:

Handling your CDR Report

Under the Consumer Data Right, the Australian Competition and Consumer Commissioner (ACCC) and the Office of the Australian Information Commissioner (OAIC) are co-regulators.

While the ACCC is typically best placed to respond to CDR reports, information submitted in a report may be provided to the OAIC if it is best placed to respond.

As such, the information you submit as part of your report may be provided to either or both, the ACCC and OAIC, depending on which agency is the most appropriate to provide a response.

Both the ACCC and the OAIC will handle your personal information in accordance with the Australian Privacy Principles.

If you have further questions about how we will handle your personal information, you can refer to the ACCC's privacy policy or the OAIC's privacy policy.

What will we do with your information?

The ACCC and/or the OAIC can accept and record your reports about the CDR. We will use the information you have provided to assess and, where appropriate, respond to your report.

Accessing your information

If you would like to access information about you that the ACCC holds, please email privacy@accc.gov.au

If you would like access to information about you that the OAIC holds, please contact the OAIC enquiries line at enquiries@oaic.gov.au.

Continue

5.26 The CDR consumer is then directed to the first page of the report user form titled, 'Who is the Report about?'. The user form includes the following structured text boxes:

(a) the name of the business;

(b) the ABN (if known); and

(c) the ACN (if known).

5.27 In a free text box, the CDR consumer is asked to, 'please provide a description of the conduct or issue you wish to report'. A CDR consumer is asked if they have any electronic documents that they wish to submit with their form. If the CDR consumer selects 'yes', a corresponding field will appear which will allow them to select and upload files.

5.28 The CDR consumer cannot move to the next stage of the form if they do not provide information in the two mandatory text boxes: the business name; and description of the conduct or issue they wish to report.

5.29 After selecting 'next', the CDR consumer is directed to provide their contact information into the report user form. The user form notes that the CDR consumer can use a pseudonym. The contact information request is listed above in paragraph 5.22(c). Again, prior to submitting their form, the CDR consumer is provided an opportunity to review the information provided and change any details prior to submission.

Complaint User Form

5.30 If a CDR consumer elects to make an complaint, they receive the following preliminary information about the complaint user form:

CDR Complaint Form

About this Form

You can use this form to submit a complaint relating to the handling of your CDR Data to the Office of the Australian Information Commission (OAIC).

The Consumer Data Right (CDR) scheme is governed under Part IVD of the Competition and Consumer Act 2010 (Cth) (Competition and Consumer Act). Under the CDR scheme, the Australian Competition and Consumer Commission (ACCC) and the Office of the Australian Information Commissioner (OAIC) are co-regulators.

Under s 56ET of the Competition and Consumer Act, the OAIC can accept CDR complaints from individuals and small businesses. about the alleged mishandling of their CDR information under the privacy safeguards or CDR Rules that relate to the privacy or confidentiality of CDR data.

Before you complain to us, contact the CDR entity you think has mishandled your CDR information to make a complaint. They should generally respond to your complaint in 30 days. If they don't respond to your complaint, or you're not satisfied with their response, you may lodge a complaint with the OAIC using this form.

Complaints can also be submitted by:

- post to GPO Box 5218, Sydney NSW 2001 (send it by registered mail if you're concerned about sending it by standard post)
- fax, send it to 02 9284 9666

Further information about your ability to make a CDR complaint can be found on the OAIC's website.

Continue

5.31 After the CDR consumer selects continue, they are directed to the following privacy notice:

Your personal information
The Office of the Australian Information Commissioner (OAIC) can investigate complaints about the handling of a consumer's CDR data.

The OAIC will handle your personal information in accordance with the Australian Privacy Principles.
If the OAIC makes inquiries into or investigates your complaint, we will usually disclose the information you give us, including a copy of your complaint, to the entity you have complained about (the respondent).

The ACCC and the OAIC are co-regulators for the CDR. As such, the OAIC may refer your complaint under the CDR scheme and the information you provide us in relation to that complaint, directly the ACCC. Depending on the nature of your complaint, we may decide not to investigate but rather refer the matter directly to the Australian Financial Complaints Authority (AFCA), or to another recognised external dispute resolution scheme. You will be advised of the circumstances where this may occur.

I understand that the OAIC may need to disclose my personal information - including to the ACCC or to a recognised external dispute resolution scheme - for the purpose of dealing with my complaint under the CDR scheme.

For further guidance on the personal information we collect and how we will handle your information, please see the OAIC privacy policy.

What will we do with your information?

We will use the information you have provided to assess your complaint, make inquiries into your complaint, conduct any investigation into the matter and attempt to conciliate the complaint. If the OAIC makes inquiries into or investigates your complaint, we will usually disclose the information you give us, including a copy of your complaint, to the entity you have complained about (the respondent).

We may also disclose your information to others, if necessary, for the purpose of resolving your complaint under the CDR scheme. For example, as co-regulators of the CDR, we may refer your complaint and the information you provide us, to the ACCC or to a recognised external dispute resolution scheme to investigate, including the Australian Financial Complaints Authority (AFCA). Where the OAIC refers your complaint to another entity, we will notify you of the referral.

If we think we may need to disclose your information to an overseas entity to handle your complaint, we will discuss this with you first. In case of a challenge to a decision by the OAIC, we may need to disclose some information to a review body, for example a court or tribunal, or legal representatives.

What information will we collect?

We may need to collect further information from you in order to investigate your complaint. If you do not provide this information to the OAIC, it may affect how we handle your complaint. In some circumstances, it may mean we decide not to investigate your complaint further.

We will usually collect information about you from the respondent. We may also collect information about you from others if they have information relevant to your complaint.

Accessing your information

If you would like to access information about you that the ACCC holds, please email privacy@accc.gov.au.

If you would like access to information about you that the OAIC holds, please contact the OAIC enquiries line at enquiries@oaic.gov.au.

Documents held by the OAIC may be subject to the *Freedom of Information Act 1982*.

Continue

5.32 The CDR consumer is then directed to provide the following information:

(a) the CDR consumer must select whether they are:

(i) an individual;

(ii) a small business;

(iii) a large business; or

(iv) a CDR participant.

5.33 If a CDR consumer selects 'small business', the following text appears:

As a small business consumer, we will need confirmation that your annual turnover does not exceed $3 million and that you have authority to represent the business in this complaint. Please attach:

- Evidence of turnover. This can be a BAS or IAS documents covering the previous financial year, or a Statutory Declaration; and
- Documentation to confirm authority to represent the business in this complaint.

5.34 If a CDR consumer selects 'large business', the following text appears:

This form is for individuals and small business consumers. If you have a complaint that relates to the CDR, you may wish to contact the ACCC.

If you are unsure, you can contact the OAIC's Enquiries team on 1300 363 992

5.35 The CDR consumer is then directed to provide the following information on the details of their complaint:

(a) the respondent to their claim;

(b) 'yes' or 'no' in relation to whether the CDR consumer has complained to the respondent and allowed 30 days to receive a response:

(i) If the CDR consumer selects 'yes', they are asked to provide:

(A) the date the CDR consumer complained;

(B) a copy of their complaint to and the response from the respondent;

(C) if the CDR consumer does not have a copy of their complaint, they are asked to provide details of their contact with the respondent; and

(D) a brief explanation about why they remain unsatisfied.

(ii) if the CDR consumer selects 'no', a free text box appears with the note:

'It is only in exceptional circumstances that the OAIC will investigate complaints where you have not complained to the respondent'.

In the free text box, the CDR consumer must explain why it is not appropriate to complain to the respondent.

(c) 'yes' or 'no' in relation to whether the CDR consumer has complained to another dispute resolution body:

(i) If the CDR consumer selects 'yes', they are asked to provide:

(A) the name of the dispute resolution body; and

(B) a brief explanation of their complaint to the other dispute resolution body and why it is not dealing with their complaint.

(d) Whether the CDR consumer would like to add any additional respondents to their complaint. If they select 'yes', additional text boxes appear which allow the CDR consumer to include other respondent names;

(e) In a free text box the CDR consumer must provide details of their allegations. The complaint user form notes that it would assist the OAIC if the CDR consumer could explain the following:

(i) what happened;

(ii) when it happened (including dates);

(iii) how and when the CDR consumer found out about it;

(iv) what information was involved; and

(v) who did it (include names of individuals involved if known);

(f) In a free text box the CDR consumer must outline what they are seeking to resolve their complaint. This text box includes the following note:

'The OAIC generally tries to resolve complaints through conciliation between you and the respondent. If you ate seeking financial compensation, please set out what loss you have suffered and provide any information or evidence to demonstrate a link between the incident and the amount you ate claiming.'

5.36 The CDR consumer is then asked to select 'yes' or 'no' in relation to whether they would like to attach any documents to their complaint user form. If they select 'yes', drop down boxes appear which allow the CDR consumer to select and upload files. The complaint user form notes that all complaints must include any correspondence the CDR consumer has had with the respondent.

5.37 The CDR consumer is then directed to provide the information outlined in paragraph 5.22(c). If they have previously lodged a complaint or enquiry with the OAIC before, the CDR consumer is asked to provide their reference number.

5.38 They are also asked to select 'yes' or 'no' in relation to whether the CDR consumer has someone they would like to represent them in their complaint. If the CDR consumer selects yes, they can provide the following details:

(a) given name of the representative;

(b) family name of the representative; and

(c) the representative's preferred contact method. Depending on which method the CDR consumer selects, they will have to provide the relevant contact information which may include an email address, phone number, postal address or other.

5.39 Prior to submitting their form, the CDR customer is provided an opportunity to review the information and can select to return to the form if they would like to change any information.

Management of information collected and held by the System

s 47E(d)

s 47E(d)

[redacted]

Further development of the System

5.43 The OAIC intends to enhance the functionality of the service desk and integrate it with Resolve in a later phase of development of the System. This will allow for the user forms to be automatically triaged and assigned to the appropriate agency for processing, as well as supporting workflows and reporting within the individual agencies. This version of the service desk will also include role based access permissions to prevent participants in the System that are not engaged in the management of complaints or reports from accessing particular information.

Analysis

6. Assumptions

6.1 This PIA Report is drafted on the assumptions that:

(a) the OAIC's current information handling practices in relation to the handling of privacy complaints are compliant with the OAIC's privacy obligations; and

s 47E(d) [redacted]

7. Community expectations

7.1 One of the matters which must be taken into account when conducting a PIA is how consistent the project is with community values about privacy. To assess this question, APP entities can conduct consultations, review community responses to similar projects, or consider research into community attitudes about privacy.

7.2 There has been ongoing consultation with the community in relation the implementation of the CDR. The ACCC has carried out community consultation on issues including how to best facilitate participation of third party service providers and the draft CDR Rules. However, the OAIC has not conducted any specific consultation with the community to assess their views regarding the proposed handling of personal information in connection with the System. Accordingly, it is appropriate to consider research into community attitudes more generally.

7.3 The OAIC commissioned the *Australian Community Attitudes to Privacy Survey 2017*, which assists in understanding contemporary community expectations regarding the management of personal information. The following findings are of relevance to this project:

(a) Australians believe that the biggest privacy risks facing the community are online services, including social media sites (32%), ID fraud and theft (19%), data security breaches (17%), risks to financial data (12%), and personal details being too easily available/ accessible/ not secure (7%);

(b) 83% of respondents to the survey believe that privacy risks are greater when dealing with an organisation online compared with other means;

(c) the pieces of information Australians are most reluctant to provide are financial details (42%), address (24%), date of birth (14%), phone numbers (13%), name (10%) and email address (5%). These figures are similar to those obtained when the OAIC last conducted the survey in 2013;

(d) when the community was asked how trustworthy they considered different types of organisation to be, the highest levels of trust were recorded for health service providers (79%), financial institutions (59%) and state and federal government departments (58%); and

(e) only 16% would avoid dealing with a government agency because of privacy concerns, compared with 58% who would avoid dealing with a private company.

7.4 Given that survey respondents advised that names and contact details are among the pieces of information that they are most reluctant to provide, it is relevant that CDR consumers will be able to remain anonymous when submitting a report or enquiry user form through the System.

7.5 Seventeen per cent of survey respondents considered that data security breaches presented the biggest privacy risk. It is probable (although difficult to assess) that the community would be reassured by a description of the security features of the System, noting that the survey

respondents indicated a relatively high level of trust in the information handling practices of federal government agencies. Moreover, the online form is not the only means of making an enquiry, or submitting a complaint. Enquiries can be made by telephone, whereas complaints can be posted or faxed. The provision of a choice of communication channels is a privacy positive step.

7.6 Only sixteen per cent of survey respondents advised they would avoid dealing with a government agency because of privacy concerns and are considered trustworthy by over half of the survey respondents. It is probable that the community would be reassured that they are providing their personal information to a government agency for the purposes of investigation of their complaint rather than a private company.

7.7 In the absence of specific consultation with the community, it is difficult to gauge precisely how the community may respond to the proposed handling of personal information in connection with the System. However, in light of the research conducted by the OAIC and the discussion above, this PIA finds that it is likely that the implementation of the System will be consistent with community values about privacy.

8. Privacy impacts

8.1 In addition to assessing compliance with the Privacy Act and APPs (discussed below), a PIA should also assess the broader privacy implications of a project. The OAIC recommends that APP entities consider the key questions set out below.

(a) Do individuals have to give up control of their personal information?

CDR consumers who submit an enquiry or report using the System are advised that they can use a pseudonym and have discretion as to the nature and extent of any personal information they provide. They need not give up control over their personal information. CDR consumers who make a complaint do have to give up some control over their personal information to enable the handling of their complaint by the OAIC. However, the CDR leverages the existing complaint investigation processes in Part V of the Privacy Act and complainants are free to withdraw a complaint at any stage prior to determination. Engaging in the complaints process is optional and CDR consumers are provided with a comprehensive privacy notice for review prior to submitting any personal information.

(b) Will the project change the way individuals interact with the entity, such as through more frequent identity checks, costs, or impacts on individuals or groups who do not have identity documents?

The System will provide individuals with a new channel for interacting with the OAIC. In general, it will not involve identity checks, costs or impacts on individuals without identity documents. However, individuals who seek to represent CDR consumers who are small businesses will be required to provide documentation to support their claim that they are authorised to represented that business.

(c) Will decisions that have consequences for individuals be made as a result of the way personal information is handled in the project (such as decisions about services or benefits)?

The primary purpose of the project is to assist the Information Commissioner and ACCC to perform their statutory functions by receiving complaints, enquiries or reports about CDR data holders, accredited data recipients and other stakeholders. The way in which information is handled by the OAIC will have consequences for individuals in the form of the outcome of the complaint itself. However, it is important to note that the OAIC will continue to apply its existing complaint handling practices and the System is not intended to bring about any material change in the OAIC's decision making processes in relation to complaints.

(d) How will the OAIC handle any privacy breaches or complaints?

The OAIC's Privacy Policy sets out its internal procedures for responding to a privacy complaint or CDR data breach. While it is beyond the scope of this PIA to consider the effectiveness of those procedures, we consider that it is likely that the OAIC would respond to privacy breaches or complaints about the handling of CDR data in an appropriate manner.

(e) Are there audit and oversight mechanisms in place (including emergency procedures) in case the system fails?

s 47E(d) [redacted]

(f) Does the project recognise the risk of function creep? (For example, is there an interest in using the personal information collected for the project for other purposes that might occur in the future?)

The System does not specifically recognise the risk of function creep. This PIA has found that the overall risk of function creep associated with the System is low but has nonetheless recommended that measures be taken to further reduce this risk (see Recommendation 1).

(g) How valuable would the information be to unauthorised users? (For example, is it information that others would pay money for or try to access via hacking?)

s 47E(d) [redacted]

(h) Is any intrusion or surveillance fully justified and in proportion to the project's anticipated benefits? Is it the only way of achieving the aims of the project, and done in the least intrusive manner? Is it subject to legislative or judicial authority? What auditing and oversight measures are in place?

The design of the System does not involve any intrusion or surveillance of individuals.

(i) How consistent is the project with community values about privacy?

As concluded in section 7 above, although it is difficult to assess it is likely that the System will be consistent with community values about privacy.

8.2 The answers to the key questions set out above suggest that the System is likely to have a low impact on the privacy of individuals and that potential privacy risks can be appropriately mitigated by the controls which are already proposed as part of the design of the System, in combination with the implementation of the Recommendations set out above. Compliance with the APPs is assessed below.

9. Personal information flows

9.1 The term 'personal information' is defined in subsection 6(1) of the Privacy Act to mean information or an opinion about an identified individual, or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not; and

(b) whether the information or opinion is recorded in a material form or not.

9.2 The key flows of personal information, from the perspective of analysing privacy impacts, are set out below.

Identity verification

s 47E(d)

Collection

9.4 The OAIC will collect personal information in the implementation of the System for the purpose of handling enquiries, reports and complaints in relation to the CDR. As set out above, the Information Commissioner has new functions under Part IVD of the CCA. The information that the OAIC intends to collect is dependent on which user form the CDR consumer elects to complete as follows:

(a) if a CDR consumer elects to complete an enquiry user form the collection will include the information listed at 5.21 and 5.22;

(b) if a CDR consumer elects to complete a report user form the collection will include the information listed at 5.22, 5.26 and 5.27; and

(c) if a CDR consumer elects to complete a complaint user form the collection will include the information listed at 5.32, 5.35, 5.37 and 5.38.

9.5 Users can submit reports and enquiries under a pseudonym. Each of the user forms will include free text boxes and allow the CDR consumer to upload files relevant to their submission. This may include personal information about the CDR consumer or a third party (such as CDR data holders, accredited data recipients and other stakeholders). The OAIC anticipates that this collection of information will assist in conducting complaint investigations and enhance enforcement of CDR legislation obligations on scheme participants by providing information of a higher quality and with greater context. The information collected by the OAIC will be held in accordance with the OAIC's existing cloud storage arrangements.

9.6 The OAIC has developed privacy notices to be displayed to CDR consumers prior to the collection of their personal information through any of the three user forms.

Use

9.7 The personal information collected will be used by the OAIC to assist in the performance of the Information Commissioner's complaint handling and other functions under the CDR. The OAIC proposes to use the personal information collected as follows:

(a) Any personal information collected in connection with an enquiry or report will be used for the purposes of assessing and (if appropriate) responding to the enquiry or report;

(b) Any personal information collected in connection with a complaint will be used to assess the complaint, make inquiries into the complaint, conduct any investigation into the matter and attempt to conciliate the complaint.

(c) Other types of personal information collected using the System will be used by the OAIC to inform the response to a user form.

Disclosure

9.8 The OAIC may disclose personal information collected through the System to the ACCC, in circumstances where the ACCC is best placed to respond to an enquiry, complaint or report, having regard to the different roles of the two entities as CDR regulators. This is likely to occur in relation to information received in report user forms that is relevant to issues such as accreditation criteria, the accreditation register or serious breaches of the CDR which the ACCC holds statutory responsibility to regulate. The Information Commissioner is authorised to disclose certain information to the ACCC pursuant to section 29 of the AIC Act.

9.9 In accordance with its current practice, the OAIC will generally disclose at least some of the personal information it collects in connection with a complaint to the respondent. The OAIC may also disclose personal information to an external dispute resolution scheme. As is the case with its existing complaint handling procedures, the OAIC may also disclose personal information in the event of a challenge or review of a decision made under the CDR scheme, such as a tribunal or court.

Information quality

9.10 CDR consumers will be able to review and edit the user forms prior to submission.

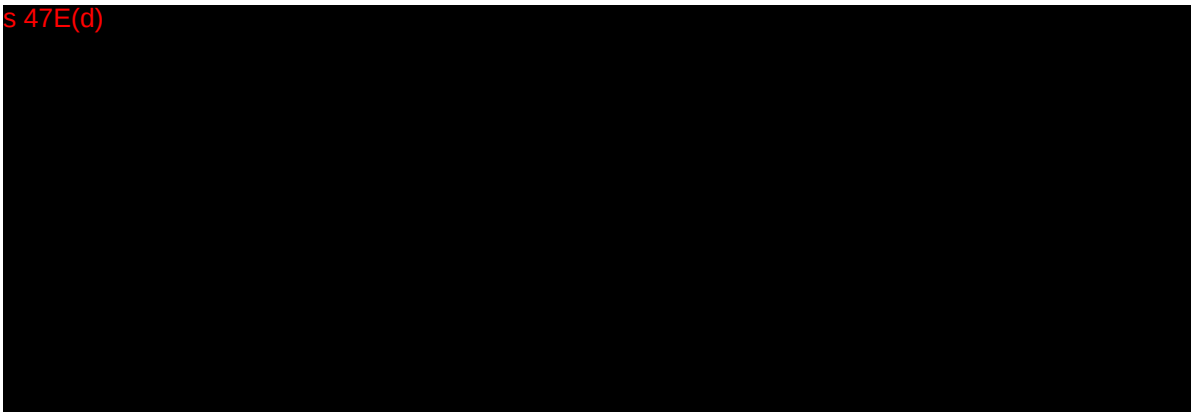
9.11 The personal information will be collected for enquiry, report and complaint handling and investigation purposes. Depending on the outcome of a complaint or investigation, there could be adverse consequences for CDR data holders, accredited data recipients or other stakeholders as a result of the handling of the information, including an adverse determination by the Information Commissioner. If CDR data holders, accredited data recipients or other stakeholders become part of an investigation or other regulatory action taken by the OAIC, as a matter of procedural fairness that person will be provided with an opportunity to respond to the complaint or report and any personal information submitted by the complainant.

Security

9.12 The OAIC proposes to implement the following security safeguards:

s 47E(d)

s 47E(d)



Retention and destruction

9.6 The implementation of the System will not replace Resolve and information from the System will be manually entered into Resolve. It is anticipated that the System will be integrated with Resolve in the next phase of development, thus allowing information collected in the System to be stored in Resolve with limited manual intervention. The records management requirements and disposal authority which apply in connection with information held in Resolve will continue in accordance with existing practices.

Access and correction

9.13 Individuals can request access to or correction of their personal information in accordance with established procedures that are set out in the OAIC Privacy Policy, available on its website.

10. Assessment of compliance with the APPs

10.1 Each collection, use and disclosure of personal information for the purposes of implementing the System must be assessed against the APPs. An analysis of the System in terms of compliance with the APPs is set out below and a summary of the Recommendations of this PIA with respect to the APPs is found at section 3 above. The analysis does not address in detail those elements of the APPs which represent broader compliance obligations of the OAIC, but which do not specifically relate to the System. For convenience, the full text of the APPs is set out at Schedule 2.

APP 1 - Open and transparent management of personal information

10.2 The obligations imposed on the OAIC under APP 1 may be summarised as follows:

(a) the obligation to take reasonable steps to implement practices, procedures and systems to comply with the APPs and the *Privacy (Australian Government Agencies — Governance) APP Code 2017*, and to enable the OAIC to deal with inquiries or complaints from individuals about its compliance with the APPs or that Code (**APP 1.2**);

(b) the obligation to have a clearly expressed and up-to-date policy about the OAIC's management of personal information (**APP 1.3 and 1.4**); and

(c) the obligation to take reasonable steps to make the OAIC's privacy policy available free of charge, and in an appropriate form (**APP 1.5 and 1.6**).

10.3 APP 1.2 is a general obligation and applies to the functions and activities of the OAIC as a whole. It is beyond the scope of this PIA to assess the OAIC's compliance with APP 1.2 in respect of all of its functions and activities. Accordingly, this PIA Report is limited in its consideration of APP 1.2 to whether, in the context of the System, the requirements of that APP have been complied with.

10.4 The commissioning of this PIA by the OAIC is evidence of the OAIC taking reasonable steps to ensure compliance with the APPs and the *Privacy (Australian Government Agencies — Governance) APP Code 2017*. The OAIC will continue to apply its pre-existing privacy processes and policies to the management of its compliance with the APPs, in relation to the System.

10.5 This PIA has found that there is a low risk that the System itself might be used for purposes other than those intended at the outset of this project, as it involves the use of IT infrastructure specifically designed to collect and hold information received in reports, enquiries and complaints in relation to the CDR. However, when personal information is collected for a particular purpose, there is often a residual risk of 'function creep'. Function creep is the incremental expansion in the purpose of a system or project, to a point where information is used for purposes not initially agreed to or envisaged and unrelated to its original intent. Such expansion is generally organic in nature and may lack overall direction, planning or oversight. To manage any risk of personal information collected through the System being used or disclosed for purposes other than those initially intended, this PIA recommends that the OAIC implement processes or governance arrangements to ensure that function creep does not occur (**Recommendation 1**). For example, the OAIC could consider implementing a regular review of the operation of the System and, in particular, the nature and scope of personal information collected (perhaps by reference to a sample of enquiries, reports and complaints) and the actual and proposed uses and disclosures of that personal information, to confirm that the uses and disclosures remain consistent with those anticipated at the outset.

10.6 Given that the implementation of the System involves a new platform to be used in conjunction with an established complaint handling solution (Resolve), it offers an opportunity to provide staff with training on privacy compliance in the specific context of the CDR and the OAIC's regulatory powers under that scheme. This PIA therefore recommends that the OAIC deliver privacy training to personnel who will access the System or handle personal information for the purposes of assessing, responding to or investigating enquiries, reports or complaints collected through the System. This training could be included as a component of any broader training to be delivered to those staff in connection with the System. To the extent possible, privacy compliance training should be tailored to the role and seniority of the attendees and use practical examples which are relevant to those roles.

10.7 This PIA recommends that the privacy training, and any written guidance material developed for internal use, include at least the following topics (**Recommendation 2**):

(a) the purposes for which any personal information collected using the System may be used, including information about when the OAIC will have authority to respond to an enquiry, report or complaint;

(b) instructions as to how to treat any unsolicited personal information collected through the System;

(c) the content of the privacy notices displayed to CDR consumers prior to submission or their enquiry, report or complaint;

(d) the purposes for which personal information may be disclosed to the ACCC or another third party, such as an external dispute resolution service, and the circumstances in which disclosures should be made;

(e) information about the requirement to take steps to protect personal information from misuse, interference and loss and from unauthorised access, modification or disclosure, for example:

(i) the need to ensure that only authorised staff have access to the System;

(ii) that access to the System is monitored and audit logged;

(iii) what to do if the staff member becomes aware of a suspected misuse, interference or loss of personal information, or unauthorised access, modification or disclosure of that information; and

(f) awareness of the procedures in the OAIC's Privacy Policy for dealing with privacy complaints and requests for access to or correction of personal information collected through the System.

10.8 Noting that the MVP will entail access to the Service Desk component of the System by only two members of the OAIC's personnel, the OAIC may wish to defer the delivery of training until a time immediately prior to a wider range of staff having access to the System.

10.9 As is the case with APP 1.2, the obligation in APP 1.3 to have a clearly expressed and up-to-date policy about the management of personal information by the OAIC is one of general application. Accordingly, the assessment of whether the OAIC's privacy policy complies with the APPs would ordinarily be beyond the scope of this PIA. However, it is noted that to comply with APPs 1.3 and 1.5, the OAIC has adopted a Privacy Policy, which is available from its website. The OAIC's Privacy Policy is clearly expressed, and was last updated recently, in July 2020.

10.10 APP 1.4(a) requires the OAIC to include in its Privacy Policy information about the kinds of personal information collected and held by the OAIC. The Privacy Policy provides that the OAIC collects personal information such as contact details and complaint, review, request, data breach notification or report details when individuals undertake activities such as making a complaint about a privacy breach. This PIA finds that the Privacy Policy sets out the kinds of personal information collected by the OAIC in terms which are sufficient to comply with APP 1.4(a) in the context of this project.

10.11 APP 1.4(b) requires the OAIC's Privacy Policy to set out how the OAIC collects and holds personal information. The System will introduce a new online channel by which personal information is collected by the OAIC (i.e., on the user forms on the CDR website). s 47E(d) [redacted] The Privacy Policy states that the main way the OAIC collects personal information is when it is provided by the individual concerned. As such, this PIA has found that the Privacy Policy contains sufficient information about how the OAIC collects personal information in the context of the System. The Privacy Policy also notes a range of measures taken by the OAIC to secure the personal information it holds. However, it does not contain information about the specific ways in which the OAIC holds personal information (s 47E(d) [redacted]). This PIA therefore recommends that the OAIC consider adding such detail when it next reviews its Privacy Policy (**Recommendation 3**).

10.12 APP 1.4(c) requires that the OAIC's Privacy Policy set out the purposes for which personal information is collected, held, used and disclosed. The Privacy Policy states that the OAIC collects, holds, uses and discloses personal information to carry out functions or activities under the AIC Act, the Privacy Act, the FOI Act 'and other legislation that confers functions on the OAIC'. There is no specific reference to the CDR in the Privacy Policy, and the link to 'other legislation' directs the user to a webpage which does not refer to the CDR. While APP 1.4(c) does not require the OAIC to identify every purpose for which it handles personal information, this PIA has found that it would aid transparency and assist the public to understand the OAIC's functions if a reference to the OAIC's functions under the CCA were to be included in its Privacy Policy (or made available from a link in that policy). For that reason, this PIA recommends that the OAIC add a reference to those functions when it next reviews its Privacy Policy (**Recommendation 3**).

10.13 This PIA finds that it is not necessary to assess the OAIC's Privacy Policy against APP 1.4(d) or (e). This is because the System does not alter the OAIC's procedures for individuals to

request access to or correction of their personal information, or the procedures for making and handling a privacy complaint.

10.14 APP 1.4(f) and (g) require the OAIC to include information in its Privacy Policy about whether the OAIC is likely to disclose personal information to overseas recipients, and if so, the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy. The OAIC may disclose personal information overseas in the context of handling a complaint made under the CDR if, for example, the respondent is based overseas. The Privacy Policy advises that personal information will generally only be disclosed overseas so that the OAIC can properly handle a complaint, such as where the respondent is based overseas. Accordingly, this PIA has found that the Privacy Policy contains sufficient information to comply with APP 1.4(f) and (g) in the context of the System.

10.15 Subject to the implementation of Recommendations 1, 2 and 3 above, this PIA Report finds that the OAIC will comply with APP 1 in its delivery of the System.

APP 2 — Anonymity and pseudonymity

10.16 APP 2.1 provides that individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with the OAIC in relation to a particular matter. However, APP 2.2 states that APP 2.1 does not apply in relation to a matter where either: the OAIC is required or authorised by or under an Australian law to deal with individuals who have identified themselves; or it is impracticable for the OAIC to deal with individuals who have not identified themselves or who have used a pseudonym.

10.17 When submitting a report or enquiry, CDR consumers will be explicitly advised that they can use a pseudonym. This PIA report has therefore found that the OAIC will comply with APP 2.1 in its delivery of the enquiry and report handling functionality of the System.

10.18 Individuals who wish to make a complaint will be required to identify themselves (whether they are making a complaint in their own right or as a representative of a small business). This PIA has found that the OAIC is authorised under the CCA (and the provisions of Part V of the Privacy Act which are effectively extended by the CCA to encompass complaints made under the CCA) to deal with individuals who have identified themselves. Section 56ET of the CCA applies to a privacy safeguard breach in relation to the CDR data of a CDR consumer who is an individual, or a small business carried on by a CDR consumer for the CDR data. The Information Commissioner could not properly investigate a complaint of a privacy safeguard breach unless the complainant (or representative of the small business) is identified to the Commissioner (and thus the OAIC) for the purposes of handling that complaint under Part V of the Privacy Act, as modified by the CCA. As such, this PIA has found that APP 2.2 applies, and the OAIC will comply with APP 2 in its delivery of the complaint handling functionality of the System.

APP 3 - Collection of solicited personal information

10.19 APP 3 deals with 'solicited' personal information. The OAIC solicits personal information if it 'requests another entity to provide the personal information, or to provide a kind of information in which that personal information is included'.[11] The relevant 'request' may be made to an agency, organisation, individual or a small business operator. A 'request' is an active step taken by the OAIC to collect personal information, and may not involve direct communication between the OAIC and an individual.[12] APP 3 applies to the System, as the OAIC is actively implementing a new online channel by which individuals can submit personal information in a report, enquiry or complaint form.

APP 3.1

10.20 Under APP 3.1, the OAIC must only collect such personal information as is reasonably necessary for or directly related to, one or more of its functions or activities. New Part IVD of

[11] Privacy Act subsection 6(1).
[12] APP Guidelines, Chapter 3, paragraph 3.6.

the CCA, and other legislative amendments made by the Treasury Laws Amendment Act, have extended the functions of the Information Commissioner. A summary table of the Information Commissioner's functions under Part IVD is at Schedule 1. Those functions include investigation of complaints about possible privacy safeguard breaches under Part V of the Privacy Act (with some modifications). The Information Commissioner will also have the power to initiate an investigation on her own initiative, or conduct an assessment under section 56ER of the CCA (which may occur, for example, in response to a report made in relation to the CDR data handling practices of a CDR participant).

10.21 For the purposes of APP 3.1, the APP Guidelines provide that personal information will be 'directly related to' one or more of the OAIC's functions or activities if there is a 'clear and direct connection' between the personal information being collected and the relevant functions or activities.[13]

10.22 The 'reasonably necessary' test is an objective test: whether a reasonable person who is properly informed would agree that the collection is necessary. It is the responsibility of the OAIC to be able to justify that the particular collection is reasonably necessary.[14]

10.23 Factors relevant to determining whether a collection of personal information is reasonably necessary for a function or activity include:

- the primary purpose of collection;
- how the personal information will be used in undertaking the function or activity (for example, in most circumstances collection on the basis that personal information could become necessary for a function or activity in the future, would not be reasonably necessary); and
- whether the agency could undertake the function or activity without collecting that personal information, or by collecting a lesser amount of personal information.[15]

10.24 The System will collect personal information from CDR consumers in relation to a complaint, enquiry or report about the CDR. The personal information to be collected by the OAIC through the System will vary depending on which user form the CDR consumer elects to complete. We deal with each user form in turn below.

Reports

10.25 The first step in assessing compliance with APP 3.1 is to identify the relevant functions or activities of the agency. The APP Guidelines provide that an agency's functions will be conferred either by legislation or an executive scheme or arrangement established by government. Identifying an agency's functions involves examining the legal instruments that confer or describe the agency's functions. These include legislation, the Administrative Arrangements Order made by the Governor-General and government decisions or ministerial statements.[16] The activities of an agency are related to its functions and include incidental and support activities, such as human resource, corporate administration, property management and public relations activities.

[13] APP Guidelines, Chapter 3, paragraph 3.16.
[14] APP Guidelines, Chapter 3, paragraph 3.18.
[15] APP Guidelines, Chapter 3, paragraph 3.19.
[16] APP Guidelines, Chapter 3, paragraph 3.10.

10.26 Section 10 of the AIC Act deals with the functions and powers of the Information Commissioner and provides as follows:

> 10 Functions and powers of the Information Commissioner
>
> (1) The Information Commissioner has the following functions:
>
> (a) the information commissioner functions;
>
> (b) the freedom of information functions;
>
> (c) the privacy functions.
>
> (2) The Information Commissioner has power to do all things necessary or convenient to be done for or in connection with the performance of functions conferred by this section.

10.27 Paragraph 9(1)(b) of the AIC Act provides that the 'privacy functions' of the Information Commissioner are functions conferred on the Information Commissioner by an Act if they are conferred by Part IVD of the CCA, an instrument made under Part IVD, or another Act because of Part IVD.

10.28 Pursuant to section 27 of the Privacy Act, the Information Commissioner's functions relevantly include:

> (a) the functions that are conferred on the Commissioner by or under:
>
> (i) this Act; or
>
> (ii) any other law of the Commonwealth;
>
> …
>
> (e) to do anything incidental or conducive to the performance of any of the above functions.

10.29 As the functions conferred on the Information Commissioner under Part IVD of the CCA are conferred by a 'law of the Commonwealth', paragraph 27(e) of the Privacy Act also applies to those functions.

10.30 The Information Commissioner does not have an express legislative function of handling reports made in relation to the CDR. Likewise, no government decision or ministerial statement conferring a report-handling function on the Commissioner has been identified. The question of whether the Commissioner is empowered to collect and deal with information in reports therefore turns on the scope of the 'incidental or conducive' and 'necessary or convenient' powers. This PIA focuses on the latter formulation, as it has been the subject of more frequent judicial consideration than the former. The OAIC has formed the view that the operation of the report-handling component of the System would be authorised by subsection 10(2) of the AIC Act, as something ‘convenient’ to be done for or in connection with the performance of the Information Commissioner’s statutory privacy functions.

10.31 Courts have found that the phrase 'necessary or convenient' indicates an ancillary power to carry into effect what is enacted in the statute, that is, to enable the repository of the power to perform the functions which are prescribed by the Act.[17] A leading authority in the interpretation of provisions conferring 'necessary or convenient' powers is *Shanahan v Scott*, in which the

[17] *Binsaris v Northern Territory* [2020] HCA 22, [100].

High Court was required to determine the scope of a regulation-making power. The High Court held that:

> [S]uch a power does not enable the authority by regulations to extend the scope or general operation of the enactment but is strictly ancillary. It will authorise the provision of subsidiary means of carrying into effect what is enacted in the statute itself and will cover what is incidental to the execution of its specific provisions. But such a power will not support attempts to widen the purposes of the Act, to add new and different means of carrying them out or to depart from or vary the plan which the legislature has adopted to attain its ends.[18]

10.32 The principles which emerge from *Shanahan* and subsequent decisions on the scope of such powers were recently summarised in *Northern Land Council v Quall* as follows:

> (a) "Necessary or convenient" powers are "strictly ancillary" powers.
>
> (b) This means they do not extend the general operation or scope of an enactment. The scope of their operation is tied to the specific functions conferred on the repository under other parts of the enactment ...
>
> (c) By definition, incidental or ancillary powers provide a source of power that is in addition to the existing powers conferred on a repository under an enactment. However, the power provided is supplementary to some other existing object or function conferred by the enactment.
>
> (d) Ancillary powers are not a freestanding source of power to expand the objects of the enactment, or to circumvent the means provided for in the enactment for pursuing the relevant statutory objects.
>
> (e) In summary, when one asks whether a person or body has statutory power to engage in an activity, the starting point is the powers and functions conferred on that person by the legislation — not the presence of a "necessary or convenient" power or any other collocation used to describe incidental or ancillary powers conferred on the person or body.[19]

10.33 In *Quall*, the Court also cited the following passage from the decision of the Full Court of the Federal Court of Australia in *Hird v Chief Executive Officer of Australian Sports Anti-Doping Authority*:

> The parliament has commonly used provisions like s 22 of the ASADA Act to ensure that a statutory body has sufficient power to discharge its functions in circumstances that the parliament could not practically set down, although they lie within the contemplation of its enactment. The authorities that have discussed the scope of a "necessary" or "convenient" power such as that in s 22 of the ASADA Act support the general proposition that s 22 is to be construed in conformity "with the width of the language in which it is expressed" … As Ryan J stated in *Anthony Lagoon* … "[t]he language of a grant of power to do 'all things necessary or convenient to be done for or in connexion with the performance of' an enumerated list of functions is of considerable width" … Plainly enough, the scope of a grant of power of this kind should be interpreted in light of the functions that the parliament has conferred on the body in question ... Where, as here, the legislature confers a function in general terms, a grant of power in the terms of s 22 will, generally speaking, have a commensurably wide scope ... In this case, the functions given to the CEO in s 21(1) of the ASADA Act … are conferred in general terms, and the CEO is given a wide discretion as to the means by which these functions are fulfilled, including in relation to the conduct of investigations into possible anti-doping rule violations.

[18] (1957) 96 CLR 145, 250.
[19] (2019) 164 ALD 63, [107].

> Having regard to the foregoing, we are confirmed in our conclusion that s 22 is to be construed broadly.[20]

10.34 Individuals who complete the 'report' user form are asked to provide a name (which may be a pseudonym) and preferred contact method and details (which may or may not include personal information, such as where an email address is supplied which includes a person's name). The user is then asked to complete a free text box with information about the conduct complained of, and may also upload electronic documents. It is likely that some (but not all) individuals who complete such a report will elect to include some degree of personal information in the report. The purpose of the report form is to enable individuals to report information about business practices and behaviours relating to the CDR that are of concern to them.

10.35 Prior to submitting a report, individuals are advised that:

> While the ACCC is typically best placed to respond to CDR reports, information submitted in a report may be provided to the OAIC if it is best placed to respond.
>
> As such, the information you submit as part of your report may be provided to either or both, the ACCC and OAIC, depending on which agency is the most appropriate to provide a response.

10.36 The second step in assessing compliance with APP 3.1 is to determine whether the particular collection of personal information is reasonably necessary for (or, for agencies, directly related to) one of those functions or activities. The starting point when assessing the scope of the necessary or convenient power is to identify one or more specific functions conferred on the Information Commissioner which might be supplemented by that ancillary power so as to include the handling of reports. The OAIC proposes to collect reports about business practices or behaviours relating to the CDR that are of concern to the author. This PIA discusses below each of the specific functions which may be supplemented by the ancillary power so as to authorise the collection of such reports.

10.37 Pursuant to section 56ER of the CCA, the Information Commissioner may conduct assessments of whether a CDR participant, or designated gateway, for CDR data is maintaining and handling the CDR data in accordance with the privacy safeguards or the consumer data rules (to the extent that those rules relate to the privacy safeguards, or the privacy or confidentiality of the CDR data). This PIA has found that the collection of information about possible non-compliance by CDR participants or designated gateways for CDR data with the privacy safeguards or the consumer data rules (to the extent that those rules relate to the privacy safeguards, or the privacy or confidentiality of the CDR data) is at least convenient to the performance of the Information Commissioner's function under section 56ER of the CCA. This is because:

(a) The power to conduct an assessment is expressed in very broad terms. The CCA provides for the Information Commissioner to conduct the assessment in the manner she considers appropriate; and

(b) The CCA does not expressly deal with the circumstances in which the Information Commissioner may choose to conduct such an assessment. For example, it does not explicitly dictate or limit the matters to which the Commissioner may have regard in determining whether to conduct an assessment. As such, it does not preclude the Commissioner from inviting reports which may be evaluated for the purposes of deciding whether to conduct an assessment.

10.38 This PIA also finds that the function of the Information Commissioner under subsection 9.6(2) of the Consumer Data Rules — auditing the compliance of any CDR participant with the privacy safeguards or the consumer data rules (to the extent that they relate to the privacy safeguards or the privacy and confidentiality of CDR data) — also supports the collection of reports about those matters, for the same reasons.

[20] *Hird v Chief Executive Officer of Australian Sports Anti-Doping Authority* (2015) 148 ALD 428, [210] (citations omitted).

10.39 Under section 56ES of the CCA, the functions of the Information Commissioner include handling CDR data breaches in accordance with Part IIIC of the Privacy Act, as modified by the CCA. The Information Commissioner has the power under section 26WR of the Privacy Act to direct a CDR participant or designated gateway to prepare and notify or otherwise publish the contents of a statement notifying a CDR data security breach. This PIA has found that the collection of reports about possible CDR data security breaches is at least convenient for or in connection with the performance of the Information Commissioner's functions under Part IIIC of the Privacy Act (as extended and modified). This is because:

(a) The Commissioner's power under subsection 26WR(1) is enlivened where the Commissioner is 'aware that there are reasonable grounds' to believe that there has been an eligible data breach;

(b) Neither the Privacy Act nor the CCA expressly provides for the matters to which the Information Commissioner may or must have regard when deciding whether to commence the procedures prescribed by section 26WR (i.e. to invite the CDR participant or designated gateway to make a submission in relation to the proposed direction);

(c) The Explanatory Memorandum to the Privacy Amendment (Notifiable Data Breaches) Bill 2016 noted that it was 'envisaged that this provision may be enlivened in circumstances such as where an eligible data breach comes to the attention of the Commissioner but has not come to the attention of an entity' but did not comment on the specific means by which this might come to the attention of the Commissioner; and

(d) The collection of reports about possible CDR data security breaches would not expand the functions of the Commissioner under Part IIIC but may instead provide another source of information about possible breaches, with the potential to support the Commissioner's function of issuing directions under section 26WR.

10.40 Pursuant to section 56ET of the CCA, the functions of the Information Commissioner include conducting investigations into acts or practices that may be privacy safeguard breaches in accordance with Part V of the Privacy Act, as modified by the CCA. In certain circumstances, the Information Commissioner is required to investigate an act or practice where it is the subject of a complaint made under section 56ET.

10.41 Subsection 40(2) of the Privacy Act (as it applies in the CDR context) also empowers the Commissioner to investigate acts or practices on her own initiative, where those acts or practices may be privacy safeguard breaches or a breach of section 56ED of the CCA, and the Commissioner thinks that it is desirable that the act or practice be investigated. For the reasons set out below, this PIA has found that the collection of reports about acts or practices which may be 'privacy safeguard breaches' or breaches of section 56ED is at least convenient for or in connection with the performance of the Information Commissioner's functions under Part V of the Privacy Act (as extended and modified):

(a) Neither the Privacy Act nor the CCA expressly provides for the matters to which the Information Commissioner may or must have regard when deciding whether to initiate an investigation under Part V;

(b) The collection of reports may bring possible privacy safeguard breaches to the attention of the Privacy Commissioner, where that would not otherwise have been the case (such as where the person making the report would not have been entitled to make a complaint under section 56ET); and

(c) The collection of reports would not expand or circumvent the way in which the Commissioner is required to perform her functions under Part V of the Privacy Act.

10.42 Finally, sections 56EU, 56EW and 56EX of the CCA enable the Information Commissioner to enforce compliance with the privacy safeguards through applications for civil penalties, enforceable undertakings or an injunction. It may be unlikely that a report to the Commissioner

(essentially a 'tip-off') would provide a proper basis for such enforcement action in its own right. However, this PIA has concluded that the collection of reports is also convenient to the performance of those functions, as such reports may lead to the initiation of other regulatory steps (such as the opening of an investigation under Part V of the Privacy Act) which ultimately result in formal enforcement action being taken where appropriate.

10.43 This PIA has not identified any other functions conferred on the Information Commissioner by Part IVD of the CCA which would authorise the soliciting or collection of reports in relation to the CDR. Accordingly, this PIA has found that the Information Commissioner is authorised under her ancillary powers to solicit and collect reports from any person about:

(a) acts or practices that may be 'privacy safeguard breaches' (as defined in subsection 56ET(1) of the CCA) or breaches of section 56ED of the CCA (privacy safeguard 1); or

(b) possible CDR data security breaches.

To the extent that such reports contain personal information (whether because the individual provides their name or an individual is otherwise reasonably identifiable from the information provided), this PIA has found that the collection of that personal information is at least directly related to the performance of the Information Commissioner's functions under Part IVD of the CCA and would therefore comply with APP 3.1.

10.44 However, this PIA has found that the Information Commissioner is not authorised under her ancillary powers to solicit reports about *any* business practice or behaviour relating to the CDR that is of concern to the author. The collection of reports about any business practice or behaviour relating to the CDR that is of concern to the person making the report goes beyond what is convenient for or in connection with the performance of the Information Commissioner's particular functions under Part IVD of the CCA. Indeed, it might be said to be inconvenient to their performance as the triage of those reports necessarily increases the workload of the Commissioner and her staff and the associated costs to the OAIC, diverting resources away from the performance of the Information Commissioner's regulatory functions. This is because the OAIC anticipates that the ACCC will be best placed to respond to a proportion of reports.

10.45 The Information Commissioner and the ACCC have been described as 'co-regulators' of the CDR. This may be a helpful term for describing their roles at a high level and when explaining the scheme to the public. However, it is apt to mislead at the level of identifying specific functions which might be relied on to support the collection of solicited personal information for the purposes of compliance with APP 3.1. This is because the Information Commissioner and the ACCC have distinct and discrete regulatory functions under the CCA — they do not share responsibility over the same subject matter in connection with the scheme. The Information Commissioner's role is a narrower one than that of the ACCC and is focused on compliance with the privacy safeguards and certain aspects of the CDR Rules relating to privacy and confidentiality.

10.46 In particular, this PIA observes that, consistent with the authorities discussed above, the scope of the Information Commissioner's functions and powers is not affected by what is convenient or efficient to the implementation of the CDR as a whole, or what might be most convenient, efficient or practical for the ACCC.

10.47 Accordingly, this PIA has concluded that the design of the reports handling functionality of the System presents a real risk of breach of APP 3.1. This is because the System invites the provision of information, including personal information, in reports about business practices or behaviours relating to the CDR generally. If individuals provide personal information in reports that fall outside the matters identified at [10.43] above, the Information Commissioner will collect solicited personal information that is not reasonably necessary for the Information Commissioner to perform her relevant functions under the CCA. That is, it has not been suggested that the Information Commissioner could not collect reports about the matters identified at [10.43] above without also soliciting reports about any other business practice or behaviour relating to the CDR. Further, the extent to which the Information Commissioner would

use a proportion of the personal information to be collected and held is expected to be limited to assessment and triage of which agency should respond, notwithstanding that the information will be held on s 47E(d) [redacted].

10.48 This PIA has also concluded that the proposed collection is not directly related to the performance of any function of the Information Commissioner, because it is not within the scope of any express function or ancillary power. As such, there would not be a clear and direct connection between any function of the Information Commissioner and any personal information collected in a report falling outside the matters identified at [10.43] above.

10.49 In these circumstances, this PIA recommends that the OAIC not proceed with the reports handling functionality of the System as designed (**Recommendation 4**). There are different options available to the OAIC to redesign the System so as to comply with APP 3.1. For example, individuals making a report could be required to answer a question from a multiple choice list about the subject matter of their report. Depending on the answer, the report could be sent to the OAIC's service desk or securely transmitted to the ACCC. In that scenario, the OAIC would not collect solicited personal information in reports to which the ACCC is best placed to respond. In the event that an individual inaccurately answered a question about the subject matter of their report, this would not be a breach of APP 3.1 (as any personal information would not have been solicited) and the OAIC could proceed to redirect the report to the ACCC.

10.50 Another option might be for the OAIC to ensure that reports are held for a short, defined period of time until the triage and assessment process has been completed. Reports that are best dealt with by the ACCC could then be permanently deleted or de-identified following transfer of the information to the ACCC. This may ensure that the OAIC does not 'collect' that personal information for the purposes of the Privacy Act, as it would not be collected for inclusion in a record.[21]

Enquiries

10.51 As with the report user form, individuals who complete the 'enquiry' user form are asked to provide a name (which may be a pseudonym) and preferred contact method and details (which may or may not include personal information). Individuals may upload an electronic document in relation to their enquiry. It is likely that some (but not all) individuals who submit a completed enquiry form will elect to provide some degree of personal information in the report. The purpose of the enquiry form is to enable individuals to find out general information about the CDR, including the roles and functions of the ACCC and OAIC and the rights and obligations of different categories of participants in the CDR.

10.52 Prior to submitting their enquiry, individuals are advised that:

> Depending on the nature of your enquiry, the ACCC or OAIC may be best placed to respond. Therefore, information submitted in an enquiry may be provided to the ACCC, OAIC or both agencies.

10.53 The Information Commissioner has no express function of collecting or handling enquiries. Similarly, no government decision or ministerial statement conferring an enquiry-handling function on the Commissioner has been identified. The OAIC has formed the view that the operation of the enquiry-handling component of the System would be authorised by subsection 10(2) of the AIC Act, as something 'convenient' to be done for or in connection with the performance of the Information Commissioner's statutory privacy functions. As with reports, the starting point when assessing the scope of the Information Commissioner's ancillary powers is to identify one or more specific functions conferred on the Information Commissioner which might be supplemented by that ancillary power so as to include the handling of enquiries.

10.54 Under paragraph 56EQ(1)(b) of the CCA, the Information Commissioner has the function of promoting an understanding and acceptance of the privacy safeguards. This PIA has found that that collecting and responding to enquiries about the privacy safeguards is at least convenient

[21] Privacy Act subsection 6(1).

to the performance of that function and is therefore within the scope of the Information Commissioner's power. This is because:

(a) the function is drafted in very broad terms and the legislature has not sought to prescribe the manner in which the Information Commissioner must perform that function;

(b) there is no express prohibition or limitation on the Information Commissioner's power to collect and handle enquiries about the privacy safeguards; and

(c) answering enquiries about the privacy safeguards can readily be seen to promote the understanding and acceptance of those safeguards, by responding to the specific query of the enquirer in each case.

10.55 This PIA has concluded that the expression 'promoting an understanding and acceptance of the privacy safeguards' should be given a broad interpretation. The scope of the power to handle enquiries about the privacy safeguards should therefore be taken to cover enquiries about any aspect of those safeguards, including the rights and obligations of individuals or entities bound by or affected by those safeguards, and the means by which compliance with the privacy safeguards can be enforced by the Information Commissioner.

10.56 This PIA has also found that the Information Commissioner's functions under sections 56ES and 56ET of the CCA — which extend and modify the application of Parts IIIC and V respectively of the Privacy Act — can properly be supplemented by the necessary or convenient power to authorise the handling of enquiries about those functions. These are functions which necessarily involve direct dealings between the Information Commissioner (or the OAIC) and participants in the CDR. An enquiries service is convenient to the performance of these functions as it may assist participants in the CDR to understand their respective rights and obligations under that scheme. Further, an initial channel for communication of a general nature may assist in streamlining the processes associated with making complaints and notifying the Commissioner of a CDR data breach.

10.57 In turn, the service can be expected to support the efficient and effective administration of these functions and powers. This is particularly relevant in the context of the CDR, as understanding the operation of Parts IIIC and V of the Privacy Act requires a careful reading of both pieces of legislation 'side by side' and it may be difficult for many individuals to understand the interaction between the two Acts.

10.58 This PIA has not identified any other functions conferred on the Information Commissioner by Part IVD of the CCA which would authorise the collection of enquiries. Accordingly, this PIA has found that the Information Commissioner is authorised to collect enquiries from any person about:

(a) any aspect of the privacy safeguards; or

(b) the Information Commissioner's functions under Parts IIIC and V of the Privacy Act (as modified and extended by the CCA).

10.59 This PIA has found — for substantially the same reasons given above in relation to reports — that the Information Commissioner is not authorised under her ancillary powers to solicit and collect enquiries about the CDR generally. Accordingly, this PIA has concluded that the collection of solicited personal information in enquiries about the CDR generally is not authorised by APP 3.1. This is because the collection of such personal information is not reasonably necessary for the Information Commissioner to perform her relevant functions under the CCA. That is, the Information Commissioner is readily able to collect enquiries about the matters identified at [10.58] above without soliciting personal information in enquiries about the CDR as a whole.

10.60 This PIA has also concluded that the collection of any personal information in enquiries falling outside the matters identified at [10.58] above would not be directly related to the performance

of any function of the Information Commissioner, because it is not within the scope of any express function or ancillary power.

10.61 In these circumstances, this PIA has recommended that the OAIC not proceed with the enquiries handling functionality of the System as designed (**Recommendation 4**). The observations at [10.49]-[10.50] above about possible ways of implementing the System with modifications are equally applicable in the context of enquiries.

Complaints

10.62 The Information Commissioner has an express function of handling complaints in relation to possible privacy safeguard breaches under section 56ET of the CCA. CDR consumers who wish to make a complaint are required to identify themselves and provide their title, first and last name, and contact details for their preferred contact method. Individuals who represent a small business complainant must also provide documents which evidence their authority to represent that business.

10.63 The complaint user form includes a free text box which allows the CDR consumer to describe the allegation, as well as the functionality to attach electronic documents in support of the complaint. The information provided in those formats is entirely dependent on the nature of the allegation and the way in which the complainant chooses to describe or substantiate it. It is possible that the complainant includes additional personal information with the complaint (including sensitive information) which may or may not be relevant to the question of whether there has been a breach of a privacy safeguard.

10.64 However, it is inherent in the nature of complaints processes that the complainant have some degree of discretion in framing the complaint and determining how to substantiate that complaint. In particular, when section 56ET of the CCA is read together with section 36 of the Privacy Act, those provisions allow for a complaint to be made about an act or practice which 'may be' a privacy safeguard breach. The purpose of those provisions is to allow certain CDR consumers an avenue to complain about acts or practices which might constitute such a breach, even if the complaint is ultimately found to be lacking in substance or no breach is established. As such, this PIA has found that the OAIC would not be able to effectively perform its complaints investigation function without collecting all the information (including personal information) which the complainant chooses to provide in support of the complaint. This PIA has therefore concluded that the OAIC will comply with APP 3.1 in relation to the complaints functionality of the System. Importantly, the privacy notice which will accompany the complaint user form explains the purpose of the form and how the collection relates to the Information Commissioner's functions. This will assist to ensure that individuals only provide personal information that is reasonably necessary for or directly related to the Information Commissioner's functions under section 56ET of the CCA.

APP 3.3

10.65 The OAIC will not expressly request that complainants provide any sensitive information when they lodge a complaint. However, consistent with the discussion above, to the extent that an individual chooses to provide such information, it will comply with APP 3.2, as it will be collected with the consent of the individual.

APP 3.5

10.66 Under APP 3.5, the OAIC must only collect personal information by lawful and fair means. As no law, court or tribunal order prevents the OAIC from collecting the personal information by way of the System, the collection of that information is therefore by lawful means. The collection of personal information will be by 'fair' means if it does not involve intimidation or deception, and is not unreasonably intrusive.[22] This PIA has found that the collection of solicited personal

[22] APP Guidelines, Chapter 3, paragraph 3.62.

information through the System will be by fair means as there is no intimidation or deception, and the information provided is at the discretion of the user who completes the form.

APP 3.6

10.67 APP 3.6 requires that the OAIC collect personal information about an individual only from the individual unless an exception applies. In the context of complaints, the right to complain under section 36 of the Privacy Act (as extended by section 56ET of the CCA) is afforded to the CDR consumer affected by the alleged privacy safeguard breach. As such, the OAIC will only collect solicited personal information where this is provided directly by the affected individual, in compliance with APP 3.6.

APP 4 — Dealing with unsolicited personal information

10.68 APP 4 applies if the OAIC receives unsolicited personal information in connection with its implementation of the System. Unsolicited information is information that an APP entity receives, but has taken no active steps to solicit.

10.69 It is possible that the OAIC may receive unsolicited personal information collected using the System. This is because the user forms include free text boxes and the capacity for CDR consumers (and others) to upload files for attachment to their form. If the OAIC receives unsolicited personal information, it must assess whether it could have collected the personal information pursuant to APP 3. It is likely that, in at least some cases, the OAIC would conclude that it could not have collected the information under APP 3. For example, individuals may use the forms to submit hoax or nuisance information, or complaints unrelated to the CDR or the OAIC's other functions. The OAIC's obligations in relation to the handling of that unsolicited personal information would then depend on whether the information is contained in a Commonwealth record.

10.70 The term 'Commonwealth record' is defined in section 3 of the *Archives Act 1983* and means:

(a) a record that is the property of the Commonwealth or of a Commonwealth institution; or

(b) a record that is to be deemed to be a Commonwealth record by virtue of a regulation under subsection (6) or by virtue of section 22,

but does not include a record that is 'exempt material'. The term 'record' is in turn defined to mean a document, or an object, in any form (including any electronic form) that is, or has been, kept by reason of:

(a) any information or matter that it contains or that can be obtained from it; or

(b) its connection with any event, person, circumstance or thing.

10.71 This PIA has found that any unsolicited personal information collected through the System will likely be a Commonwealth record as it will be stored on s 47E(d) [redacted], and the OAIC is therefore not required to destroy or de-identify that information. That information must be handled in accordance with APPs 5 to 13, as if the OAIC had collected it under APP 3.

APP 5 - Notification of the collection of personal information

10.72 APP 5 requires that where the OAIC collects personal information about an individual, the OAIC takes reasonable steps to notify the individual of certain matters (**APP 5 Matters**) or otherwise, to ensure that the individual is aware of those matters. Such a notification must occur at or before the time of the collection, or if that is not practicable, as soon as practicable afterwards.

10.73 The APP 5 Matters include: the identity and contact details of the OAIC; the purposes for which the OAIC collects the information; the main consequences (if any) for the individual if some or all of the personal information is not collected by the OAIC; and any other APP entity, body or

person (or the types of such entities, bodies or persons) to which the OAIC usually discloses personal information of that kind.

10.74 Whether the OAIC has taken reasonable steps to notify the individual of the APP 5 Matters is to be determined objectively. The relevant test is whether a reasonable person would agree that in the circumstances, the OAIC had acted reasonably in providing notice or ensuring awareness of the APP 5 Matters.

10.75 Whether the OAIC has satisfied this test will depend on:

(a) the type of personal information collected, including whether it includes any sensitive information;

(b) the possible adverse consequences for an individual as a result of the collection. More rigorous steps may be required as the risk of adversity increases;

(c) the special needs (if any) of the individual. More rigorous steps may be required if personal information is collected from an individual from a non-English speaking background who may not readily understand the APP 5 Matters; and

(d) the practicality, including time and cost involved, and whether these factors make it unreasonable to take particular steps will depend on whether the burden is excessive in all the circumstances. However, the OAIC would not be automatically excused from taking particular steps by reason only that it would be inconvenient, time or resource consuming to do so.[23]

10.76 In the circumstances of the System, the following factors are relevant to this assessment:

(a) the OAIC is collecting new categories of personal information to support new functions and may collect a broad scope of personal information that could contain sensitive information;

(b) the OAIC's primary purpose for this collection is to enable it to perform its statutory functions in respect of the CDR;

(c) the OAIC may use the information collected for the purpose of responding to enquiries, resolving identified concerns about handling CDR data and investigating CDR participants' conduct;

(d) there may be adverse consequences for entities which are found to have engaged in a privacy safeguard breach; and

(e) the individuals who will be affected are CDR consumers or their representatives.

10.77 The OAIC has suggested in its APP Guidelines that reasonable steps that an APP entity could consider include:

(a) if the entity collects personal information directly from an individual who completes a form or uses an online facility — clearly and prominently displaying the APP 5 Matters in the form or providing a readily accessible link to an APP 5 notice, and asking the individual to confirm that they have reviewed the notice before providing their personal information;

(b) if personal information is collected by telephone, explaining the APP 5 matters to the individual at the commencement of the call (perhaps following a template script or using an automated message). Where this is not practicable, an entity should give the individual information about the APP 5 matters as soon as possible afterwards, such as

[23] APP Guidelines, Chapter 5, paragraph 5.4.

in any subsequent electronic or paper-based communication, or directing the individual to the relevant notice on the entity's website; or

(c) if the entity collects personal information from another entity, confirming whether the other entity has provided the relevant APP 5 notice to the individual, or whether the individual was otherwise aware of the APP 5 matters at the time of the collection.[24]

10.78 Having regard to these considerations, this PIA has found that it is reasonable and appropriate for the OAIC to take steps to notify CDR consumers of the applicable APP 5 Matters. APP 5 requires entities to notify individuals of the APP 5 Matters at the time of collection of their personal information, or if that is not practicable, as soon as practicable afterwards. The APP Guidelines state that this requirement recognises that it is preferable that an individual can make an informed choice about whether to provide personal information to an APP entity.[25]

10.79 We note that the OAIC has developed discrete privacy notices (extracted in full at [5.20], [5.25] and [5.31] above) which will be displayed to users before they complete a report, enquiry or complaint form. We note that our comments on each of the forms below are made based on the current design of the System. If the OAIC adopts Recommendation 4, further modifications to the privacy notices for the enquiry and report forms would be required.

Enquiry form privacy notice

10.80 The enquiry form privacy notice identifies the OAIC and/or the ACCC as potential recipients of any personal information supplied, and includes email addresses for both, thus addressing the matter in APP 5.2(a).

10.1 The notice does not address the matter in APP 5.2(c), which is that if the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order — the fact that the collection is so required or authorised (including the name of the Australian law, or details of the court/tribunal order, that requires or authorises the collection). For the reasons set out above, this PIA has concluded that the OAIC is not authorised to solicit personal information in enquiries in relation to the CDR generally. However, as the enquiries functionality of the System is intended to support both the OAIC and the ACCC to carry out their respective regulatory functions under Part IVD of the CCA, this PIA has found that it would be preferable for the enquiry form privacy notice to specifically refer to that legislation and recommends that the notice be amended accordingly (**Recommendation 5(a)**). Suggested amendments to give effect to this recommendation are shown in Schedule 3.

10.2 The enquiry form privacy notice also addresses the matters in APP 5.2(d) and (f). The notice partially addresses the matters in APP 5.2(g) and (h). This PIA therefore recommends that the OAIC amend the notice to address those matters comprehensively (**Recommendation 5(b)**). Suggested amendments to give effect to this recommendation are shown at Schedule 3.

10.3 This PIA has found that it is reasonable for the notice not to address APP 5.2(b) (which applies where an APP entity collects personal information indirectly) or APP 5.2(e) (consequences if some or all of the information is not collected) in the context of a general enquiry form. Similarly, it is reasonable not to address the matters in APP 5.2(i) and (j), as it is impracticable to inform users of whether the OAIC is likely to disclose their personal information to overseas recipients in circumstances in which the OAIC has no reliable way to predict what information might be collected through the form.

10.4 The notice does not clearly state exactly which entity collects any personal information in the first instance, stating that personal information 'submitted in an enquiry may be provided to the OAIC, ACCC or both agencies'. This suggests that the information is collected by an unspecified third party (or that it is not collected at all) rather than transmitted to s 47E(d) [redacted]. Given that the user forms will be accessed from the CDR website (hosted by the ACCC) users may not appreciate that the information is collected by the OAIC in the first instance. This PIA

[24] APP Guidelines, Chapter 5, paragraph 5.6.
[25] APP Guidelines, Chapter 5, paragraph 5.35.

recommends that the OAIC amend the privacy notice to state that personal information will be collected by the OAIC in the first instance, and that personal information will be disclosed to the ACCC if it is best placed to respond to the enquiry (**Recommendation 5(c)**). Suggested amendments to give effect to this recommendation are shown in Schedule 3.

Report form privacy notice

10.5 The report form privacy notice identifies the OAIC and/or the ACCC as potential recipients of any personal information supplied, and includes email addresses for both, thus satisfying APP 5.2(a).

10.6 The notice does not address the matter in APP 5.2(c), which is that if the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order — the fact that the collection is so required or authorised (including the name of the Australian law, or details of the court/tribunal order, that requires or authorises the collection). For the reasons set out above, this PIA has concluded that the OAIC is not authorised to solicit personal information in reports in relation to any business practice or behaviour relating to the CDR that is of concern to the author of the report. As such, it would not be appropriate to include a statement to the contrary in the privacy notice. However, as the reports functionality of the System is intended to support both agencies to carry out their regulatory functions under Part IVD of the CCA, this PIA has found that it would be preferable for the report form privacy notice to specifically refer to that legislation and recommends that the notice be amended accordingly (**Recommendation 6(a)**). Suggested amendments to give effect to this recommendation are shown in Schedule 3.

10.7 The report form privacy notice addresses the matters in APP 5.2(d) and (f). The notice partially addresses the matters in APP 5.2(g) and (h). This PIA recommends that the OAIC amend the notice to address those matters comprehensively (**Recommendation 6(b)**). Suggested amendments to give effect to this recommendation are shown at Schedule 3.

10.8 As with the enquiry form, this PIA has found that it is reasonable not to address the matters in APP 5.2(b), (e), (i) or (j) for the reasons discussed above.

10.9 Once again, the notice does not clearly state exactly which entity collects any personal information in the first instance, stating that 'the information you submit as part of your report may be provided to either or both, the ACCC and OAIC, depending on which agency is the most appropriate to provide a response.' For the reasons discussed above in relation to the enquiry form, this PIA recommends that the OAIC amend the privacy notice to state that personal information will be collected by the OAIC in the first instance, and that personal information will be disclosed to the ACCC if it is best placed to respond to the report (**Recommendation 6(c)**).

Complaint form privacy notice

10.10 The complaint privacy notice addresses all of the APP 5 Matters other than APP 5.2(b), which is not relevant given that complaints must be made by the affected individual or small business. The notice partially addresses the matters in APP 5.2(g) and (h). This PIA recommends that the OAIC amend the notice to address those matters comprehensively (**Recommendation 7**). Suggested amendments to give effect to this recommendation are shown at Schedule 3.

APP 6 - Use or disclosure of personal information

10.11 The intent of APP 6 is that the OAIC will generally use and disclose an individual's personal information only in ways the individual would expect or where one of the exceptions applies.

Use of personal information

10.12 The term 'use' is not defined in the Privacy Act. The APP Guidelines provide that the OAIC 'uses' information where it handles or undertakes an activity with the information, within the

OAIC's effective control.[26] Examples include the OAIC accessing and reading the personal information; and the OAIC passing the personal information from one part of the OAIC to another.

10.13 The implementation of the System will involve the collection of personal information in enquiry, report and complaint forms.

10.14 The information submitted in enquiry and report forms will be collected for the primary purpose of assessing the enquiry or report (including determining whether the ACCC or the OAIC is best placed to respond) and, if appropriate, responding to the enquiry or report. The OAIC will use any personal information collected in enquiries for this purpose in compliance with APP 6.

10.15 The personal information collected in complaint forms will be collected for the primary purpose of performing the Information Commissioner's complaint handling functions under section 56ET of the CCA. The personal information collected will be used by the OAIC for the primary purpose of collection, including assessing, inquiring into, investigating and conciliating the complaint in accordance with the Information Commissioner's powers and the regulatory processes in Part V of the Privacy Act. This PIA therefore finds that the OAIC will use the personal information collected for the primary purpose of collection.

10.16 s 47E(d) [redacted]

The APP Guidelines state that a transfer of information from an agency to a contracted service provider will ordinarily be a disclosure for the purposes of the APPs. However, in certain limited circumstances, the transfer of information may be a use rather than a disclosure. This occurs where the agency does not release the subsequent handling of the personal information from its effective control. We have assumed that the OAIC will retain effective control over the personal information to be hosted in the cloud.

Disclosure of personal information

10.17 The term 'disclose' is not defined in the Privacy Act. In accordance with the APP Guidelines, an APP entity 'discloses' personal information where it makes it accessible to others outside the entity and releases the subsequent handling of the information from its effective control. This focuses on the act done by the disclosing party.[27]

10.18 The OAIC intends to disclose personal information collected in an enquiry, report or complaint to the ACCC where the ACCC is best placed to respond to that submission because that information is relevant to the ACCC's statutory functions. The ACCC is responsible for accreditation criteria and processes for data recipients, the accreditation register and the investigation of serious and systemic breaches of the CDR. These disclosures will be made for the primary purpose of collection of the personal information, as in each case the OAIC collects the information to enable the assessment and response to enquiries, reports and complaints about the CDR. While section 29 of the AIC Act restricts the handling of information collected by the Information Commissioner in the performance of her functions, that provision does not apply to disclosures of certain information to the ACCC, being information that:

(a) was acquired in the course of performing a function described in paragraph 9(1)(b) of the AIC Act (about the consumer data right), or exercising a related power; or

(b) could be relevant to either of the following decisions:

(i) a decision under subsection 56CA(1) (about accreditation for the consumer data right) of the CCA;

(ii) a decision under the consumer data rules relating to a person's accreditation under subsection 56CA(1) of that Act.

[26] APP Guidelines, Chapter 6, paragraph 6.8.
[27] APP Guidelines, Chapter 6, paragraph 6.9.

10.19 This PIA concludes that the OAIC will comply with APP 6 in its implementation of the Project.

APP 7 — Direct marketing

10.20 APP 7 regulates the use and disclosure of personal information for the purpose of direct marketing. APP 7 applies to Organisations as defined in the Privacy Act. Pursuant to subsection 7A(1) of the Privacy Act, that Act applies to the acts or practices of certain agencies as if they were acts or practices of Organisations. However, the OAIC is only subject to the requirements of APP 7 if:

(a) the OAIC is listed in Part I of Schedule 2 to the FOI Act and is prescribed by regulations; or

(b) the OAIC's acts or practices in respect of the System relate to a commercial activity of the OAIC, and the OAIC is specified in Division 1 of Part II of Schedule 2 to the FOI Act.[28]

10.21 As neither of the circumstances described in [10.20] above arises, APP 7 does not apply to the OAIC with respect to the System.

APP 8 — Cross-border disclosure of personal information

10.22 APP 8 requires that an entity must, before disclosing personal information to an overseas recipient, take steps that are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs. An exception applies where the disclosure of the information is required or authorised by or under an Australian law. The OAIC does not intend to disclose any personal information to an overseas recipient as a direct result of the implementation of the System. The servers on which the System will be hosted are located in Australia.

10.23 The OAIC may disclose personal information to an overseas recipient in the course of investigating a complaint about a privacy safeguard breach, such as where the respondent is based overseas. A disclosure in these circumstances would be consistent with the manner in which the OAIC currently handles privacy complaints made under the Privacy Act and would be implicitly authorised by that Act as it applies to the CDR. Accordingly, it is not necessary to assess compliance with APP 8 in further detail for this PIA Report.

APP 9 — Adoption, use or disclosure of government related identifiers

10.24 As with APP 7, APP 9 is directed toward Organisations as defined in the Privacy Act. As neither of the circumstances described in [10.20] above arises, APP 9 does not apply to the OAIC with respect to the System.

APP 10 — Quality of personal information

10.25 Under APP 10.1, the OAIC needs to determine what steps (if any) are reasonable for it to take in order to verify that the personal information collected through the System is accurate, up-to-date and complete. In the context of APP 10, the 'reasonable steps' that the OAIC should take will depend upon circumstances that include:

(a) the sensitivity of the personal information;

(b) the nature of the OAIC (including its size, resources and business models);

(c) the possible adverse consequences for an individual if the quality of personal information is not ensured; and

[28] Privacy Act section 7A.

(d) the practicability, including time and cost involved. However, the OAIC is not excused from taking particular steps by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take particular steps will depend on whether the burden is excessive in all the circumstances.[29]

10.26 The features of the System and its implementation that are relevant to an assessment of compliance with APP 10.1 include:

(a) the OAIC will collect information directly from CDR consumers, meaning that it is generally reasonable to assume that the information is accurate and up-to-date;

(b) for the purposes of assessing and responding to enquiries, the OAIC does not require information on the CDR consumer to be accurate (while the provision of inaccurate personal information may result in a less helpful response, this is a risk that can reasonably be borne by the person making the enquiry);

(c) the OAIC will require small businesses to submit information intended to allow the OAIC to confirm that it has jurisdiction to investigate their complaint, and that the purported representative of the business is indeed authorised to represent that business;

(d) the complaint form prompts the complainant to provide certain information about the allegation, including what happened and when, and which information or individuals were involved, which will assist to increase the likelihood that complete information is provided about the substance of the complaint; and

(e) each of the report forms allows for review and editing prior to submission.

10.27 This PIA has found that these are reasonable steps for the OAIC to take to verify that the personal information it collects is accurate, up-to-date and complete and that the OAIC will comply with APP 10.1 in its delivery of the System.

10.28 APP 10.2 requires the OAIC to take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the OAIC uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant. The efficient triage of submissions through the Service Desk will assist the OAIC to ensure that personal information remains up-to-date at the time it is used or disclosed. Importantly, in circumstances where there are potential consequences for affected individuals or entities as a result of the use or disclosure of personal information submitted with a complaint (or a report about privacy-related matters), the quality of that information will be assessed, evaluated and tested in accordance with the OAIC's standard practice before any such decision is made. This PIA has found that the OAIC will comply with APP 10.2 in its implementation of the System.

10.29 Accordingly, this PIA Report finds that the OAIC will comply with APP 10 in its delivery of the System.

APP 11 — Security of personal information

10.30 APP 11.1 requires that the OAIC take such steps as are reasonable to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure. APP 11.1 is of particular relevance in the context of the System, which involves the introduction of IT changes which will alter the ways in which personal information is received, stored, transferred and accessed by OAIC staff.

10.31 The term 'reasonable' is not defined in the Privacy Act. The APP Guidelines provide that the term bears its ordinary meaning, as being based upon, or according to, reason and capable of

[29] APP Guidelines, Chapter 10, paragraph 10.6.

sound explanation. What is reasonable is a question of fact in each individual case. It is an objective test that has regard to how a reasonable person, who is properly informed, would be expected to act in the circumstances. What is reasonable can be influenced by current standards and practices.[30] The reasonable steps that an APP entity should take under APP 11.1 are influenced by the following considerations:

(a) the nature of the APP entity. Relevant considerations include an APP entity's size, resources, the complexity of its operations and its business model;

(b) the amount and sensitivity of the personal information held. Generally, as the amount and/or sensitivity of personal information that is held increases, so too will the steps that it is reasonable to take to protect it;

(c) the possible adverse consequences for an individual in the case of a breach. More rigorous steps may be required as the risk of adversity increases;

(d) the practical implications of implementing the security measure, including time and cost involved. However, an entity is not excused from taking particular steps to protect information by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take particular steps will depend on whether the burden is excessive in all the circumstances; and

(e) whether a security measure is in itself privacy invasive. For example, while an APP entity should ensure that an individual is authorised to access information, it should not require an individual to supply more information than is necessary to identify themselves when dealing with the entity.

10.32 To resolve the question of whether the steps proposed by the OAIC to protect personal information are 'reasonable' for the purposes of APP 11.1, it is necessary to look to the technical and operational security features of the System, and any security assessments, certifications, or accreditations to which that solution has been subjected. Reasonable steps should include, where relevant, implementing strategies in relation to:

(a) governance, culture and training;

(b) internal practices, procedures and systems;

(c) ICT security;

(d) access security;

(e) third party providers (including cloud computing);

(f) data breaches;

(g) physical security;

(h) destruction and de-identification; and

(i) standards.[31]

[30] APP Guidelines, Chapter B, paragraph B.105.
[31] APP Guidelines, Chapter 11, paragraph 11.8.

10.33 The System will undergo rigorous security testing including threat-modelling and automated scanning, and third-party audits will be carried out.

10.34 The OAIC will implement the following security measures in relation to the System:

(a) a governance framework documented in the MOU with the ACCC;

s 47E(d)

10.35 As outlined above, this PIA has been drafted on the assumption that the information security measures in place in relation to Resolve are compliant with the APPs. We have concluded that the measures discussed above in relation to the System would be characterised as 'reasonable' steps for the purposes of meeting the obligations of the OAIC under APP 11.1. This PIA has also recommended that training delivered to users of the System include information about relevant information security measures and requirements.

10.36 APP 11.2 imposes a general obligation on the OAIC to take such steps as are reasonable in the circumstances to destroy information or to ensure that information is de-identified where it is no longer needed for the purpose for which it was collected. However, that obligation does not apply to information which is contained in a Commonwealth record. The OAIC will retain and dispose of records containing information collected by the System in accordance with the relevant records disposal authority. As such, this PIA has found that the OAIC will comply with APP 11.2 in relation to the System.

APP 12 — Access to personal information

10.37 Under APP 12, the OAIC is required to give an individual access to their personal information held by it unless it is authorised to refuse access under the FOI Act or other Commonwealth or Norfolk Island legislation. The exceptions to access in APP 12.3 only apply to Organisations and would not apply to an Agency such as the OAIC.

10.38 The OAIC must give the individual access to their personal information within 30 days of the request, and in the form reasonably requested by the individual. The OAIC cannot charge the individual for making the request or giving access to the information.

10.39 The OAIC has existing procedures described in its Privacy Policy for dealing with requests for access to personal information made under the Privacy Act, which will not be affected by the implementation of the System. Each of the three privacy notices also provides information about how individuals can request access to their personal information held by the OAIC. As such, it is unnecessary to give further consideration to compliance with APP 12 in this PIA.

APP 13 — Correction of personal information

10.40 Under APP 13, the OAIC must take reasonable steps to correct personal information to ensure that, having regard to the purpose for which it is held, it is accurate, up-to-date, complete, relevant and not misleading.

10.41 The OAIC already has existing procedures described in its Privacy Policy for dealing with requests for correction of personal information made under the Privacy Act, which will not be affected by the implementation of the System. This PIA has recommended that the OAIC amend the privacy notices to advise individuals that its Privacy Policy contains information about correction of personal information. As such, it is unnecessary to give further consideration to compliance with APP 13 in this PIA.

Glossary

Acronyms and Initialisms	
ACCC	The Australian Competition and Consumer Commission
API	application programming interface
APP	Australian Privacy Principle
CCA	*Competition and Consumer Act 2010* (Cth)
CDR	means the Consumer Data Right
MOU	the proposed Memorandum of Understanding between the OAIC and ACCC
MVP	minimum viable product
OAIC	Office of the Australian Information Commissioner
PIA	Privacy Impact Assessment
SSL	means secure socket layer.

Definitions	
APP Guidelines or Guidelines	The APP Guidelines published by the OAIC at http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/ as revised on 2 March 2018. The APP Guidelines outline the mandatory requirements of the APPs, how the OAIC will interpret the APPs, and matters that may be taken into account when assessing an Agency's compliance with the Privacy Act and the APPs.
APPs	means the Australian Privacy Principles.
APP Entity	has the same meaning given under the *Privacy Act 1988* (Cth).
Approved Privacy Code	means an APP Code, as defined under section 26C of the Privacy Act.
AIC Act	The *Australian Information Commissioner Act 2010* (Cth).
CDR consumers	means Australian consumers.
Commonwealth entity	has the same meaning given under the *Public Governance, Performance and Accountability Act 2013* (Cth). This PIA also refers to Commonwealth entities as 'Agencies'.
Cypha	means Cypha Interactive Pty Limited.
Explanatory Memorandum	The Explanatory Memorandum to the *Treasury Laws Amendment (Consumer Data Right) Bill 2019 (Cth)*.
Organisation	has the same meaning given under section 6C of the Privacy Act.
Personal information	means information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not, as defined in section 6 of the Privacy Act. Personal information may, in certain circumstances, include the following:

	(a) an email address (where that address contains a person's name); (b) an email address (in cases where that address does not contain a person's name, but the identity of the email account holder can be reasonably identified, including by reference to account-related information holdings); and (c) a telephone number (in cases where the person associated with the telephone number can be reasonably identified by reference to account-related information holdings).
Privacy Act	The *Privacy Act 1988* (Cth).
Project Description	The description of the System contained in section 5 of this PIA Report.
Sensitive information	means: (a) information or an opinion about an individual's: (i) racial or ethnic origin; or (ii) political opinions; or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or (v) philosophical beliefs; or (vi) membership of a professional or trade association; or (vii) membership of a trade union; or (viii) sexual orientation or practices; or (ix) criminal record; that is also personal information; or (b) health information about an individual; or (c) genetic information about an individual that is not otherwise health information; or (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or (e) biometric templates.
System	means the Consumer Data Right Complaints and Reports Handling System.
Treasury Laws Amendment Act	The *Treasury Laws Amendment (Consumer Data Right) Act 2019* (Cth).

Schedule 1

Functions of the Information Commissioner under Part IVD of the CCA

Provision of Part IVD	Function
56AD(3)	Participate in consultation with the Minister prior to the Minister making an instrument under subsection 56AC(2) designating a sector of the economy to be subject to the CDR.
56AE(1)(c)(i)	Participate in consultation with the Commission about the matters in paragraphs 56AD(1)(a) to (e) in relation to an instrument proposing to designate a sector.
56AF	When consulted by the Minister under 56AD(3), analyse the likely effect of making the instrument on the privacy or confidentiality of consumers' information, report to the Minister about that analysis and publish the report (except for any excluded part).
56BI(1)(d), (e), (f)	Receive reports (from CDR participants for CDR data, accredited persons, designated gateways, the Data Recipient Accreditor, the Accreditation Registrar and the Data Standards Chair) under the requirements of the consumer data rules.
56BQ(1)(b)(i)	Participate in consultation with the Commission about proposed consumer data rules.
56BS	Participate in consultation with the Commission about any proposed 'emergency' consumer data rules.
56DA(4)	Participate in consultation with the Commission about any proposal to recognise an external dispute resolution scheme.
56EQ(1)(a)	Making guidelines for the avoidance of acts or practices that may breach the privacy safeguards.
56EQ(1)(b)	Promoting an understanding and acceptance of the privacy safeguards.

Provision of Part IVD	Function
56EQ(1)(c)	Undertaking educational programs for the purposes of promoting the protection of CDR data.
56ER	Conducting assessments of whether a CDR participant, or designated gateway, for CDR data is maintaining and handling the CDR data in accordance with the privacy safeguards or the consumer data rules (to the extent that those rules relate to the privacy safeguards, or the privacy or confidentiality of the CDR data).
56ES	Handling CDR data breaches in accordance with Part IIIC of the Privacy Act, as modified by the CCA.
56ET	Handling complaints about acts or practices that may be privacy safeguard breaches in accordance with Part V of the Privacy Act, as modified by the CCA.
Section 56EU; section 56EW; section 56EX	Enforcing compliance with the privacy safeguards through applications for civil penalties, enforceable undertakings or an injunction.
56GA(1)(a)	The functions conferred on the Information Commissioner by another provision of Part IVD, or by an instrument made under that Part.
	The Consumer Data Rules confer additional functions on the Information Commissioner, being: • Rule 7.2(1): The Commissioner may approve a form for a CDR policy; • Rule 8.9(2)(b)(iii): Participate in consultation with the Data Standards Chair on a draft proposed data standard or amendment; and • 9.6(2): Auditing the compliance of any CDR participant with the privacy safeguards or the consumer data rules (to the extent that they relate to the privacy safeguards or the privacy and confidentiality of CDR data).
Section 56GA(1)(b)	Consult with or advise the Minister, Commission or Data Standards Chair about any matter relevant to the operation

Provision of Part IVD	Function
	of Part IVD (or the operation of instruments made under that Part).

Schedule 2

Australian Privacy Principles

Australian Privacy Principle 1 — open and transparent management of Personal Information

1.1 The object of this principle is to ensure that APP entities manage Personal Information in an open and transparent way.

Compliance with the Australian Privacy Principles etc.

1.2 An APP entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that:

(a) will ensure that the entity complies with the Australian Privacy Principles and a registered APP code (if any) that binds the entity; and

(b) will enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the Australian Privacy Principles or such a code.

APP Privacy policy

1.3 An APP entity must have a clearly expressed and up to date policy (the ***APP privacy policy***) about the management of Personal Information by the entity.

1.4 Without limiting subclause 1.3, the APP privacy policy of the APP entity must contain the following information:

(a) the kinds of Personal Information that the entity collects and holds;

(b) how the entity collects and holds Personal Information;

(c) the purposes for which the entity collects, holds, uses and discloses Personal Information;

(d) how an individual may access Personal Information about the individual that is held by the entity and seek the correction of such information;

(e) how an individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;

(f) whether the entity is likely to disclose Personal Information to overseas recipients;

(g) if the entity is likely to disclose Personal Information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy.

Availability of APP privacy policy etc.

1.5 An APP entity must take such steps as are reasonable in the circumstances to make its APP privacy policy available:

(a) free of charge; and

(b) in such form as is appropriate.

Note: An APP entity will usually make its APP privacy policy available on the entity's website.

1.6 If a person or body requests a copy of the APP privacy policy of an APP entity in a particular form, the entity must take such steps as are reasonable in the circumstances to give the person or body a copy in that form.

Australian Privacy Principle 2 — anonymity and pseudonymity

2.1 Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter.

2.2 Subclause 2.1 does not apply if, in relation to that matter:

(a) the APP entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves; or

(b) it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym.

Australian Privacy Principle 3 — collection of solicited personal information

Personal information other than sensitive information

3.1 If an APP entity is an agency, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.

3.2 If an APP entity is an organisation, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity's functions or activities.

Sensitive information

3.3 An APP entity must not collect sensitive information about an individual unless:

(a) the individual consents to the collection of the information and:

(i) if the entity is an agency — the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or

(ii) if the entity is an organisation — the information is reasonably necessary for one or more of the entity's functions or activities; or

(b) subclause 3.4 applies in relation to the information.

3.4 This subclause applies in relation to sensitive information about an individual if:

(a) the collection of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(b) a permitted general situation exists in relation to the collection of the information by the APP entity; or

(c) the APP entity is an organisation and a permitted health situation exists in relation to the collection of the information by the entity; or

(d) the APP entity is an enforcement body and the entity reasonably believes that:

(i) if the entity is the Immigration Department — the collection of the information is reasonably necessary for, or directly related to, one or more enforcement related activities conducted by, or on behalf of, the entity; or

(ii) otherwise — the collection of the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or

(e) the APP entity is a non-profit organisation and both of the following apply:

(i) the information relates to the activities of the organisation;

(ii) the information relates solely to the members of the organisation, or to individuals who have regular contact with the organisation in connection with its activities.

Note: For permitted general situation, see section 16A. For permitted health situation, see section 16B.

Means of collection

3.5 An APP entity must collect personal information only by lawful and fair means.

3.6 An APP entity must collect personal information about an individual only from the individual unless:

(a) if the entity is an agency:

(i) the individual consents to the collection of the information from someone other than the individual; or

(ii) the entity is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual; or

(b) it is unreasonable or impracticable to do so.

Solicited personal information

3.7 This principle applies to the collection of personal information that is solicited by an APP entity.

Australian Privacy Principle 4 — dealing with unsolicited Personal Information

4.1 If:

(a) an APP entity receives Personal Information; and

(b) the entity did not solicit the information;

the entity must, within a reasonable period after receiving the information, determine whether or not the entity could have collected the information under Australian Privacy Principle 3 if the entity had solicited the information.

4.2 The APP entity may use or disclose the Personal Information for the purposes of making the determination under subclause 4.1.

4.3 If:

(a) the APP entity determines that the entity could not have collected the Personal Information; and

(b) the information is not contained in a Commonwealth record;

the entity must, as soon as practicable but only if it is lawful and reasonable to do so, destroy the information or ensure that the information is de-identified.

4.4 If subclause 4.3 does not apply in relation to the Personal Information, Australian Privacy Principles 5 to 13 apply in relation to the information as if the entity had collected the information under Australian Privacy Principle 3.

Australian Privacy Principle 5 — notification of the collection of Personal Information

5.1 At or before the time or, if that is not practicable, as soon as practicable after, an APP entity collects Personal Information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances:

(a) to notify the individual of such matters referred to in subclause 5.2 as are reasonable in the circumstances; or

(b) to otherwise ensure that the individual is aware of any such matters.

5.2 The matters for the purposes of subclause 5.1 are as follows:

(a) the identity and contact details of the APP entity;

(b) if:

(i) the APP entity collects the Personal Information from someone other than the individual; or

(ii) the individual may not be aware that the APP entity has collected the Personal Information;

the fact that the entity so collects, or has collected, the information and the circumstances of that collection;

(c) if the collection of the Personal Information is required or authorised by or under an Australian law or a court/tribunal order — the fact that the collection is so required or authorised (including the name of the Australian law, or details of the court/tribunal order, that requires or authorises the collection);

(d) the purposes for which the APP entity collects the Personal Information;

(e) the main consequences (if any) for the individual if all or some of the Personal Information is not collected by the APP entity;

(f) any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which the APP entity usually discloses Personal Information of the kind collected by the entity;

(g) that the APP privacy policy of the APP entity contains information about how the individual may access the Personal Information about the individual that is held by the entity and seek the correction of such information;

(h) that the APP privacy policy of the APP entity contains information about how the individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;

(i) whether the APP entity is likely to disclose the Personal Information to overseas recipients;

(j) if the APP entity is likely to disclose the Personal Information to overseas recipients — the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.

Australian Privacy Principle 6 — use or disclosure of Personal Information

Use or disclosure

6.1 If an APP entity holds Personal Information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless:

(a) the individual has consented to the use or disclosure of the information; or

(b) subclause 6.2 or 6.3 applies in relation to the use or disclosure of the information.

Note: Australian Privacy Principle 8 sets out requirements for the disclosure of Personal Information to a person who is not in Australia or an external Territory.

6.2 This subclause applies in relation to the use or disclosure of Personal Information about an individual if:

(a) the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is:

(i) if the information is Sensitive Information — directly related to the primary purpose; or

(ii) if the information is not Sensitive Information — related to the primary purpose; or

(b) the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(c) a permitted general situation exists in relation to the use or disclosure of the information by the APP entity; or

(d) the APP entity is an organisation and a permitted health situation exists in relation to the use or disclosure of the information by the entity; or

(e) the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

Note: For permitted general situation, see section 16A. For permitted health situation, see section 16B.

6.3 This subclause applies in relation to the disclosure of Personal Information about an individual by an APP entity that is an agency if:

(a) the agency is not an enforcement body; and

(b) the information is biometric information or biometric templates; and

(c) the recipient of the information is an enforcement body; and

(d) the disclosure is conducted in accordance with the guidelines made by the Commissioner for the purposes of this paragraph.

6.4 If:

(a) the APP entity is an organisation; and

(b) subsection 16B(2) applied in relation to the collection of the Personal Information by the entity;

the entity must take such steps as are reasonable in the circumstances to ensure that the information is de-identified before the entity discloses it in accordance with subclause 6.1 or 6.2.

Written note of use or disclosure

6.5 If an APP entity uses or discloses Personal Information in accordance with paragraph 6.2(e), the entity must make a written note of the use or disclosure.

Related bodies corporate

6.6 If:

(a) an APP entity is a body corporate; and

(b) the entity collects Personal Information from a related body corporate;

this principle applies as if the entity's primary purpose for the collection of the information were the primary purpose for which the related body corporate collected the information.

Exceptions

6.7 This principle does not apply to the use or disclosure by an organisation of:

(a) Personal Information for the purpose of direct marketing; or

(b) government related identifiers.

Australian Privacy Principle 7 — direct marketing

Direct marketing

7.1 If an organisation holds Personal Information about an individual, the organisation must not use or disclose the information for the purpose of direct marketing.

Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Exceptions — Personal Information other than Sensitive Information

7.2 Despite subclause 7.1, an organisation may use or disclose Personal Information (other than Sensitive Information) about an individual for the purpose of direct marketing if:

(a) the organisation collected the information from the individual; and

(b) the individual would reasonably expect the organisation to use or disclose the information for that purpose; and

(c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and

(d) the individual has not made such a request to the organisation.

7.3 Despite subclause 7.1, an organisation may use or disclose Personal Information (other than Sensitive Information) about an individual for the purpose of direct marketing if:

(a) the organisation collected the information from:

(i) the individual and the individual would not reasonably expect the organisation to use or disclose the information for that purpose; or

(ii) someone other than the individual; and

(b) either:

(i) the individual has consented to the use or disclosure of the information for that purpose; or

(ii) it is impracticable to obtain that consent; and

(c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and

(d) in each direct marketing communication with the individual:

(i) the organisation includes a prominent statement that the individual may make such a request; or

(ii) the organisation otherwise draws the individual's attention to the fact that the individual may make such a request; and

(e) the individual has not made such a request to the organisation.

Exception — Sensitive Information

7.4 Despite subclause 7.1, an organisation may use or disclose Sensitive Information about an individual for the purpose of direct marketing if the individual has consented to the use or disclosure of the information for that purpose.

Exception — contracted service providers

7.5 Despite subclause 7.1, an organisation may use or disclose Personal Information for the purpose of direct marketing if:

(a) the organisation is a contracted service provider for a Commonwealth contract; and

(b) the organisation collected the information for the purpose of meeting (directly or indirectly) an obligation under the contract; and

(c) the use or disclosure is necessary to meet (directly or indirectly) such an obligation.

Individual may request not to receive direct marketing communications etc.

7.6 If an organisation (the **first organisation**) uses or discloses Personal Information about an individual:

(a) for the purpose of direct marketing by the first organisation; or

(b) for the purpose of facilitating direct marketing by other organisations;

the individual may:

(c) if paragraph (a) applies — request not to receive direct marketing communications from the first organisation; and

(d) if paragraph (b) applies — request the organisation not to use or disclose the information for the purpose referred to in that paragraph; and

(e) request the first organisation to provide its source of the information.

7.7 If an individual makes a request under subclause 7.6, the first organisation must not charge the individual for the making of, or to give effect to, the request and:

(a) if the request is of a kind referred to in paragraph 7.6(c) or (d) — the first organisation must give effect to the request within a reasonable period after the request is made; and

(b) if the request is of a kind referred to in paragraph 7.6(e) — the organisation must, within a reasonable period after the request is made, notify the individual of its source unless it is impracticable or unreasonable to do so.

Interaction with other legislation

7.8 This principle does not apply to the extent that any of the following apply:

(a) the *Do Not Call Register Act 2006*;

(b) the *Spam Act 2003*;

(c) any other Act of the Commonwealth, or a Norfolk Island enactment, prescribed by the regulations.

Australian Privacy Principle 8 — cross-border disclosure of Personal Information

8.1 Before an APP entity discloses Personal Information about an individual to a person (the overseas recipient):

(a) who is not in Australia or an external Territory; and

(b) who is not the entity or the individual;

the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information.

Note: In certain circumstances, an act done, or a practice engaged in, by the overseas recipient is taken, under section 16C, to have been done, or engaged in, by the APP entity and to be a breach of the Australian Privacy Principles.

8.2 Subclause 8.1 does not apply to the disclosure of Personal Information about an individual by an APP entity to the overseas recipient if:

(a) the entity reasonably believes that:

(i) the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and

(ii) there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or

(b) both of the following apply:

(i) the entity expressly informs the individual that if he or she consents to the disclosure of the information, subclause 8.1 will not apply to the disclosure;

(ii) after being so informed, the individual consents to the disclosure; or

(c) the disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the disclosure of the information by the APP entity; or

(e) the entity is an agency and the disclosure of the information is required or authorised by or under an international agreement relating to information sharing to which Australia is a party; or

(f) the entity is an agency and both of the following apply:

(i) the entity reasonably believes that the disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body;

(ii) the recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body.

Note: For permitted general situation, see section 16A.

Australian Privacy Principle 9 — adoption, use or disclosure of government related identifiers

Adoption of government related identifiers

9.1 An organisation must not adopt a government related identifier of an individual as its own identifier of the individual unless:

(a) the adoption of the government related identifier is required or authorised by or under an Australian law or a court/tribunal order; or

(b) subclause 9.3 applies in relation to the adoption.

Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Use or disclosure of government related identifiers

9.2 An organisation must not use or disclose a government related identifier of an individual unless:

(a) the use or disclosure of the identifier is reasonably necessary for the organisation to verify the identity of the individual for the purposes of the organisation's activities or functions; or

(b) the use or disclosure of the identifier is reasonably necessary for the organisation to fulfil its obligations to an agency or a State or Territory authority; or

(c) the use or disclosure of the identifier is required or authorised by or under an Australian law or a court/tribunal order; or

(d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the use or disclosure of the identifier; or

(e) the organisation reasonably believes that the use or disclosure of the identifier is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(f) subclause 9.3 applies in relation to the use or disclosure.

Note 1: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Note 2: For permitted general situation, see section 16A.

Regulations about adoption, use or disclosure

9.3 This subclause applies in relation to the adoption, use or disclosure by an organisation of a government related identifier of an individual if:

(a) the identifier is prescribed by the regulations; and

(b) the organisation is prescribed by the regulations, or is included in a class of organisations prescribed by the regulations; and

(c) the adoption, use or disclosure occurs in the circumstances prescribed by the regulations.

Note: There are prerequisites that must be satisfied before the matters mentioned in this subclause are prescribed, see subsections 100(2) and (3).

Australian Privacy Principle 10 — quality of Personal Information

10.1 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the Personal Information that the entity collects is accurate, up-to-date and complete.

10.2 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the Personal Information that the entity uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

Australian Privacy Principle 11 — security of Personal Information

11.1 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.

11.2 If:

(a) an APP entity holds Personal Information about an individual; and

(b) the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Schedule; and

(c) the information is not contained in a Commonwealth record; and

(d) the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information;

the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.

Australian Privacy Principle 12 — access to Personal Information

Access

12.1 If an APP entity holds Personal Information about an individual, the entity must, on request by the individual, give the individual access to the information.

Exception to access — agency

12.2 If:

(a) the APP entity is an agency; and

(b) the entity is required or authorised to refuse to give the individual access to the Personal Information by or under:

(i) the Freedom of Information Act; or

(ii) any other Act of the Commonwealth, or a Norfolk Island enactment, that provides for access by persons to documents;

then, despite subclause 12.1, the entity is not required to give access to the extent that the entity is required or authorised to refuse to give access.

Exception to access — organisation

12.3 If the APP entity is an organisation then, despite subclause 12.1, the entity is not required to give the individual access to the Personal Information to the extent that:

(a) the entity reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or

(b) giving access would have an unreasonable impact on the privacy of other individuals; or

(c) the request for access is frivolous or vexatious; or

(d) the information relates to existing or anticipated legal proceedings between the entity and the individual, and would not be accessible by the process of discovery in those proceedings; or

(e) giving access would reveal the intentions of the entity in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(f) giving access would be unlawful; or

(g) denying access is required or authorised by or under an Australian law or a court/tribunal order; or

(h) both of the following apply:

(i) the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in;

(ii) giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or

(i) giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(j) giving access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process.

Dealing with requests for access

12.4 The APP entity must:

(a) respond to the request for access to the Personal Information:

(i) if the entity is an agency — within 30 days after the request is made; or

(ii) if the entity is an organisation — within a reasonable period after the request is made; and

(b) give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so.

Other means of access

12.5 If the APP entity refuses:

(a) to give access to the Personal Information because of subclause 12.2 or 12.3; or

(b) to give access in the manner requested by the individual;

the entity must take such steps (if any) as are reasonable in the circumstances to give access in a way that meets the needs of the entity and the individual.

12.6 Without limiting subclause 12.5, access may be given through the use of a mutually agreed intermediary.

Access charges

12.7 If the APP entity is an agency, the entity must not charge the individual for the making of the request or for giving access to the Personal Information.

12.8 If:

(a) the APP entity is an organisation; and

(b) the entity charges the individual for giving access to the Personal Information;

the charge must not be excessive and must not apply to the making of the request.

Refusal to give access

12.9 If the APP entity refuses to give access to the Personal Information because of subclause 12.2 or 12.3, or to give access in the manner requested by the individual, the entity must give the individual a written notice that sets out:

(a) the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

12.10 If the APP entity refuses to give access to the Personal Information because of paragraph 12.3(j), the reasons for the refusal may include an explanation for the commercially sensitive decision.

Australian Privacy Principle 13 — correction of Personal Information

Correction

13.1 If:

(a) an APP entity holds Personal Information about an individual; and

(b) either:

(i) the entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading; or

(ii) the individual requests the entity to correct the information;

the entity must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up to date, complete, relevant and not misleading.

Notification of correction to third parties

13.2 If:

(a) the APP entity corrects Personal Information about an individual that the entity previously disclosed to another APP entity; and

(b) the individual requests the entity to notify the other APP entity of the correction;

the entity must take such steps (if any) as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so.

Refusal to correct information

13.3 If the APP entity refuses to correct the Personal Information as requested by the individual, the entity must give the individual a written notice that sets out:

(a) the reasons for the refusal except to the extent that it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

Request to associate a statement

13.4 If:

(a) the APP entity refuses to correct the Personal Information as requested by the individual; and

(b) the individual requests the entity to associate with the information a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading;

the entity must take such steps as are reasonable in the circumstances to associate the statement in such a way that will make the statement apparent to users of the information.

Dealing with requests

13.5 If a request is made under subclause 13.1 or 13.4, the APP entity:

(a) must respond to the request:

(i) if the entity is an agency — within 30 days after the request is made; or

(ii) if the entity is an organisation — within a reasonable period after the request is made; and

(b) must not charge the individual for the making of the request, for correcting the Personal Information or for associating the statement with the Personal Information (as the case may be).

Schedule 3

Recommended Amendments to Privacy Notices

Handling your Enquiry

The Consumer Data Right scheme is governed under Part IVD of the *Competition and Consumer Act 2010* (Cth). Under the Consumer Data Right, the ACCC and the OAIC are co-regulators.

The OAIC collects and assesses all enquiries. Depending on the nature of your enquiry, the ACCC or OAIC may be best placed to respond. Therefore, information submitted in an enquiry may be provided to the ACCC if it is the most appropriate agency to provide a response.

Both the ACCC and the OAIC will handle your personal information in accordance with the Australian Privacy Principles.

If you have further questions about how we will handle your personal information, including how you can seek correction of your personal information or make a privacy complaint, you can refer to the ACCC's privacy policy and/or the OAIC's privacy policy.

Handling your CDR Report

The Consumer Data Right scheme is governed under Part IVD of the *Competition and Consumer Act 2010* (Cth). Under the CDR scheme, the Australian Competition and Consumer Commission (ACCC) and the Office of the Australian Information Commissioner (OAIC) are co-regulators.

The OAIC collects and assesses all reports. Depending on the nature of your report, the ACCC or OAIC may be best placed to assess that report. As such, the information you submit as part of your report may be provided to the ACCC, if it is the most appropriate agency to provide a response.

Both the ACCC and the OAIC will handle your personal information in accordance with the Australian Privacy Principles.

If you have further questions about how we will handle your personal information, including how you can seek correction of your personal information or make a privacy complaint, you can refer to the ACCC's privacy policy or the OAIC's privacy policy.

CDR Complaint Form

For further guidance on the personal information we collect and how we will handle your information, including how you can seek correction of your personal information or make a privacy complaint, please see the OAIC privacy policy.